VERİ KORUMA HUKUKU

Mevzuat & İçtihat

Dr. Mehmet Bedii KAYA
Furkan Güven TAŞTAN

Veri Koruma Hukuku: Mevzuat & İçtihat

İÇİNDEKİLER

v1.0

www.mbkaya.com / www.sinerjik.org

UYARI: İşbu çalışma **Dr. Mehmet Bedii KAYA** ile **Furkan Güven TAŞTAN** tarafından Veri Koruma Hukuku alanındaki kaynaklara pratik şekilde erişmek amacıyla hazırlanmıştır.

Editörler; kaynakların bütünlüğü, doğruluğu ve güncelliği konusunda herhangi bir taahhütte bulunmamaktadır!

Her türlü görüş, yorum veya katkınız için **mehmet@mbkaya.com** ve **furkanguventastan@gmail.com** eposta adreslerine iletebilirsiniz.

GÜNCELLEME GEÇMİŞİ

v 1.0 / 01.10.2016

- Veri Koruma Hukuku'nun ulusal ve uluslararası temel kaynakları eklenmiştir.

KULLANIM İPUCU: Belge, içindekiler kısmıyla birlikte hazırlanmıştır. Acrobat Reader ve benzeri programlarda belgeyi okurken "yer işaretleri" ya da "içindekiler tablosu" özelliğini kullanarak mevzuat metinleri arasında kolaylıkla geçiş yapabilirsiniz.

İÇİNDEKİLER

§ ULUSLARARASI DÜZENLEMELER

OECD ÖZEL YAŞAMIN KORUNMASI VE KİŞİSEL VERİLERİN SINIRÖTESİ AKIŞINA İLİŞKİN REHBER İLKELER (1980)

***Düzenlemenin orijinal ismi**: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data / Recommendation Of The Council Concerning Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data (23 September 1980)*

***Not**: Metin, 2013 yılında OECD tarafından yapılan güncellemeyi içermektedir.*

Tam metin için

http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Son erişim tarihi: 17.03.2016)

Preface

The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

For this reason, OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.

The Guidelines, in the form of a Recommendation by the Council of the OECD, were developed by a group of government experts under the chairmanship of The Hon. Mr. Justice M.D. Kirby, Chairman of the Australian Law Reform Commission. The Recommendation was adopted and became applicable on 23 September 1980.

The Guidelines are accompanied by an Explanatory Memorandum intended to provide information on the discussion and reasoning underlining their formulation.

OECD Council Recommendation

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (23 September 1980)

THE COUNCIL,

Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

RECOGNISING:

- that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;
- that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;
- that transborder flows of personal data contribute to economic and social development;
- that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS:

- that Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;
- that Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
- that Member countries co-operate in the implementation of the Guidelines set forth in the Annex;
- that Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

Annex to the Recommendation of the Council of 23rd September 1980

PART ONE.
GENERAL DEFINITIONS

1. For the purposes of these Guidelines:

a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

b) "personal data" means any information relating to an identified or identifiable individual (data subject);

c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of the Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

- a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
- b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
- c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

- a) as few as possible, and
- b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO.
BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE.
BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR.
NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

- a) adopt appropriate domestic legislation;
- b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
- c) provide for reasonable means for individuals to exercise their rights;
- d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
- e) ensure that there is no unfair discrimination against data subjects.

PART FIVE.
INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

information exchange related to these Guidelines, and

mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

EXPLANATORY MEMORANDUM

INTRODUCTION

A feature of OECD Member countries over the past decade has been the development of laws for the protection of privacy. These laws have tended to assume different forms in different countries, and in many countries are still in the process of being developed. The disparities in legislation may create obstacles to the free flow of information between countries. Such flows have greatly increased in recent years and are bound to continue to grow as a result of the introduction of new computer and communication technology. The OECD, which had been active in this field for some years past, decided to address the problems of diverging national legislation and in 1978 instructed a Group of Experts to develop Guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation. The Group has now completed its work.

The Guidelines are broad in nature and reflect the debate and legislative work which has been going on for several years in Member countries. The Expert Group which prepared the Guidelines has considered it essential to issue an accompanying Explanatory Memorandum. Its purpose is to explain and elaborate the Guidelines and the basic problems of protection of privacy and individual liberties. It draws attention to key issues that have emerged in the discussion of the Guidelines and spells out the reasons for the choice of particular solutions.

The first part of the Memorandum provides general background information on the area of concern as perceived in Member countries. It explains the need for international action and summarises the work carried out so far by the OECD and certain other international organisations. It concludes with a list of the main problems encountered by the Expert Group in its work.

Part Two has two subsections. The first contains comments on certain general features of the Guidelines, the second detailed comments on individual paragraphs.

This Memorandum is an information document, prepared to explain and describe generally the work of the Expert Group. It is subordinate to the Guidelines themselves. It cannot vary the meaning of the Guidelines but is supplied to help in their interpretation and application.

I. GENERAL BACKGROUND

The problems

1. The 1970s may be described as a period of intensified investigative and legislative activities concerning the protection of privacy with respect to the collection and use of personal data. Numerous official reports show that the problems are taken seriously at the political level and at the same time that the task of balancing opposing interests is delicate and unlikely to be accomplished once and for all. Public interest has tended to focus on the risks and implications associated with the computerised processing of personal data and some countries have chosen to enact statutes which deal exclusively with computers and computer-supported activities. Other countries have preferred a more general approach to privacy protection issues irrespective of the particular data processing technology involved.

2. The remedies under discussion are principally safeguards for the individual which will prevent an invasion of privacy in the classical sense, i.e. abuse or disclosure of intimate personal data; but other, more or less closely related needs for protection have become apparent. Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended, are two random examples. Generally speaking, there has been a tendency to broaden the traditional concept of privacy ("the right to be left alone") and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.

3. As far as the legal problems of automatic data processing (ADP) are concerned, the protection of privacy and individual liberties constitutes perhaps the most widely debated aspect. Among the reasons for such widespread concern are the ubiquitous use of computers for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically dispersed locations and enables the pooling of data and the creation of complex national and international data networks. Certain problems require particularly urgent attention, e.g. those relating to emerging international data networks, and to the need of balancing competing interests of privacy on the one hand and freedom of information on the other, in order to allow a full exploitation of the potentialities of modern data processing technologies in so far as this is desirable.

Activities at national level

4. Of the OECD Member countries more than one-third have so far enacted one or several laws which, among other things, are intended to protect individuals against abuse of data relating to them and to give them the right of access to data with a view to checking their accuracy and appropriateness. In federal states, laws of this kind may be found both at the national and at the state or provincial level. Such laws are referred to differently in different countries. Thus, it is common practice in continental Europe to talk about "data laws" or "data protection laws" (lois sur la protection des données), whereas in English speaking countries they are usually known as "privacy protection laws". Most of the statutes were enacted after 1973 and this present period may be described as one of continued or even widened legislative activity. Countries which already have statutes in

force are turning to new areas of protection or are engaged in revising or complementing existing statutes. Several other countries are entering the area and have bills pending or are studying the problems with a view to preparing legislation. These national efforts, and not least the extensive reports and research papers prepared by public committees or similar bodies, help to clarify the problems and the advantages and implications of various solutions. At the present stage, they provide a solid basis for international action.

5. The approaches to protection of privacy and individual liberties adopted by the various countries have many common features. Thus, it is possible to identify certain basic interests or values which are commonly considered to be elementary components of the area of protection. Some core principles of this type are: setting limits to the collection of personal data in accordance with the objectives of the data collector and similar criteria; restricting the usage of data to conform with openly specified purposes; creating facilities for individuals to learn of the existence and contents of data and have data corrected; and the identification of parties who are responsible for compliance with the relevant privacy protection rules and decisions. Generally speaking, statutes to protect privacy and individual liberties in relation to personal data attempt to cover the successive stages of the cycle beginning with the initial collection of data and ending with erasure or similar measures, and to ensure to the greatest possible extent individual awareness, participation and control.

6. Differences between national approaches as apparent at present in laws, bills or proposals for legislation refer to aspects such as the scope of legislation, the emphasis placed on different elements of protection, the detailed implementation of the broad principles indicated above, and the machinery of enforcement. Thus, opinions vary with respect to licensing requirements and control mechanisms in the form of special supervisory bodies ("data inspection authorities"). Categories of sensitive data are defined differently, the means of ensuring openness and individual participation vary, to give just a few instances. Of course, existing traditional differences between legal systems are a cause of disparity, both with respect to legislative approaches and the detailed formulation of the regulatory framework for personal data protection.

International aspects of privacy and data banks

7. For a number of reasons the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The tremendous increase in data flows across national borders and the creation of international data banks (collections of data intended for retrieval and other purposes) have highlighted the need for concerted national action and at the same time support arguments in favour of free flows of information which must often be balanced against requirements for data protection and for restrictions on their collection, processing and dissemination.

8. One basic concern at the international level is for consensus on the fundamental principles on which protection of the individual must be based. Such a consensus would obviate or diminish reasons for regulating the export of data and facilitate resolving problems of conflict of laws. Moreover, it could constitute a first step towards the development of more detailed, binding international agreements.

9. There are other reasons why the regulation of the processing of personal data should be considered in an international context: the principles involved concern values which many nations are anxious to uphold and see generally accepted; they may help to save costs in international data traffic; countries have a common interest in preventing the creation of locations where national regulations on data processing can easily be circumvented; indeed, in view of the international mobility of people, goods and commercial and scientific

activities, commonly accepted practices with regard to the processing of data may be advantageous even where no transborder data traffic is directly involved.

Relevant international activities

10. There are several international agreements on various aspects of telecommunications which, while facilitating relations and co-operation between countries, recognise the sovereign right of each country to regulate its own telecommunications (The International Telecommunications Convention of 1973). The protection of computer data and programmes has been investigated by, among others, the World Intellectual Property Organisation which has developed draft model provisions for national laws on the protection of computer software. Specialised agreements aiming at informational co-operation may be found in a number of areas, such as law enforcement, health services, statistics and judicial services (e.g. with regard to the taking of evidence).

11. A number of international agreements deal in a more general way with the issues which are at present under discussion, viz. the protection of privacy and the free dissemination of information. They include the European Convention of Human Rights of 4th November, 1950 and the International Covenant on Civil and Political Rights (United Nations, 19th December, 1966).

12. However, in view of the inadequacy of existing international instruments relating to the processing of data and individual rights, a number of international organisations have carried out detailed studies of the problems involved in order to find more satisfactory solutions.

13. In 1973 and 1974 the Committee of Ministers of the Council of Europe adopted two resolutions concerning the protection of the privacy of individuals vis-à-vis electronic data banks in the private and public sectors respectively. Both resolutions recommend that the governments of the Member states of the Council of Europe take steps to give effect to a number of basic principles of protection relating to the obtaining of data, the quality of data, and the rights of individuals to be informed about data and data processing activities.

14. Subsequently the Council of Europe, on the instructions of its Committee of Ministers, began to prepare an international Convention on privacy protection in relation to data processing abroad and transfrontier data processing. It also initiated work on model regulations for medical data banks and rules of conduct for data processing professionals. The Convention was adopted by the Committee of Ministers on 17 September 1980. It seeks to establish basic principles of data protection to be enforced by Member countries, to reduce restrictions on transborder data flows between the Contracting Parties on the basis of reciprocity, to bring about co-operation between national data protection authorities, and to set up a Consultative Committee for the application and continuing development of the convention.

15. The European Community has carried out studies concerning the problems of harmonization of national legislations within the Community, in relation to transborder data flows and possible distortions of competition, the problems of data security and confidentiality, and the nature of transborder data flows. A sub-committee of the European Parliament held a public hearing on data processing and the rights of the individual in early 1978. Its work has resulted in a report to the European Parliament in spring 1979. The report, which was adopted by the European Parliament in May 1979, contains a resolution on the protection of the rights of the individual in the face of technical developments in data processing.

Activities of the OECD

16. The OECD programme on transborder data flows derives from computer utilisation studies in the public sector which were initiated in 1969. A Group of Experts, the Data Bank Panel, analysed and studied different aspects of the privacy issue, e.g. in relation to digital information, public administration, transborder data flows, and policy implications in general. In order to obtain evidence on the nature of the problems, the Data Bank Panel organised a Symposium in Vienna in 1977 which provided opinions and experience from a diversity of interests, including government, industry, users of international data communication networks, processing services, and interested intergovernmental organisations.

17. A number of guiding principles were elaborated in a general framework for possible international action. These principles recognised:

- a) the need for generally continuous and uninterrupted flows of information between countries,
- b) the legitimate interests of countries in preventing transfers of data which are dangerous to their security or contrary to their laws on public order and decency or which violate the rights of their citizens,
- c) the economic value of information and the importance of protecting "data trade" by accepted rules of fair competition,
- d) the needs for security safeguards to minimise violations of proprietary data and misuse of personal information, and
- e) the significance of a commitment of countries to a set of core principles for the protection of personal information.

18. Early in 1978 a new ad hoc Group of Experts on Transborder Data Barriers and Privacy Protection was set up within the OECD which was instructed to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate a harmonization of national legislations, without this precluding at a later date the establishment of an international Convention. This work was to be carried out in close co-operation with the Council of Europe and the European Community and to be completed by 1 July 1979.

19. The Expert Group, under the chairmanship of the Honourable Mr. Justice Kirby, Australia, and with the assistance of Dr. Peter Seipel (Consultant), produced several drafts and discussed various reports containing, for instance, comparative analyses of different approaches to legislation in this field. It was particularly concerned with a number of key issues set out below.

- a) The specific, sensitive facts issue. The question arose as to whether the Guidelines should be of a general nature or whether they should be structured to deal with different types of data or activities (e.g. credit reporting). Indeed, it is probably not possible to identify a set of data which are universally regarded as being sensitive.
- b) The ADP issue. The argument that ADP is the main cause for concern is doubtful and, indeed, contested.

- c) The legal persons issue. Some, but by no means all, national laws protect data relating to legal persons in a similar manner to data related to physical persons.

- d) The remedies and sanctions issue. The approaches to control mechanisms vary considerably: for instance, schemes involving supervision and licensing by specially constituted authorities might be compared to schemes involving voluntary compliance by record-keepers and reliance on traditional judicial remedies in the Courts.

- e) The basic machinery or implementation issue. The choice of core principles and their appropriate level of detail presents difficulties. For instance, the extent to which data security questions (protection of data against unauthorised interference, fire, and similar occurrences) should be regarded as part of the privacy protection complex is debatable; opinions may differ with regard to time limits for the retention, or requirements for the erasure, of data and the same applies to requirements that data be relevant to specific purposes. In particular, it is difficult to draw a clear dividing line between the level of basic principles or objectives and lower level "machinery" questions which should be left to domestic implementation.

- f) The choice of law issue. The problems of choice of jurisdiction, choice of applicable law and recognition of foreign judgements have proved to be complex in the context of transborder data flows. The question arose, however, whether and to what extent it should be attempted at this stage to put forward solutions in Guidelines of a non-binding nature.

- g) The exceptions issue. Similarly, opinions may vary on the question of exceptions. Are they required at all? If so, should particular categories of exceptions be provided for or should general limits to exceptions be formulated?

- h) The bias issue. Finally, there is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth.

20. During its work the Expert Group maintained close contacts with corresponding organs of the Council of Europe. Every effort was made to avoid unnecessary differences between the texts produced by the two organisations; thus, the set of basic principles of protection are in many respects similar. On the other hand, a number of differences do occur. To begin with, the OECD Guidelines are not legally binding, whereas the Council of Europe has produced a convention which will be legally binding among those countries which ratify it. This in turn means that the question of exceptions has been dealt with in greater detail by the Council of Europe. As for the area of application, the Council of Europe Convention deals primarily with the automatic processing of personal data whereas the OECD Guidelines apply to personal data which involve dangers to privacy and individual liberties, irrespective of the methods and machinery used in their handling. At the level of details, the basic principles of protection proposed by the two organisations are not identical and the terminology employed differs in some respects. The institutional framework for continued co-operation is treated in greater detail in the Council of Europe Convention than in the OECD Guidelines.

21. The Expert Group also maintained co-operation with the Commission of the European Communities as required by its mandate.

II. THE GUIDELINES

A. Purpose and Scope

General

22. The Preamble of the Recommendation expresses the basic concerns calling for action. The Recommendation affirms the commitment of Member countries to protect privacy and individual liberties and to respect the transborder flows of personal data.

23. The Guidelines set out in the Annex to the Recommendation consist of five parts. Part One contains a number of definitions and specifies the scope of the Guidelines, indicating that they represent minimum standards. Part Two contains eight basic principles (Paragraphs 7-14) relating to the protection of privacy and individual liberties at the national level. Part Three deals with principles of international application, i.e. principles which are chiefly concerned with relationships between Member countries.

24. Part Four deals, in general terms, with means of implementing the basic principles set out in the preceding parts and specifies that these principles should be applied in a non-discriminatory manner. Part Five concerns matters of mutual assistance between Member countries, chiefly through the exchange of information and by avoiding incompatible national procedures for the protection of personal data. It concludes with a reference to issues of applicable law which may arise when flows of personal data involve several Member countries.

Objectives

25. The core of the Guidelines consists of the principles set out in Part Two of the Annex. It is recommended to Member countries that they adhere to these principles with a view to:

- a) achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data;
- b) reducing differences between relevant domestic rules and practices of Member countries to a minimum;
- c) ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and
- d) eliminating, as far as possible, reasons which might induce Member countries to restrict transborder flows of personal data because of the possible risks associated with such flows.

As stated in the Preamble, two essential basic values are involved: the protection of privacy and individual liberties and the advancement of free flows of personal data. The Guidelines attempt to balance the two values against one another; while accepting certain restrictions to free transborder flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.

26. Finally, Parts Four and Five of the Guidelines contain principles seeking to ensure:

- a) effective national measures for the protection of privacy and individual liberties;

- b) avoidance of practices involving unfair discrimination between individuals; and
- c) bases for continued international co-operation and compatible procedures in any regulation of transborder flows of personal data.

Level of detail

27. The level of detail of the Guidelines varies depending upon two main factors, viz. (a) the extent of consensus reached concerning the solutions put forward, and (b) available knowledge and experience pointing to solutions to be adopted at this stage. For instance, the Individual Participation Principle (Paragraph 13) deals specifically with various aspects of protecting an individual's interest, whereas the provision on problems of choice of law and related matters (Paragraph 22) merely states a starting-point for a gradual development of detailed common approaches and international agreements. On the whole, the Guidelines constitute a general framework for concerted actions by Member countries: objectives put forward by the Guidelines may be pursued in different ways, depending on the legal instruments and strategies preferred by Member countries for their implementation. To conclude, there is a need for a continuing review of the Guidelines, both by Member countries and the OECD. As and when experience is gained, it may prove desirable to develop and adjust the Guidelines accordingly.

Non-Member countries

28. The Recommendation is addressed to Member countries and this is reflected in several provisions which are expressly restricted to relationships between Member countries (see Paragraphs 15, 17 and 20 of the Guidelines). Widespread recognition of the Guidelines is, however, desirable and nothing in them should be interpreted as preventing the application of relevant provisions by Member countries to non-Member countries. In view of the increase in transborder data flows and the need to ensure concerted solutions, efforts will be made to bring the Guidelines to the attention of non-Member countries and appropriate international organisations.

The broader regulatory perspective

29. It has been pointed out earlier that the protection of privacy and individual liberties constitutes one of many overlapping legal aspects involved in the processing of data. The Guidelines constitute a new instrument, in addition to other, related international instruments governing such issues as human rights, telecommunications, international trade, copyright, and various information services. If the need arises, the principles set out in the Guidelines could be further developed within the framework of activities undertaken by the OECD in the area of information, computer and communications policies.

30. Some Member countries have emphasized the advantages of a binding international Convention with a broad coverage. The Mandate of the Expert Group required it to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, without this precluding at a later stage the establishment of an international Convention of a binding nature. The Guidelines could serve as a starting-point for the development of an international Convention when the need arises.

Legal persons, groups and similar entities

31. Some countries consider that the protection required for data relating to individuals may be similar in nature to the protection required for data relating to business enterprises, associations and groups which may or may not possess legal personality. The experience of a number of countries also shows that it is difficult to define clearly the dividing line between personal and non-personal data. For example, data relating to a small company may also concern its owner or owners and provide personal information of a more or less sensitive nature. In such instances it may be advisable to extend to corporate entities the protection offered by rules relating primarily to personal data.

32. Similarly, it is debatable to what extent people belonging to a particular group (i.e. mentally disabled persons immigrants, ethnic minorities) need additional protection against the dissemination of information relating to that group.

33. On the other hand, the Guidelines reflect the view that the notions of individual integrity and privacy are in many respects particular and should not be treated the same way as the integrity of a group of persons, or corporate security and confidentiality. The needs for protection are different and so are the policy frameworks within which solutions have to be formulated and interests balanced against one another. Some members of the Expert Group suggested that the possibility of extending the Guidelines to legal persons (corporations, associations) should be provided for. This suggestion has not secured a sufficient consensus. The scope of the Guidelines is therefore confined to data relating to individuals and it is left to Member countries to draw dividing lines and decide policies with regard to corporations, groups and similar bodies (cf. paragraph 49 below).

Automated and non-automated data

34. In the past, OECD activities in privacy protection and related fields have focused on automatic data processing and computer networks. The Expert Group has devoted special attention to the issue of whether or not these Guidelines should be restricted to the automatic and computer-assisted processing of personal data. Such an approach may be defended on a number of grounds, such as the particular dangers to individual privacy raised by automation and computerised data banks, and increasing dominance of automatic data processing methods, especially in transborder data flows, and the particular framework of information, computer and communications policies within which the Expert Group has set out to fulfil its Mandate.

35. On the other hand, it is the conclusion of the Expert Group that limiting the Guidelines to the automatic processing of personal data would have considerable drawbacks. To begin with, it is difficult, at the level of definitions, to make a clear distinction between the automatic and non-automatic handling of data. There are, for instance, "mixed" data processing systems, and there are stages in the processing of data which may or may not lead to automatic treatment. These difficulties tend to be further complicated by ongoing technological developments, such as the introduction of advanced semi-automated methods based on the use of microfilm, or microcomputers which may increasingly be used for private purposes that are both harmless and impossible to control. Moreover, by concentrating exclusively on computers the Guidelines might lead to inconsistency and lacunae, and opportunities for record-keepers to circumvent rules which implement the Guidelines by using non-automatic means for purposes which may be offensive.

36. Because of the difficulties mentioned, the Guidelines do not put forward a definition of "automatic data processing" although the concept is referred to in the preamble and in paragraph 3 of the Annex. It may be

assumed that guidance for the interpretation of the concept can be obtained from sources such as standard technical vocabularies.

37. Above all, the principles for the protection of privacy and individual liberties expressed in the Guidelines are valid for the processing of data in general, irrespective of the particular technology employed. The Guidelines therefore apply to personal data in general or, more precisely, to personal data which, because of the manner in which they are processed, or because of their nature or context, pose a danger to privacy and individual liberties.

38. It should be noted, however, that the Guidelines do not constitute a set of general privacy protection principles; invasions of privacy by, for instance, candid photography, physical maltreatment, or defamation are outside their scope unless such acts are in one way or another associated with the handling of personal data. Thus, the Guidelines deal with the building-up and use of aggregates of data which are organised for retrieval, decision-making, research, surveys and similar purposes. It should be emphasized that the Guidelines are neutral with regard to the particular technology used; automatic methods are only one of the problems raised in the Guidelines although, particularly in the context of transborder data flows, this is clearly an important one.

B. DETAILED COMMENTS

General

39. The comments which follow relate to the actual Guidelines set out in the Annex to the Recommendation. They seek to clarify the debate in the Expert Group.

Paragraph 1: Definitions

40. The list of definitions has been kept short. The term "data controller" is of vital importance. It attempts to define a subject who, under domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data. As defined, the data controller is a party who is legally competent to decide about the contents and use of data, regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. The data controller may be a legal or natural person, public authority, agency or any other body. The definition excludes at least four categories which may be involved in the processing of data, viz.:

- a) licensing authorities and similar bodies which exist in some Member countries and which authorise the processing of data but are not entitled to decide (in the proper sense of the word) what activities should be carried out and for what purposes;
- b) data processing service bureaux which carry out data processing on behalf of others;
- c) telecommunications authorities and similar bodies which act as mere conduits; and
- d) "dependent users" who may have access to data but who are not authorised to decide what data should be stored, who should be able to use them, etc. In implementing the Guidelines, countries may develop more complex schemes of levels and types of responsibilities.

Paragraphs 14 and 19 of the Guidelines provide a basis for efforts in this direction.

41. The terms "personal data" and "data subject" serve to underscore that the Guidelines are concerned with physical persons. The precise dividing line between personal data in the sense of information relating to identified or identifiable individuals and anonymous data may be difficult to draw and must be left to the regulation of each Member country. In principle, personal data convey information which by direct (e.g. a civil registration number) or indirect linkages (e.g. an address) may be connected to a particular physical person.

42. The term "transborder flows of personal data" restricts the application of certain provisions of the Guidelines to international data flows and consequently omits the data flow problems particular to federal states. The movements of data will often take place through electronic transmission but other means of data communication may also be involved. Transborder flows as understood in the Guidelines includes the transmission of data by satellite.

Paragraph 2: Area of application

43. The Section of the Memorandum dealing with the scope and purpose of the Guidelines introduces the issue of their application to the automatic as against non-automatic processing of personal data. Paragraph 2 of the Guidelines, which deals with this problem, is based on two limiting criteria. The first is associated with the concept of personal data: the Guidelines apply to data which can be related to identified or identifiable individuals. Collections of data which do not offer such possibilities (collections of statistical data in anonymous form) are not included. The second criterion is more complex and relates to a specific risk element of a factual nature, viz. that data pose a danger to privacy and individual liberties. Such dangers can arise because of the use of automated data processing methods (the manner in which data are processed), but a broad variety of other possible risk sources is implied. Thus, data which are in themselves simple and factual may be used in a context where they become offensive to a data subject. On the other hand, the risks as expressed in Paragraph 2 of the Guidelines are intended to exclude data collections of an obviously innocent nature (e.g. personal notebooks). The dangers referred to in Paragraph 2 of the Guidelines should relate to privacy and individual liberties. However, the protected interests are broad (cf. paragraph 2 above) and may be viewed differently by different Member countries and at different times. A delimitation as far as the Guidelines are concerned and a common basic approach are provided by the principles set out in Paragraphs 7 to 13.

44. As explained in Paragraph 2 of the Guidelines, they are intended to cover both the private and the public sector. These notions may be defined differently by different Member countries.

Paragraph 3: Different degrees of sensitivity

45. The Guidelines should not be applied in a mechanistic way irrespective of the kind of data and processing activities involved. The framework provided by the basic principles in Part Two of the Guidelines permits Member countries to exercise their discretion with respect to the degree of stringency with which the Guidelines are to be implemented, and with respect to the scope of the measures to be taken. In particular, Paragraph 3(b) provides for many "trivial" cases of collection and use of personal data (cf. above) to be completely excluded from the application of the Guidelines. Obviously this does not mean that Paragraph 3 should be regarded as a vehicle for demolishing the standards set up by the Guidelines. But, generally speaking, the Guidelines do not presuppose their uniform implementation by Member countries with respect to details. For instance, different traditions and different attitudes by the general public have to be taken into account. Thus, in one country universal personal identifiers may be considered both harmless and useful whereas in another country they may be regarded as highly sensitive and their use restricted or even forbidden. In one country, protection may be

afforded to data relating to groups and similar entities whereas such protection is completely non-existent in another country, and so forth. To conclude, some Member countries may find it appropriate to restrict the application of the Guidelines to the automatic processing of personal data. Paragraph 3(c) provides for such a limitation.

Paragraph 4: Exceptions to the Guidelines

46. To provide formally for exceptions in Guidelines which are part of a non-binding Recommendation may seem superfluous. However, the Expert Group has found it appropriate to include a provision dealing with this subject and stating that two general criteria ought to guide national policies in limiting the application of the Guidelines: exceptions should be as few as possible, and they should be made known to the public (e.g. through publication in an official government gazette). General knowledge of the existence of certain data or files would be sufficient to meet the second criterion, although details concerning particular data etc. may have to be kept secret. The formula provided in Paragraph 4 is intended to cover many different kinds of concerns and limiting factors, as it was obviously not possible to provide an exhaustive list of exceptions - hence the wording that they include national sovereignty, national security and public policy ("ordre public"). Another overriding national concern would be, for instance, the financial interests of the State ("crédit public"). Moreover, Paragraph 4 allows for different ways of implementing the Guidelines: it should be borne in mind that Member countries are at present at different stages of development with respect to privacy protection rules and institutions and will probably proceed at different paces, applying different strategies, e.g. the regulation of certain types of data or activities as compared to regulation of a general nature ("omnibus approach").

47. The Expert Group recognised that Member countries might apply the Guidelines differentially to different kinds of personal data. There may be differences in the permissible frequency of inspection, in ways of balancing competing interests such as the confidentiality of medical records versus the individual's right to inspect data relating to him, and so forth. Some examples of areas which may be treated differently are credit reporting, criminal investigation and banking. Member countries may also choose different solutions with respect to exceptions associated with, for example, research and statistics. An exhaustive enumeration of all such situations and concerns is neither required nor possible. Some of the subsequent paragraphs of the Guidelines and the comments referring to them provide further clarification of the area of application of the Guidelines and of the closely related issues of balancing opposing interests (compare with Paragraphs 7, 8, 17 and 18 of the Guidelines). To summarise, the Expert Group has assumed that exceptions will be limited to those which are necessary in a democratic society.

Paragraph 5: Federal countries

48. In Federal countries, the application of the Guidelines is subject to various constitutional limitations. Paragraph 5, accordingly, serves to underscore that no commitments exist to apply the Guidelines beyond the limits of constitutional competence.

Paragraph 6: Minimum standards

49. First, Paragraph 6 describes the Guidelines as minimum standards for adoption in domestic legislation. Secondly, and in consequence, it has been agreed that the Guidelines are capable of being supplemented by additional measures for the protection of privacy and individual liberties at the national as well as the international level.

Paragraph 7: Collection Limitation Principle

50. As an introductory comment on the principles set out in Paragraphs 7 to 14 of the Guidelines it should be pointed out that these principles are interrelated and partly overlapping. Thus, the distinctions between different activities and stages involved in the processing of data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole. Paragraph 7 deals with two issues, viz.:

- a) limits to the collection of data which, because of the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive; and

- b) requirements concerning data collection methods. Different views are frequently put forward with respect to the first issue. It could be argued that it is both possible and desirable to enumerate types or categories of data which are per se sensitive and the collection of which should be restricted or even prohibited.

There are precedents in European legislation to this effect (race, religious beliefs, criminal records, for instance). On the other hand, it may be held that no data are intrinsically " private" or "sensitive" but may become so in view of their context and use. This view is reflected, for example, in the privacy legislation of the United States.

51. The Expert Group discussed a number of sensitivity criteria, such as the risk of discrimination, but has not found it possible to define any set of data which are universally regarded as sensitive. Consequently, Paragraph 7 merely contains a general statement that there should be limits to the collection of personal data. For one thing, this represents an affirmative recommendation to lawmakers to decide on limits which would put an end to the indiscriminate collection of personal data. The nature of the limits is not spelt out but it is understood that the limits may relate to:

data quality aspects (i.e. that it should be possible to derive information of sufficiently high quality from the data collected, that data should be collected in a proper information framework, etc.);

- limits associated with the purpose of the processing of data (i.e. that only certain categories of data ought to be collected and, possibly, that data collection should be restricted to the minimum necessary to fulfil the specified purpose);

- "earmarking" of specially sensitive data according to traditions and attitudes in each Member country;

- limits to data collection activities of certain data controllers;

- civil rights concerns.

52. The second part of Paragraph 7 (data collection methods) is directed against practices which involve, for instance, the use of hidden data registration devices such as tape recorders, or deceiving data subjects to make them supply information. The knowledge or consent of the data subject is as a rule essential, knowledge being the minimum requirement. On the other hand, consent cannot always be imposed, for practical reasons. In addition, Paragraph 7 contains a reminder ("where appropriate") that there are situations where for practical or policy reasons the data subject's knowledge or consent cannot be considered necessary. Criminal investigation

activities and the routine up-dating of mailing lists may be mentioned as examples. Finally, Paragraph 7 does not exclude the possibility of a data subject being represented by another party, for instance in the case of minors, mentally disabled person, etc.

Paragraph 8: Data Quality Principle

53. Requirements that data be relevant can be viewed in different ways. In fact, some members of the Expert Group hesitated as to whether such requirements actually fitted into the framework of privacy protection. The conclusion of the Group was to the effect, however, that data should be related to the purpose for which they are to be used. For instance, data concerning opinions may easily be misleading if they are used for purposes to which they bear no relation, and the same is true of evaluative data. Paragraph 8 also deals with accuracy, completeness and up-to-dateness which are all important elements of the data quality concept. The requirements in this respect are linked to the purposes of data, i.e. they are not intended to be more far-reaching than is necessary for the purposes for which the data are used. Thus, historical data may often have to be collected or retained; cases in point are social research, involving so-called longitudinal studies of developments in society, historical research, and the activities of archives. The "purpose test" will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating.

Paragraph 9: Purpose Specification Principle

54. The Purpose Specification Principle is closely associated with the two surrounding principles, i.e. the Data Quality Principle and the Use Limitation Principle. Basically, Paragraph 9 implies that before, and in any case not later than at the time data collection it should be possible to identify the purposes for which these data are to be used, and that later changes of purposes should likewise be specified. Such specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies. According to Paragraphs 9 and 10, new purposes should not be introduced arbitrarily; freedom to make changes should imply compatibility with the original purposes. Finally, when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form. The reason is that control over data may be lost when data are no longer of interest; this may lead to risks of theft, unauthorised copying or the like.

Paragraph 10: Use Limitation Principle

55. This paragraph deals with uses of different kinds, including disclosure, which involve deviations from specified purposes. For instance, data may be transmitted from one computer to another where they can be used for unauthorised purposes without being inspected and thus disclosed in the proper sense of the word. As a rule the initially or subsequently specified purposes should be decisive for the uses to which data can be put. Paragraph 10 foresees two general exceptions to this principle: the consent of the data subject (or his representative - see Paragraph 52 above) and the authority of law (including, for example, licences granted by supervisory bodies). For instance, it may be provided that data which have been collected for purposes of administrative decision-making may be made available for research, statistics and social planning.

Paragraph 11: Security Safeguards Principle

56. Security and privacy issues are not identical. However, limitations on data use and disclosure should be reinforced by security safeguards. Such safeguards include physical measures (locked doors and identification cards, for instance), organisational measures (such as authority levels with regard to access to data) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them). It should be emphasized that the category of organisational measures includes obligations for data processing personnel to maintain confidentiality. Paragraph 11 has a broad coverage. The cases mentioned in the provision are to some extent overlapping (e.g. access/ disclosure). "Loss" of data encompasses such cases as accidental erasure of data, destruction of data storage media (and thus destruction of data) and theft of data storage media. "Modified" should be construed to cover unauthorised input of data, and "use" to cover unauthorised copying.

Paragraph 12: Openness Principle

57. The Openness Principle may be viewed as a prerequisite for the Individual Participation Principle (Paragraph 13); for the latter principle to be effective, it must be possible in practice to acquire information about the collection, storage or use of personal data. Regular information from data controllers on a voluntary basis, publication in official registers of descriptions of activities concerned with the processing of personal data, and registration with public bodies are some, though not all, of the ways by which this may be brought about. The reference to means which are "readily available" implies that individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost.

Paragraph 13: Individual Participation Principle

58. The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard. This view is shared by the Expert Group which, although aware that the right to access and challenge cannot be absolute, has chosen to express it in clear and fairly specific language. With respect to the individual sub-paragraphs, the following explanations are called for.

59. The right to access should as a rule be simple to exercise. This may mean, among other things, that it should be part of the day-to-day activities of the data controller or his representative and should not involve any legal process or similar measures. In some cases it may be appropriate to provide for intermediate access to data; for example, in the medical area a medical practitioner can serve as a go-between. In some countries supervisory organs, such as data inspection authorities, may provide similar services. The requirement that data be communicated within reasonable time may be satisfied in different ways. For instance, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests. Normally, the time is to be counted from the receipt of a request. Its length may vary to some extent from one situation to another depending on circumstances such as the nature of the data processing activity. Communication of such data "in a reasonable manner" means, among other things, that problems of geographical distance should be given due attention. Moreover, if intervals are prescribed between the times when requests for access must be met, such intervals should be reasonable. The extent to which data subjects should be able to obtain copies of data relating to them is a matter of implementation which must be left to the decision of each Member country.

60. The right to reasons in Paragraph 13(c) is narrow in the sense that it is limited to situations where requests for information have been refused. A broadening of this right to include reasons for adverse decisions in general, based on the use of personal data, met with sympathy in the Expert Group. However, on final consideration a right of this kind was thought to be too broad for insertion in the privacy framework constituted by the Guidelines. This is not to say that a right to reasons for adverse decisions may not be appropriate, e.g. in order to inform and alert a subject to his rights so that he can exercise them effectively.

61. The right to challenge in 13(c) and (d) is broad in scope and includes first instance challenges to data controllers as well as subsequent challenges in courts, administrative bodies, professional organs or other institutions according to domestic rules of procedure (compare with Paragraph 19 of the Guidelines). The right to challenge does not imply that the data subject can decide what remedy or relief is available (rectification, annotation that data are in dispute, etc.): such matters will be decided by domestic law and legal procedures. Generally speaking, the criteria which decide the outcome of a challenge are those which are stated elsewhere in the Guidelines.

Paragraph 14: Accountability Principle

62. The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly. it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel, "dependent users" (see paragraph 40) and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information (cf. paragraph 19 of the Guidelines). Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.

Paragraphs 15-18: Basic Principles of International Application

63. The principles of international application are closely interrelated. Generally speaking, Paragraph 15 concerns respect by Member countries for each other's interest in protecting personal data, and the privacy and individual liberties of their nationals and residents. Paragraph 16 deals with security issues in a broad sense and may be said to correspond, at the international level, to Paragraph 11 of the Guidelines. Paragraphs 17 and 18 deal with restrictions on free flows of personal data between Member countries; basically, as far as protection of privacy and individual liberties is concerned, such flows should be admitted as soon as requirements of the Guidelines for the protection of these interests have been substantially, i.e. effectively, fulfilled. The question of other possible bases of restricting transborder flows of personal data is not dealt with in the Guidelines.

64. For domestic processing Paragraph 15 has two implications. First, it is directed against liberal policies which are contrary to the spirit of the Guidelines and which facilitate attempts to circumvent or violate protective legislation of other Member countries. However, such circumvention or violation, although condemned by all Member countries, is not specifically mentioned in this Paragraph as a number of countries felt it to be unacceptable that one Member country should be required to directly or indirectly enforce, extraterritorially, the laws of other Member countries. -- It should be noted that the provision explicitly mentions the re-export of personal data. In this respect, Member countries should bear in mind the need to support each other's efforts

to ensure that personal data are not deprived of protection as a result of their transfer to territories and facilities for the processing of data where control is slack or non-existent.

65. Secondly, Member countries are implicitly encouraged to consider the need to adapt rules and practices for the processing of data to the particular circumstances which may arise when foreign data and data on non-nationals are involved. By way of illustration, a situation may arise where data on foreign nationals are made available for purposes which serve the particular interests of their country of nationality (e.g. access to the addresses of nationals living abroad).

66. As far as the Guidelines are concerned, the encouragement of international flows of personal data is not an undisputed goal in itself. To the extent that such flows take place they should, however, according to Paragraph 16, be uninterrupted and secure, i.e. protected against unauthorised access, loss of data and similar events. Such protection should also be given to data in transit, i.e. data which pass through a Member country without being used or stored with a view to usage in that country. The general commitment under Paragraph 16 should, as far as computer networks are concerned, be viewed against the background of the International Telecommunications Convention of Malaga-Torremolinos (25th October, 1973). According to that convention, the members of the International Telecommunications Union, including the OECD Member countries, have agreed, inter alia, to ensure the establishment, under the best technical conditions, of the channels and installations necessary to carry on the rapid and uninterrupted exchange of international telecommunications. Moreover, the members of ITU have agreed to take all possible measures compatible with the telecommunications system used to ensure the secrecy of international correspondence. As regards exceptions, the right to suspend international telecommunications services has been reserved and so has the right to communicate international correspondence to the competent authorities in order to ensure the application of internal laws or the execution of international conventions to which members of the ITU are parties. These provisions apply as long as data move through telecommunications lines. In their context, the Guidelines constitute a complementary safeguard that international flows of personal data should be uninterrupted and secure.

67. Paragraph 17 reinforces Paragraph 16 as far as relationships between Member countries are concerned. It deals with interests which are opposed to free transborder flows of personal data but which may nevertheless constitute legitimate grounds for restricting such flows between Member countries. A typical example would be attempts to circumvent national legislation by processing data in a Member country which does not yet substantially observe the Guidelines. Paragraph 17 establishes a standard of equivalent protection, by which is meant protection which is substantially similar in effect to that of the exporting country, but which need not be identical in form or in all respects. As in Paragraph 15, the re-export of personal data is specifically mentioned - in this case with a view to preventing attempts to circumvent the domestic privacy legislation of Member countries. - The third category of grounds for legitimate restrictions mentioned in Paragraph 17, concerning personal data of a special nature, covers situations where important interests of Member countries could be affected. Generally speaking, however, paragraph 17 is subject to Paragraph 4 of the Guidelines which implies that restrictions on flows of personal data should be kept to a minimum.

68. Paragraph 18 attempts to ensure that privacy protection interests are balanced against interests of free transborder flows of personal data. It is directed in the first place against the creation of barriers to flows of personal data which are artificial from the point of view of protection of privacy and individual liberties and fulfil restrictive purposes of other kinds which are thus not openly announced. However, Paragraph 18 is not

intended to limit the rights of Member countries to regulate transborder flows of personal data in areas relating to free trade, tariffs, employment, and related economic conditions for intentional data traffic. These are matters which were not addressed by the Expert Group, being outside its Mandate.

Paragraph 19: National Implementation

69. The detailed implementation of Parts Two and Three of the Guidelines is left in the first place to Member countries. It is bound to vary according to different legal systems and traditions, and Paragraph 19 therefore attempts merely to establish a general framework indicating in broad terms what kind of national machinery is envisaged for putting the Guidelines into effect. The opening sentence shows the different approaches which might be taken by countries, both generally and with respect to control mechanisms (e.g. specially set up supervisory bodies, existing control facilities such as courts, public authorities, etc.).

70. In Paragraph 19(a) countries are invited to adopt appropriate domestic legislation, the word "appropriate" foreshadowing the judgement by individual countries of the appropriateness or otherwise of legislative solutions. Paragraph 19(b) concerning self-regulation is addressed primarily to common law countries where non-legislative implementation of the Guidelines would complement legislative action. Paragraph 19(c) should be given a broad interpretation; it includes such means as advice from data controllers and the provision of assistance, including legal aid. Paragraph 19(d) permits different approaches to the issue of control mechanisms: briefly, either the setting-up of special supervisory bodies, or reliance on already existing control facilities, whether in the form of courts, existing public authorities or otherwise. Paragraph 19(e) dealing with discrimination is directed against unfair practices but leaves open the possibility of "benign discrimination" to support disadvantaged groups, for instance. The provision is directed against unfair discrimination on such bases as nationality and domicile, sex, race, creed, or trade union affiliation.

Paragraph 20: Information Exchange and Compatible Procedures

71. Two major problems are dealt with here, viz. (a) the need to ensure that information can be obtained about rules, regulations, decisions, etc. which implement the Guidelines, and (b) the need to avoid transborder flows of personal data being hampered by an unnecessarily complex and disparate framework of procedures and compliance requirements. The first problem arises because of the complexity of privacy protection regulation and data policies in general. There are often several levels of regulation (in a broad sense) and many important rules cannot be laid down permanently in detailed statutory provisions; they have to be kept fairly open and left to the discretion of lower-level decision-making bodies.

72. The importance of the second problem is, generally speaking, proportional to the number of domestic laws which affect transborder flows of personal data. Even at the present stage, there are obvious needs for co-ordinating special provisions on transborder data flows in domestic laws, including special arrangements relating to compliance control and, where required, licences to operate data processing systems.

Paragraph 21: Machinery for Co-operation

73. The provision on national procedures assumes that the Guidelines will form a basis for continued co-operation. Data protection authorities and specialised bodies dealing with policy issues in information and data communications are obvious partners in such a co-operation. In particular, the second purpose of such measures, contained in Paragraph 21(ii), i.e. mutual aid in procedural matters and requests for information, is

future-oriented: its practical significance is likely to grow as international data networks and the complications associated with them become more numerous.

Paragraph 22: Conflicts of Laws

74. The Expert Group has devoted considerable attention to issues of conflicts of laws, and in the first place to the questions as to which courts should have jurisdiction over specific issues (choice of jurisdiction) and which system of law should govern specific issues (choice of law). The discussion of different strategies and proposed principles has confirmed the view that at the present stage, with the advent of such rapid changes in technology, and given the non-binding nature of the Guidelines, no attempt should be made to put forward specific, detailed solutions. Difficulties are bound to arise with respect to both the choice of a theoretically sound regulatory model and the need for additional experience about the implications of solutions which in themselves are possible.

75. As regards the question of choice of law, one way of approaching these problems is to identify one or more connecting factors which, at best, indicate one applicable law. This is particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty. Moreover, it is not evident what value should presently be attributed to rules which by mechanistic application establish the specific national law to be applied. For one thing, the appropriateness of such a solution seems to depend upon the existence of both similar legal concepts and rule structures, and binding commitments of nations to observe certain standards of personal data protection. In the absence of these conditions, an attempt could be made to formulate more flexible principles which involve a search for a "proper law" and are linked to the purpose of ensuring effective protection of privacy and individual liberties. Thus, in a situation where several laws may be applicable, it has been suggested that one solution could be to give preference to the domestic law offering the best protection of personal data. On the other hand, it may be argued that solutions of this kind leave too much uncertainty, not least from the point of view of the data controllers who may wish to know, where necessary in advance, by which national systems of rules an international data processing system will be governed.

76. In view of these difficulties, and considering that problems of conflicts of laws might best be handled within the total framework of personal and non-personal data, the Expert Group has decided to content itself with a statement which merely signals the issues and recommends that Member countries should work towards their solution.

Follow-up

77. The Expert Group called attention to the terms of Recommendation 4 on the Guidelines which suggests that Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of the Guidelines.

BM BİLGİSAYARLA İŞLENEN KİŞİSEL VERİ DOSYALARINA İLİŞKİN REHBER İLKELER (1990)

Düzenlemenin orijinal ismi: *Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990*
Tam metin için: *http://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=3ddcafaac*
(Son erişim tarihi: 18.03.2016)

The procedures for implementing regulations concerning computerized personal data files are left to the initiative of each State subject to the following orientations:

A. PRINCIPLES CONCERNING THE MINIMUM GUARANTEES THAT SHOULD BE PROVIDED IN NATIONAL LEGISLATIONS

1. Principle of lawfulness and fairness

Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.

2. Principle of accuracy

Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.

3. Principle of the purpose-specification

The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:

(a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified;

(b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;

(c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified.

4. Principle of interested-person access

Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case ofunlawful, unnecessary or inaccurate entries and, when it is being

communicated, to be informed of the addressees. Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.

5. Principle of non-discrimination

Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.

6. Power to make exceptions

Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.

Exceptions to principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles I and 4, may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination.

7. Principle of security

Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.

8. Supervision and sanctions

The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-a- vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

9. Transborder data flows

When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocalsafeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.

10. Field of application

The present principles should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.

B. APPLICATION OF THE GUIDELINES TO PERSONAL DATA FILES KEPT BY GOVERNMENTAL INTERNATIONAL ORGANIZATIONS

The present guidelines should apply to personal data files kept by governmental international organizations, subject to any adjustments required to take account of any differences that might exist between files for internal purposes such as those that concern personnel management and files for external purposes concerning third parties having relations with the organization.

Each organization should designate the authority statutorily competent to supervise the observance of these guidelines.

Humanitarian clause: a derogation from these principles may be specifically provided for when the purpose of the file is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance.

A similar derogation should be provided in national legislation for governmental international organizations whose headquarters agreement does not preclude the implementation of the said national legislation as well as for non-governmental international organizations to which this law is applicable.

İNSAN HAKLARI EVRENSEL BEYANNAMESİNİN İLGİLİ HÜKÜMLERİ (1948)

> ***Düzenlemenin orijinal ismi:*** *Universal Declaration of Human Rights.*
> ***Düzenleme künyesi:*** *Birleşmiş Milletler Genel Kurulu'nun 10 Aralık 1948 tarih ve 217 A(III) sayılı Kararı.*
> ***Düzenlemenin orijinal metni için:*** *http://www.un.org/en/universal-declaration-human-rights/*
> *(Son erişim tarihi: 16.04.2016)*
> ***Düzenlemenin Türkiye künyesi:*** *6 Nisan 1949 tarih ve 9119 Sayılı Bakanlar Kurulu ile "İnsan Hakları Evrensel Beyannamesi'nin Resmi Gazete ile yayınlanması yayımdan sonra okullarda ve diğer eğitim müesseselerinde okutulması ve yorumlanması ve bu Beyanname hakkında radyo ve gazetelerde münasip neşriyatta bulunulması" kararlaştırılmıştır. Bakanlar Kurulu Kararı 27 Mayıs 1949 tarih ve 7217 Sayılı Resmi Gazete'de yayınlanmıştır.*
> ***Düzenlemenin Türkçe tam metni için:*** *http://www.ombudsman.gov.tr/contents/files/688B1--Insan-Haklari-Evrensel-Beyannamesi.pdf (Son erişim tarihi: 16.04.2016)*

Birleşmiş Milletler Genel Kurulu;

İnsanlık topluluğunun bütün bireyleriyle kuruluşlarının bu Bildirgeyi her zaman göz önünde tutarak eğitim ve öğretim yoluyla bu hak ve özgürlüklere saygıyı geliştirmeye, giderek artan ulusal ve uluslararası önlemlerle gerek üye devletlerin halkları ve gerekse bu devletlerin yönetimi altındaki ülkeler halkları arasında bu hakların dünyaca etkin olarak tanınmasını ve uygulanmasını sağlamaya çaba göstermeleri amacıyla tüm halklar ve uluslar için ortak ideal ölçüleri belirleyen bu İnsan Hakları Evrensel Bildirgesini ilan eder.

Madde 12

Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır.

KİŞİSEL VE SİYASAL HAKLAR SÖZLEŞMESİNİN İLGİLİ HÜKÜMLERİ (1966)

Düzenlemenin orijinal ismi: *International Covenant on Civil and Political Rights*
Düzenleme künyesi: *Birleşmiş Milletler Genel Kurulu tarafından 19 Aralık 1966 tarihinde 2200 A (XXI) sayılı kararıyla kabul edilmiştir.*
Düzenlemenin orijinal tam metni için:
https://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-English.pdf
(Son erişim tarihi: 18.03.2016)
Düzenlemenin Türkiye künyesi: Türkiye sözleşmeyi 15 Ağustos 2000 tarihinde imzalamıştır, ancak sözleşme TBMM ve Cumhurbaşkanı tarafından onaylanmamıştır.
Düzenlemenin Türkçe tam metni için:
http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktaraflisoz/bm/bm_05.pdf
(Son erişim tarihi: 18.03.2016)

Madde 17- Mahremiyet Hakkı

(1) Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz.

(2) Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir.

§ AVRUPA KONSEYİ DÜZENLEMELERİ

108 NO'LU KİŞİSEL VERİLERİN, OTOMATİK İŞLEMESİ KARŞISINDA BİREYLERİN KORUNMASI SÖZLEŞMESİ (1981)

Düzenlemenin orijinal ismi: *Convention For The Protection Of İndividuals With Regard To Automatic Processing Of Personal Data*
Düzenlemenin künyesi: *European Treaty Series No. 108 / 28.01.1981*
Düzenlemenin orijinal metni için:
http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37
(Son erişim tarihi: 16.04.2016)
Düzenlemenin Türkiye künyesi: *28.01.1981 tarihinde Türkiye, bu sözleşmeyi imzalayan ilk ülkelerden birisi olmuştur. Ancak sözleşmenin uygun bulunması ve onaylanması yaklaşık 35 yıl sürmüştür: Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi 6669 sayılı Kanun'la uygun bulunmuş ve bu Kanun, ilişik beyanlarla birlikte onaylanarak 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazete'de yayınlanmıştır.*
Düzenlemenin Türkçe metni için:
http://www.resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf (Son erişim tarihi: 22.04.2016)

Gerekçe

Günümüzde insan haklarının korunması bilincinin gelişmesiyle eş zamanlı olarak, kişisel verilerin korunmasının önemi de her geçen gün artmaktadır. Bu çerçevede gelişmiş ülkelerde kişisel verilerin korunması alanında detaylı yasal düzenlemelerin uygulanmakta olduğu dikkat çekmektedir. Öte yandan, 20 inci yüzyılda bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişmeler nedeniyle kişisel verilerin kayıt altına alınmasında ciddi bir artış yaşanmış, internetin yaygınlaşması ise konuyu daha hassas bir boyuta taşımıştır.

Türkiye, kişisel verilerin korunmasıyla ilgili uluslararası düzenlemeleri takip ederek, ulusal düzenlemelerine bu çerçevede yön vermektedir. 2010 yılında Anayasada yapılan değişikliklerle kişisel verilerin korunması anayasal bir hak haline getirilmiştir.

Avrupa Konseyi (AK) bünyesinde hazırlanarak 28 Ocak 1981 tarihinde Strazburg'da imzaya açılan ve 1 Ekim 1985 tarihinde yürürlüğe giren 'Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi' ülkemiz tarafından 28 Ocak 1981 tarihinde imzalanmıştır. Anılan Sözleşmeye AK dışındaki ülkelerin de taraf olma imkanı bulunmaktadır.

108 sayılı Sözleşme olarak da bilinen ve 27 maddeden oluşan Sözleşmenin temel amacı; her üye ülkede, uyruğu veya ikametgahı ne olursa olsun gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren

kişisel nitelikteki verilerin otomatik bilgi işleme tabi tutulması karşısında özel yaşam haklarım güvence altına almaktır. Bu itibarla Sözleşme, hükümetlerin vatandaşlarını korumasına yönelik önemli bir araç niteliğindedir.

Bugüne kadar AK üyesi bütün ülkeler ve AK dışından Uruguay olmak üzere toplam 47 ülke Sözleşmeye taraf olmuş, 46 ülke ise Sözleşmeyi onaylamıştır. Türkiye Sözleşmeyi imzalamış olmasına rağmen, onay işlemlerini henüz tamamlamayıp yürürlüğe koymayan tek ülke konumundadır.

108 sayılı Sözleşmenin ülkemizce onaylanarak yürürlüğe konması konusunda zamanında yapılan değerlendirmede, Sözleşmenin iç hukuk düzenlemelerinin tamamlanmasının ardından onaylanması ve yürürlüğe konulmasının uygun olacağı sonucuna varılmıştır. Konunun önemi çerçevesinde, Sözleşme ile ilgili iç hukuk gereklerinin Sözleşmenin onay süreciyle birlikte eş zamanlı yürütülmesi keyfiyeti gündeme gelmiştir.

Ülkemizde kişisel verilerin korunması bağlamında sürdürülmekte olan ulusal mevzuat çalışmalarına da paralel olarak, sözkonusu Sözleşmenin onaylanması, ülkemizin Avrupa Konseyi çerçevesinde oluşturulan ortak hukuk sistemine kişisel verilerin korunması alanında da dâhil olmasını sağlayarak, vatandaşlarımızın insan haklarının ihlal edilmesinin önüne geçilmesine ve ülkemizin uluslararası saygınlığına katkıda bulunacaktır.

Giriş

İşbu Sözleşmeyi imzalayan Avrupa Konseyi Üyesi Devletler,

Avrupa Konseyinin amacının özellikle hukukun üstünlüğüne ve insan hakları ile temel özgürlüklere saygılı olarak, üyeleri arasında daha yakın bir birliğin gerçekleştirilmesi olduğuna inanarak;

Otomatik işleme tabi olan kişisel verilerin sınırlar ötesi akışının yoğunluk kazanması karşısında, temel hak ve özgürlüklere ilişkin güvencelerin, özellikle de özel yaşama saygı hakkının genişletilmesinin arzu edilebilir olduğunu değerlendirerek;

Aynı zamanda sınırları dikkate almaksızın haber alma özgürlüğüne ilişkin yükümlülüklerini de teyit ederek;

Temel değerler olan özel yaşama saygı ile halklar arasında serbest bilgi akışını birbiriyle uzlaştırma gerekliliğini kabul ederek;

Aşağıdaki hususlarda anlaşmışlardır:

Bölüm I - Genel hükümler

Madde 1 Konu ve amaç

İşbu Sözleşmenin amacı, her bir Tarafın ülkesinde, uyruğu veya ikamet yeri ne olursa olsun her gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayata saygı hakkını güvence altına almaktır. ("verilerin korunması").

Madde 2 Tanımlar

Bu Sözleşmenin amaçları bakımından:

a) "Kişisel veriler": Kimliği belirli veya belirlenebilir bir gerçek kişi ("ilgili kişi") hakkındaki tüm bilgileri ifade eder;

b) "Otomatik veri dosyası" otomatik işleme konu olan bilgilerin tümünü ifade eder;

c) "Otomatik işlem"den, tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılır.

d) "Dosya yöneticisi", otomatik veri dosyasının amacının ne olacağı, hangi kişisel veri kategorilerinin kaydedilmesi gerektiği ve bunlara hangi işlemlerin uygulanacağı hakkında karar verebilecek olan gerçek veya tüzel kişileri, kamu kurumunu, birimi veya ulusal kanunlara göre yetkili olan diğer kuruluşları ifade eder.

Madde 3 Kapsam

1. Taraflar, işbu Sözleşmeyi kamu sektöründe ve özel sektörde, otomatik kişisel veri dosyalarına ve kişisel verilerin otomatik işleme tabi tutulması konusunda uygulamayı taahhüt ederler.

2. Her devlet, imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgelerin.in tevdi edilmesi sırasında veya daha sonra herhangi bir zamanda Avrupa Konseyi Genel Sekreterine muhatap bir beyanla:

a) İşbu Sözleşmeyi, listesi tevdi edilecek olan belli otomatik kişisel veri dosyası kategorilerine uygulamayacağını bildirebilir. Ancak, devlet bu listeye, kendi iç hukukunun otomatik verilerin korunmasına ilişkin hükümlerine tabi olan otomatik dosya kategorilerini dahil edemez. Bu nedenle, ilave otomatik kişisel veri dosyası kategorilerinin kendi iç hukukunun verilerin korunmasına ilişkin hükümlerine tabi kılınması halinde, yapacağı yeni bir beyanla sözkonusu listeyi tadil eder;

b) İşbu Sözleşmeyi, topluluklar, dernekler, vakıflar, şirketler, kurumlar ve tüzel kişiliğe sahip olsun veya olmasın, doğrudan veya dolaylı olarak gerçek kişilerin bir araya gelmesiyle oluşmuş her çeşit diğer kuruluş hakkında da uygulayacağını bildirebilir;

c) İşbu Sözleşmeyi, otomatik bilgi işleme konu olmayan kişisel veri dosyaları hakkında da uygulayacağını bildirebilir.

3. Yukarıdaki 2. fıkranın b veya c bendinde tanımlanan beyanlardan biriyle işbu Sözleşmen.in uygulama alanını genişleten her devlet, sözkonusu beyanda, genişletmen.in ancak tevdi edeceği bir listede gösterilen bazı kişisel dosya kategorilerine uygulanacağını belirtebilir.

4. Yukarıdaki 2. fıkranın a bendinde öngörülen beyanla belli otomatik kişisel veri dosyası kategorilerini Sözleşmen.in uygulama alam dışında tutan Taraf, bunları uygulama alanı dışında tutmayan bir Taraftan işbu Sözleşmenin sözkonusu kategoriler hakkında uygulanmasını isteyemez.

5. Keza, işbu maddenin 2. b ve 2. c bentlerinde öngörülen kapsam genişletmelerinden herhangi birini yapmayan Taraf, bu genişletmeleri yapan herhangi bir Tarafın bu hususlarda Sözleşmeyi uygulaması gerektiğini öne süremez.

6. İşbu maddenin yukarıdaki 2. fıkrasında öngörülen beyanlar, bunları yapmış olan Devlet bakımından, bu beyanların imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgelerinin tevdi edilmesi sırasında yapılması halinde, sözleşmen.in yürürlüğe girdiği tarihte; eğer beyanlar daha sonra yapılmışsa bunların Avrupa Konseyi Genel Sekreteri tarafından alınmasından üç ay sonra hüküm ifade eder. Bu beyanlar Avrupa Konseyi Genel Sekreterine muhatap bir bildirim ile kısmen veya tamamen geri alınabilir. Beyanların geri alınması, bildirimin alındığı tarihten üç ay sonra hüküm ifade eder.

Bölüm II - Verilerin korunmasına ilişkin temel ilkeler

Madde 4 Tarafların Görevleri

1. Her Taraf, kendi iç hukukunda, işbu bölümde yer alan verilerin korunmasına ilişkin temel ilkelere işlerlik kazandırmak amacıyla gerekli önlemleri alır.

2. Bu önlemlerin Tarafça, en geç, Sözleşmenin kendisi bakımından yürürlüğe girdiği tarihte alınması zorunludur.

Madde 5 Verilerin niteliği

Otomatik işleme konu olan kişisel veriler:

a) Adil biçimde ve yasal yoldan elde edilir ve işlenir;

b) Belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılmaz;

c) Kaydedilme amaçlarına göre uygun ve yerinde olur ve aşırı olmaz;

d) Doğru bilgileri yansıtır ve gerektiğinde güncellenir;

e) Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır.

Madde 6 Özel veri kategorileri

İç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel veriler, otomatik işleme tabi tutulmaz. Aynı şey ceza mahkumiyetiyle ilgili kişisel veriler için de geçerlidir.

Madde 7 Verilerin güvenliği

Otomatik dosyalara kaydedilen kişisel verileri korumak için, bunların kaza sonucu veya izinsiz olarak imhasına veya kaza sonucu kaybolmasına veya bunların izinsiz olarak elde edilmesine, değiştirilmesine veya dağıtılmasına karşı uygun güvenlik önlemleri alınır,

Madde 8 İlgili kişi hakkındaki ek güvenceler

Herkes:

a) Otomatik kişisel veri dosyasının mevcudiyetini, temel amaçlarını, dosya yöneticisinin kimliğini ve mutat ikamet yerini veya başlıca işyerini öğrenmek;

b) Makul aralıklarla ve aşırı gecikmeye veya masrafa maruz kalmadan kendisi ile ilgili kişisel verilerin otomatik dosyada bulunup bulunmadığının teyidini almak ve bu bilgilerin kendisine anlaşılır bir biçim altında iletilmesini sağlamak;

c) Gerekli olan durumlarda, bu verileri düzelttirmek veya bunların, işbu Sözleşmenin 5. ve 6. maddelerinde belirtilen temel ilkelere işlerlik sağlayan iç hukuk hükümlerinin ihlali suretiyle işlenmiş olması halinde, sözkonusu verileri sildirtmek;

d) İşbu maddenin b ve c fıkralarında öngörülen teyit talebinin veya duruma göre bildirim, düzeltme veya silme talebinin yerine getirilmemesi halinde bir başvuru yolundan yararlanmak hakkına sahiptir.

Madde 9 İstisnalar ve kısıtlamalar

1. İşbu maddede belirtilen sınırlar dışında, Sözleşmenin 5, 6 ve 8. maddeleri hükümlerine hiçbir istisna getirilemez.

2. Taraf devletin kanunlarında öngörülmüş olması ve demokratik bir toplumda aşağıdaki hususların sağlanması için gerekli bir önlem oluşturması halinde işbu Sözleşmenin 5, 6 ve 8. maddelerine istisna getirilebilir:

a) Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi;

b) İlgili kişinin veya başkasının hak ve özgürlüklerinin korunması.

3. İlgili kişilerin özel yaşamlarına tecavüz tehlikesi bulunmadığının açık olduğu durumlarda, 8. maddenin b, c ve d fıkralarında düzenlenen haklar istatistiki veya bilimsel amaçlar için kullanılan kişisel veri dosyaları bakımından kanunla kısıtlanabilir.

Madde 10 Yaptırımlar ve başvuru yolları

Her bir Taraf, işbu bölümde düzenlenen verilerin korunması hakkındaki temel ilkelere işlerlik sağlayan iç hukuk kurallarının ihlaliyle ilgili uygun yaptırımlar ve başvuru yolları getirmekle yükümlüdür.

Madde 11 Genişletilmiş koruma

İşbu bölümde yer alan hükümlerden hiçbiri, her devletin, ilgili kişilere işbu Sözleşmede öngörülenden daha fazla koruyucu önlem sağlaması imkanını sınırlayacak veya buna halel getirecek şekilde yorumlanamaz.

Bölüm III - Sınır ötesi veri akışları

Madde 12 Kişisel verilerin sınır ötesi akışı ve iç hukuk

1. Otomatik işleme konu olan veya otomatik işleme konu olmak üzere toplanmış olan kişisel verilerin her türlü yoldan ulusal sınırların ötesine transferinde aşağıdaki hükümler uygulanır.

2. Bir Taraf, münhasıran özel yaşamın korunması amacıyla kişisel verilerin diğer bir Tarafa sınır ötesi akışım yasaklayamaz veya özel müsaadeye tabi tutamaz.

3. Bununla birlikte her bir Taraf, 2. fıkradaki hükümlere aşağıdaki durumlarda istisnalar getirebilir:

a) Kendi mevzuatının, belli kişisel veri veya otomatik kişisel veri dosyası kategorileri için, bu verilerin veya dosyaların doğasından kaynaklanan özel düzenlemeler içermesi, diğer Tarafın düzenlemelerinin ise eşdeğer bir koruma içermemesi durumunda;

b) Bu transferin bir Tarafın ülkesinden, bir diğer Taraf üzerinden Taraf olmayan bir devletin ülkesine yapılması durumunda, bu bendin başında atıfta bulunulan Tarafın mevzuatının boşluklarından yararlanmak üzere yapılacak bu tür transferleri engellemek amacıyla.

Bölüm IV - Karşılıklı yardımlaşma

Madde 13 Taraflar arasında işbirliği

1. Taraflar, işbu Sözleşmeyi uygulamak üzere birbirlerine karşılıklı yardımda bulunmayı taahhüt ederler.

2. Bu amaçla:

a) Taraflardan her biri bir veya birden fazla makam tayin ederek, bunların isim ve adreslerini Avrupa Konseyi Genel Sekreterine bildirir;

b) Birden fazla makam tayin eden her bir Taraf, yukarıdaki bentte atıfta bulunulan bildirimde, bu mercilerden her birinin yetkisini belirtir.

3. Taraflardan birinin tayin ettiği bir makam, diğer Tarafın tayin ettiği bir makamın talebi üzerine:

a) Verilerin korunması hakkındaki hukukuna ve idari uygulamalara ilişkin bilgileri verir.

b) İç hukukuna ve münhasıran özel yaşamın korunması amacına uygun olarak, otomatik işleme konu olan kişisel verilerin kendileri istisna olmak üzere, ülkesinde gerçekleştirilen otomatik işlemlerle ilgili somut bilgilerin sağlanması için gerekli tüm önlemleri alır.

Madde 14 Yabancı ülkelerde ikamet eden ilgili kişilere yardım

1. Taraflardan her biri, kendi iç hukukunda öngörülen, işbu Sözleşmenin 8. maddesinde belirtilen ilkelere işlerlik kazandıran hakların kullanılması için, yabancı ülkede ikamet eden tüm kişilere yardımda bulunur.

2. Eğer böyle bir kişi diğer bir Tarafın ülkesinde ikamet ediyorsa, talebini bu Tarafın tayin ettiği makama yapma imkanına da sahip olmalıdır.

3. Yardım talebi, gerekli tüm bilgileri, diğerleri yanında özellikle aşağıdakilerle ilgili bilgileri içerir:

a) Talepte bulunanın isim ve adresi ile bu kişiyi belirlemeye yarayan tüm hususlar,

b) Talebin konusu kişisel verilerin yer aldığı otomatik dosya veya yöneticisi,

c) Talebin amacı.

Madde 15 Tayin edilen makamlarca sağlanan yardıma ilişkin güvenceler

1. Bir Tarafın tayin ettiği makam, ne kendisine muhatap bir yardım talebini desteklemek amacıyla talebe eklenen bilgiyi, ne de kendi talep ettiği yardım üzerine diğer bir Tarafın tayin ettiği makamdan sağladığı bilgiyi, yardım talebinde belirtilen amaçlar dışında kullanabilir.

2. Taraflardan her biri, tayin edilen makamın personelinin veya bu makam adına hareket eden kişilerin, bu bilgilerin gizli tutulması veya paylaşılmaması hususunda yükümlülüklere tabi olmasını sağlayacaktır.

3. Tayin edilen makam hiçbir durumda, 14. maddenin 2. fıkrasına göre yabancı ülkede ika eden ilgili kişinin muvafakatini almadan, kendi insiyatifiyle bu kişi adına yardım talebinde bulunmaya yetkili kılınmayacaktır.

Madde-16 Yardım taleplerinin reddi

İşbu Sözleşmenin 13 ve 14. maddeleri uyarınca kendisine yardım talebi intikal eden tayin edilmiş makam, aşağıdaki durumlar dışında yardım talebini reddedemez:

a) Yapılan talep, yanıt vermekle sorumlu makamın verilerin korunması konusundaki yetkisi dışında kalıyorsa;
b) Talep, işbu Sözleşme hükümlerine uygun değilse;
c) Talebin yerine getirilmesi, bunu yerine getirecek makamın bağlı olduğu devletin egemenliğine, güvenliğine veya kamu düzenine veya bu devletin yetkisi altındaki kişilerin haklarına ve temel özgürlüklerine aykırı ise.

Madde 17 Yardım giderleri ve yöntemleri

1. Tarafların 13. madde uyarınca birbirlerine yaptıkları karşılıklı yardım ile 14. madde uyarınca yabancı ülkede ikamet eden ilgili kişilere yaptıkları yardım, uzman ve tercüman ücretleri dışında, hiçbir masraf veya harcı gerektirmeyecektir. Bu masraf ve harçlar, yardım talebinde bulunan makamı tayin eden Tarafça karşılanacaktır.

2. İlgili kişi, bir başka Tarafın ülkesinde kendi hesabına yapılan işlemlerle ilgili olarak, bu Tarafın ülkesinde ikamet eden kişilerce yasal olarak ödenmesi gereken harç ve masraf dışında, hiçbir harç ve masraf ödemek zorunda olmayacaktır.

3. Yardımla ilgili diğer hususlar ve özellikle yardımın şekli ve usulü ile kullanılacak dile ilişkin konular, ilgili Taraflar arasında doğrudan kararlaştırılacaktır.

Bölüm V - Danışma Komitesi

Madde 18 Komitenin oluşumu

1. İşbu Sözleşmenin yürürlüğe girmesinden soma bir Danışma Komitesi kurulur.

2. Taraflardan her biri, bu komiteye bir asıl temsilci, bir de temsilci vekili tayin eder. Sözleşmeye taraf olmayan Avrupa Konseyi üyesi her devlet Danışma Komitesinde bir gözlemci tarafından temsil edilme hakkına sahiptir.

3. Danışma Komitesi, oybirliği ile alacağı bir kararla, Avrupa Konseyi üyesi olmayan ve Sözleşmeye taraf olmayan herhangi bir devleti, belli bir oturumunda bir gözlemci tarafından temsil edilmeye davet edebilir.

Madde 19 Komitenin işlevleri Danışma Komitesi:

a. Sözleşmenin uygulanmasını kolaylaştırmak veya iyileştirmek amacıyla önerilerde bulunabilir;

b. Aşağıdaki 21. Maddeye uygun olarak Sözleşmede değişiklik yapılmasını önerebilir;

c. Sözleşmede değişiklik yapılmasına ilişkin olarak 21. maddenin 3. fıkrası uyarınca kendisine sunulan tüm öneriler hakkında görüş bildirir;

d. Taraflardan birinin talebi üzerine, işbu Sözleşmenin uygulanması ile ilgili tüm sorular hakkında görüş bildirebilir.

Madde 20 Usul

1. Danışma Komitesi, Avrupa Konseyi Genel Sekreteri tarafından toplantıya çağırılır. Komite ilk toplantısını, işbu Sözleşmenin yürürlüğe girmesini izleyen on iki ay içerisinde yapar. Komite, müteakip toplantılarını en az iki yılda bir yapar; ayrıca Tarafların temsilcilerinin üçte birinin talebi üzerine herhangi bir zamanda toplanır.

2. Danışma Komitesi toplantısı yeter sayısı, Taraf temsilcilerinin salt çoğunluğudur.

3. Danışma Komitesi, her toplantı sonunda, yaptığı çalışmalar ve Sözleşmenin işleyişi hakkında Avrupa Konseyi Bakanlar Komitesine bir rapor sunar.

4. İşbu Sözleşme hükümlerine tabi olmak üzere Danışma Komitesi iç tüzüğünü kendisi düzenler.

Bölüm VI - Değişiklikler

Madde 21 Değişiklikler

1. Taraflardan biri, Avrupa Konseyi Bakanlar Komitesi veya Danışma Komitesi işbu Sözleşmede değişiklik yapılmasını önerebilir.

2. Her değişiklik önerisi, Avrupa konseyi Genel Sekreteri tarafından, Avrupa Konseyi üyesi Devletlere ve 23. madde hükümleri uyarınca Sözleşmeye katılan veya katılmaya çağrılan üye olmayan her devlete bildirilir.

3. Taraflardan biri veya Bakanlar Komitesi tarafından yapılan her değişiklik önerisi, Bakanlar Komitesine değişiklik hakkında görüş sunacak olan Danışma Komitesine bildirilir.

4. Bakanlar Komitesi, teklif edilen değişikliği ve Danışma Komitesi tarafından sunulabilecek her türlü görüşü dikkate alarak söz konusu değişikliği kabul edebilir.

5. Bakanlar Komitesi tarafından bu maddenin 4. fıkrasına göre kabul edilen her türlü değişiklik metni, kabul için Taraflara iletilir.

6 İşbu Maddenin 4. fıkrası uyarınca kabul edilen herhangi bir değişiklik, tüm Tarafların bununu kabul ettiklerini Genel Sekretere bildirmelerini izleyen otuzuncu günde yürürlüğe girer.

Bölüm XI - Son hükümler

Madde 22 Yürürlüğe girme

1 İşbu Sözleşme Avrupa Konseyi üyesi devletlerin imzasına açıktır. Onay, kabul ya da uygun bulmaya tabidir. Onay, kabul ya da uygun bulma belgeleri, Avrupa Konseyi Genel Sekreterine teslim edilir.

2 Bu Sözleşme, en az beş Avrupa Konseyi üye devletinin önceki fıkranın hükümlerine göre Sözleşmeyle bağlı olma yönündeki muvafakatlerini ifade ettikleri tarihten itibaren üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüğe girer.

3. Daha sonra Sözleşme ile bağlı olmak istediğini beyan eden herhangi bir üye devlet bakımından Sözleşme; onay, kabul ya da uygun bulma belgesini teslim etme tarihinden itibaren üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüğe girer.

Madde 23 Üye olmayan devletlerin katılımı

1. İşbu Sözleşmenin yürürlüğe girmesinden sonra, Avrupa Konseyi Bakanlar Komitesi, Avrupa Konseyi Statüsünün 20. maddesinin d. fıkrasında öngörülen çoğunlukla ve komiteye katılına hakkına sahip Taraf Devlet temsilcilerinin oybirliğiyle Avrupa Konseyine üye olmayan herhangi bir Devleti işbu Sözleşmeye katılmaya davet edebilir.

2. Katılan her Devlet için Sözleşme, katılına belgesinin Avrupa Konseyi Genel Sekreterine tevdi edildiği tarihten sonraki üç aylık dönemin bitimini izleyen ayın ilk günü yürürlüğe girer.

Madde 24 Ülkesel hükümler

1. Herhangi bir Devlet, imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgelerini tevdi ederken, Sözleşmenin uygulanacağı ülkeyi veya ülkeleri belirtebilir.

2. Herhangi bir Devlet, daha sonraki bir tarihte Avrupa Konseyi Genel Sekreterine muhatap bir bildirimle, işbu Sözleşmenin uygulama alanını, bildirimde belirtilen başka herhangi bir ülkeye teşmil edebilir. Sözleşme, sözkonusu ülke bakımından, söz konusu beyanın Genel Sekreter tarafından alınına tarihinden itibaren üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüğe girer.

3. Önceki iki fıkra uyarınca yapılan herhangi bildirim, sözkonusu bildirimde belirtilen herhangi bir ülke bakımından Avrupa Konseyi Genel Sekreterine muhatap bir bildirim ile geri çekilebilir. Sözkonusu geri çekme, sözkonusu bildirimin Genel Sekreter tarafından alınma tarihinden itibaren altı aylık sürenin sona ermesini takip eden ayın ilk günü geçerlilik kazanır.

Madde 25 Çekinceler

İşbu Sözleşme hükümlerine hiçbir çekince konulamaz.

Madde 26 Fesih

1. Taraflardan herhangi biri, herhangi bir zamanda Avrupa Konseyi Genel Sekreterine muhatap bir bildirim yoluyla bu Sözleşmeyi feshedebilir.

2. Söz konusu fesih, söz konusu bildirimin Genel Sekreter tarafından alınma tarihinden itibaren altı aylık sürenin sona ermesini takip eden ayın ilk günü geçerlilik kazanır.

Madde 27 Bildirimler

Avrupa Konseyi Genel Sekreteri Konsey üyesi Devletlere ve bu Sözleşmeye katılan her Devlete aşağıdakileri bildirecektir:

a. her imzayı;

b. tevdi edilen her onay, kabul, uygun bulma veya taraf olma belgesini;

c. Madde 22, 23 ve 24 uyarınca her yürürlüğe giriş tarihini;

d. bu Sözleşme ile ilgili diğer her tür belge, bildirim ya da muhaberatı.

Keyfiyeti tevsiken, usulüne uygun olarak yetkilendirilmiş Sözleşmeyi imzalamışlardır.

Strazburg'da 28 Ocak 1981 tarihinde İngilizce ve Fransızca dillerinde ve her iki metin eşit derecede geçerli olacak şekilde, Avrupa Konseyi arşivlerinde saklanmak üzere tek nüsha olarak imzalanmıştır. Avrupa Konseyi Genel Sekreteri, her bir Avrupa Konseyi üye Devletine ve Sözleşmeye taraf olmaya davet edilen her Devlete onaylı nüshalarını gönderecektir.

181 NO'LU EK PROTOKOL - 2001 (108 SAYILI SÖZLEŞMENİN EKİ)

Düzenlemenin orijinal ismi: *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*
Düzenlemenin künyesi: *European Treaty Series No. 181 / 08.11.2001*
Düzenlemenin orijinal metni için:
http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626
(Son erişim tarihi: 18.03.2016)
Düzenlemenin Türkiye künyesi: *Türkiye, 08.11.2001 tarihinde sözleşmeyi imzalamış, ancak sözleşme Kanun'la uygun bulunmamıştır.*

Preamble

The Parties to this additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature in Strasbourg on 28 January 1981 (hereafter referred to as "the Convention");

Convinced that supervisory authorities, exercising their functions in complete independence, are an element of the effective protection of individuals with regard to the processing of personal data;

Considering the importance of the flow of information between peoples;

Considering that, with the increase in exchanges of personal data across national borders, it is necessary to ensure the effective protection of human rights and fundamental freedoms, and in particular the right to privacy, in relation to such exchanges of personal data,

Have agreed as follows:

Article 1 – Supervisory authorities

1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated inChapters II and III of the Convention and in this Protocol.

2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

5. In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

Article 2 –Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention

1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data :

a. if domestic law provides for it because of :

–specific interests of the data subject, or

–legitimate prevailing interests, especially important public interests, or

b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.

Article 3 – Final provisions

1. The provisions of Articles 1 and 2 of this Protocol shall be regarded by the Parties as additional articles to the Convention and all the provisions of the Convention shall apply accordingly.

2. This Protocol shall be open for signature by States Signatories to the Convention. After acceding to the Convention under the conditions provided by it, the European Communities may sign this Protocol. This Protocol is subject to ratification, acceptance or approval. A Signatory to this Protocol may not ratify, accept or approve it unless it has previously or simultaneously ratified, accepted or approved the Convention or has acceded to it. Instruments of ratification, acceptance or approval of this Protocol shall be deposited with the Secretary General of the Council of Europe.

3. a. This Protocol shall enter into force on the first day of the month following the expiry of a period of three months after the date on which five of its Signatories have expressed their consent to be bound by the Protocol in accordance with the provisions of paragraph 2 of Article 3.

b. In respect of any Signatory to this Protocol which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the fir

İNSAN HAKLARI AVRUPA SÖZLEŞMESİNİN İLGİLİ HÜKÜMLERİ (1953)

Düzenlemenin orijinal ismi: *Convention for the Protection of Human Rights and Fundamental Freedoms ("European Convention on Human Rights, ECHR")*
Düzenlemenin künyesi: *CETS No.005, İmzaya açılma tarihi 04.11.1950 / Yürürlük tarihi 03.09.1953*
Düzenlemenin orijinal metni için:
http://www.echr.coe.int/Documents/Convention_ENG.pdf (Son erişim tarihi: 18.03.2016)
Düzenlemenin Türkiye künyesi: *Türkiye Sözleşmeyi, 04.11.1950 tarihinde imzalamış ve 10.03.1954 tarih ve 6366 sayılı Kanun ile onaylamıştır.*
Düzenlemenin Türkçe metni için:
http://www.echr.coe.int/Documents/Convention_TUR.pdf (Son erişim tarihi: 18.03.2016)

Madde 8 – Özel hayata ve aile hayatına saygı hakkı

1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

§ AVRUPA BİRLİĞİ DÜZENLEMELERİ

95/46/EC SAYILI KİŞİSEL VERİLERİN İŞLENMESİ VE SERBEST DOLAŞIMI BAKIMINDAN BİREYLERİN KORUNMASINA İLİŞKİN AVRUPA PARLAMENTOSU VE AVRUPA KONSEYİ DİREKTİFİ

Düzenlemenin orijinal ismi: *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*
Düzenlemenin künyesi: *31995L0046 EU Official Journal L 281 , 23/11/1995 P. 0031 – 0050*
Düzenlemenin orijinal metni için:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046
(Son erişim tarihi: 16.04.2016)

BAŞLANGIÇ

AVRUPA PARLAMENTOSU VE AVRUPA BİRLİĞİ KONSEYİ,

Avrupa Topluluğunu Kuran Anlaşmayı ve özellikle ilgili 100a maddesini göz önünde bulundurarak,

Komisyonun teklifini[1] göz önünde bulundurarak,

Ekonomik ve Sosyal Komite'nin[2] görüşünü göz önünde bulundurarak,

Anlaşmanın 189b maddesinde ortaya koyulan prosedür uyarınca hareket ederek[3] aşağıda sıralanan nedenlerden dolayı:

(1) Topluluk'un amaçları, Avrupa Birliği Anlaşması tarafından tadil edildiği, Anlaşmada öngörüldüğü şekilde; İnsan Hakları ve Temel Özgürlüklerin Korunması Hakkındaki Avrupa Sözleşmesi'nde ve Üye Devletler'in anayasaları ve yasalarında tanınan temel haklar üzerinden demokrasiyi geliştirerek ve barış ve özgürlüğü koruyup güçlendirerek halklarının yaşama koşullarının sürekli iyileştirilmesini teşvik

[1] OJ No: C 277, 5.11.1990 syf:3 ve OJ No: C 311, 27.11.1992, syf:3

[2] OJ No: C 159, 17.6.1991, syf:38

[3] 15 Haziran 1995 tarihli Avrupa Parlamentosu Kararı (OJ No: C 166, 3.7.1995) ve 20 Şubat 1995 tarihli Komisyon ortak görüşü (OJ No: C 93, 13.4.1995, syf:1) ; 2 Eylül 1993'de onaylanan (OJ No: C 342, 20.12.1993, syf:30) 11 Mart 1992 tarihli Avrupa Parlamentosu Görüşü (OJ No: C 94, 13.4.1992, syf:198)

ederek, Avrupa'yı bölen engelleri gidermek için ortak eylemle ekonomik ve sosyal ilerlemeyi sağlayarak, Topluluk'a mensup Devletlerarasında daha yakın ilişkileri teşvik etmeyi içerir;

(2) Veri işleme sistemleri insana hizmet etmek üzere tasarlanır ve böyle olmalıdır; gerçek kişilerin milliyetine veya ikametgahlarına bakmaksızın, başta kişisel mahremiyet olmak üzere, temel haklarını ve özgürlüklerini korumalıdır ve bireylerin ekonomik ve sosyal ilerlemesine, refahına ve ticari genişlemeye katkıda bulunmalıdır;

(3) Malların, kişilerin, servislerin ve sermayenin serbest dolaşımının sağlanması hakkındaki Anlaşmanın 7a maddesi uyarınca bir iç pazarın kurulması ve işletilmesi;yalnızca kişisel verilerin bir Üye Devletten diğerine serbestçe akabilmesini değil, aynı zamanda bireylerin temel haklarının güvenceye alınmasını gerektirir;

(4) Topluluk'a, ekonomik ve sosyal faaliyetin çeşitli alanlarında kişisel verilerin işlenmesine dönük olarak artan sıklıkta başvuru yapılmaktadır; bilgi teknolojisinde sağlanan ilerlemeler, bu tür verilerin işlenmesini ve değişimini önemli ölçüde kolaylaştırmaktadır;

(5) Anlaşmanın 7a maddesinin anlamı kapsamında iç pazarın kurulması ve işlemesinden kaynaklanan ekonomik ve sosyal entegrasyon; Üye Devletlerde ekonomik ve sosyal faaliyete özel veya kamu sıfatıyla katılan herkes arasında kişisel verilerin sınır ötesi akışında zorunlu olarak önemli bir artışa yol açacaktır. Farklı Üye Devletlerdeki teşebbüsler arasında kişisel verilerin alışverişi artmaya başlamıştır; çeşitli Üye Devletlerdeki ulusal makamlardan, iç pazarın sınırları dikkate almaksızın diğer bir Üye Devletteki bir makam adına görevlerini yerine getirebilmek veya görevlerini yapabilmek hususunda topluluk hukukuna binaen, kişisel verileri takas etmesi ve iş birliği yapması istenmektedir;

(6) Üstelik Toplulukta yeni haberleşme ağlarının eşgüdümlü uygulanması ve bilimsel ve teknik işbirliğindeki artış, kişisel verilerin sınır ötesi akışını gerektirmekte ve kolaylaştırmaktadır;

(7) Üye Devletlerde uygulanan kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere bireylerin hakları ve özgürlüklerinin korunma seviyesindeki farklılıklar, bir Üye Devlet toprağından diğer Üye Devlete bu tür verilerin iletilmesini engelleyebilir; bu nedenle bu fark, Topluluk seviyesindeki birtakım ekonomik faaliyetlerin takibi için bir engel oluşturabilir, rekabeti bozabilir ve Topluluk hukuku kapsamında makamların sorumluluklarını yerini getirmesini engelleyebilir; koruma seviyesindeki bu fark, çok çeşitli ulusal kanunlar, yönetmelikler ve idari hükümlerin varlığından dolayıdır;

(8) Kişisel verilerin akışındaki engelleri kaldırmak için, bireylerin hak ve özgürlüklerinin korunma seviyesi bu tür verilerin işlenmesine ilişkin olarak tüm Üye Devletlerde eşit olmalıdır; bu amaç iç pazar için hayatidir ancak özellikle Anlaşmanın 7a maddesinde belirtilen iç pazar amacına uyan tutarlı bir şekilde kişisel verilerin sınır ötesi akışının düzenlenmesini temin etmek hususunda Üye Devletlerdeki ilgili kanunlar arasında mevcut uyuşmazlıkların ölçeği göz önüne alındığında bu, Üye Devletler tarafından tek başına başarılamaz; bu yüzden bu kanunları yaklaştırmak için Topluluk eylemine gerek duyulmaktadır;

(9) Ulusal kanunların yakınlaştırılmasından kaynaklanan eşdeğer koruma dikkate alındığında, Üye Devletler, özellikle kişisel gizlilik hakkı başta olmak üzere, bireylerin özgürlükleri ve haklarının korunması gerekçesiyle, kişisel verilerin aralarında serbest dolaşımını artık engelleyemeyeceklerdir; Üye Devletlere, Direktifin uygulanması bağlamında, iş ve sosyal ortaklar tarafından da yerine getirilebilecek bir manevra

alanı bırakılacaktır; bu nedenle Üye Devletler veri işlemenin yasallığını yöneten genel koşulları, kendi ulusal yasalarına koyabileceklerdir. Üye Devletler bu şekilde kendi mevzuatlarıyla güncel olarak sağlanan korumayı geliştirmeye çalışacaklardır; bu manevra alanının limitleri dâhilinde ve Topluluk kanuna uygun olarak, Direktifin uygulanmasında eşitsizlikler ortaya çıkabilir ve bu, Topluluğun yanı sıra bir Üye Devlet bünyesinde verilerin dolaşımı etkileyebilir;

(10) Kişisel verilerin işlenmesi hakkındaki ulusal kanunların amacı, başta kişisel mahremiyet hakkı olmak üzere, hem Topluluk kanununun genel esaslarında, hem de İnsan Hakları ve Temel Özgürlüklerini Koruma hakkındaki Avrupa Sözleşmesinin 8. maddesinde tanınan temel hakları ve özgürlükleri korumaktır; bu nedenle, bu kanunların yakınlaştırılması, sağladıkları korumanın azalmasına yol açmamalı aksine, Topluluk içinde yüksek seviyeli bir korumanın sağlanması için çabalamalıdır;

(11) Kişisel mahremiyet başta olmak üzere bireylerin haklarının ve özgürlüklerinin korunması hakkında bu Direktifte belirtilen esaslar, Kişisel Verilerin Otomatik İşlenmesine İlişkin Bireylerin Korunması Hakkındaki 28 Ocak 1981 tarihli Avrupa Konseyi Sözleşmesinde belirtilenleri güçlendirir ve genişletir;

(12) Koruma esasları, faaliyetleri Topluluk hukukunca yönetilen herhangi bir kişinin kişisel verilerinin tüm işlenmesine uygulanmalıdır; adres kayıtlarını tutma ve yazışma gibi özellikle şahsi veya ailevi olan aktiviteler esnasında, bir gerçek kişinin gerçekleştirdiği veri işleme, hariç tutulmalıdır;

(13) Avrupa Topluluğunu Kuran Anlaşmanın 100a maddesi veya madde 56 (2), madde 57 kapsamında Üye Devletler üzerine düşen yükümlülükler saklı kalmak üzere; kamu güvenliği, savunma, devlet güvenliğine dair Avrupa Birliği Anlaşmasının V ve VI. Başlığında atıfta bulunulan faaliyetler ile ceza kanunları alanındaki Devlet faaliyetleri; Topluluk hukuku kapsamında değildir; Devletin güvenlik konularıyla ilişkili olduğunda, devletin ekonomik refahını güvenceye almak için gerekli olan kişisel verilerin işlenmesi, bu Direktifin kapsamında değildir;

(14) Gerçek kişilere ilişkin ses ve görüntü verilerini yakalamak, iletmek, değiştirmek, kaydetmek, saklamak veya nakletmek için kullanılan teknolojilerin, bilgi toplumu çerçevesinde devam eden gelişmelerinin önemi dikkate alındığında, bu Direktif bu tür verileri gerektiren işlemeye uygulanmalıdır;

(15) Bu tür verilerin işlenmesi; söz konusu kişisel verilere kolay erişime izin vermek için, yalnızca otomatik olursa veya işlenen veriler, bireylere ilişkin özel kriterlere göre yapılandırılan bir dosyalama sistemi içine alınırsa veya alınması planlanırsa, bu Direktif kapsamındadır;

(16) Video gözetim durumlarındaki gibi, ses ve görüntü verilerinin işlenmesi; ceza hukuku alanına ilişkin Devlet faaliyetleri esnasında veya ulusal güvenlik, savunma kamu güvenliği amacıyla veya Topluluk hukuku kapsamına girmeyen diğer faaliyetler için yürütülürse bu Direktif kapsamına girmez;

(17) Başta görsel işitsel alan olmak üzere, ilgili edebi ve sanatsal ifade amaçlarının yanı sıra gazetecilik amaçları için ses ve görüntü verilerinin işlenmesinde; Direktifin esasları, madde 9'da öngörülen hükümlere göre, sınırlı bir şekilde uygulanacaktır;

(18) Bireylerin, bu Direktif kapsamında sağlanan korumadan yoksun kalmamalarını sağlamak için, Topluluktaki herhangi bir kişisel veri işlenmesi, Üye Devletler'den birinin kanununa uygun olarak yerine getirilmelidir; bu bağlamda, bir Üye Devlette yerleşik bir denetleyicinin sorumluluğu altında yapılan işlem, o Devletin kanununca yönetilmelidir;

(19) Bir Üye Devletin sınırları içindeki kuruluş, istikrarlı düzenlemeler aracılığıyla faaliyetin etkin ve reel olarak gerçekleştirilmesini sağlar. İster bir tüzel kişiliğin şubesi veya bağlı kuruluşu olsun bu tür kuruluşun yasal biçimi; bu bakımdan belirleyici bir faktör değildir; özellikle bağlı kuruluşlar aracılığıyla çeşitli Üye Devletlerin topraklarında tek bir denetleyici kuruluş kurulursa, ulusal kuralların boşluklarından yaralanmayı önlemek için, denetleyici kuruluşların her birinin, faaliyetlerine uygulanan ulusal kanunun emrettiği yükümlülükleri yerine getirmesi sağlanmalıdır;

(20) Verilerin işlenmesinin üçüncü bir ülkede kurulan bir tüzel kişilik tarafından yapılması, bu Direktifte sağlanan bireylerin korunma biçimine engel olmamalıdır; bu durumlarda, işleme, kullanılan yöntemlerin bulunduğu Üye Devlet kanununca yönetilmelidir ve bu Direktifte sağlanan hakların, uygulamada gözetilmesini sağlayacak garantiler olmalıdır;

(21) Bu Direktif, ülkesellik ilkeleri saklı kalmak üzere ceza konularına uygulanır;

(22) Üye Devletler, işlemenin yasallığına dair genel koşulları, çıkardıkları yasalarda veya bu Direktif kapsamındaki tedbirleri yürürlüğe koyduklarında, daha hassas olarak tanımlayacaklardır; madde 7 ve 8 ile bağlantılı olarak özellikle madde 5, genel kurallardan bağımsız olarak Üye Devletlere, madde 8'in kapsadığı çeşitli veri kategorileri için ve belirli sektörler için, özel işleme koşulları koymaya izin verir.

(23) Üye Devletler, hem kişisel verilerin işlenmesi hususunda bireylerin korunması hakkındaki genel kanunlar, hem de örneğin istatistik enstitülerine ilişkin olanlar gibi sektörel kanunlar yoluyla bireylerin korunmasını uygulamayı temin etmek üzere yetkilendirilmişlerdir;

(24) Kendilerini ilgilendiren verileri işlemeye dair tüzel kişilerin korunmasına ilişkin mevzuat, bu Direktiften etkilenmez;

(25) Korumanın esasları; bir taraftan, başta işlemenin yürütülebileceği koşullar ve denetleme makamına bildirim, teknik güvenlik ve veri kalitesi olmak üzere işlemeden sorumlu diğer kuruluşlar veya kişiler, kamu makamları, işletmeler, temsilciler üzerine yüklenen yükümlülüklere ve diğer taraftan, bireylere verilen haklara, işlemenin konusu olan verilere, işlemenin yapıldığını bildirime, verileri danışmaya, düzeltme talep etmeye ve hatta bazı koşullarda işlemeye itiraza yansıtılmalıdır;

(26) Koruma esasları, tespit edilmiş veya tespit edilebilir bir kişiye ilişkin herhangi bir bilgiye uygulanmalıdır; bir kişinin tespit edilebilir olup olmadığını belirlemek için, adı geçen şahsı tespit etmek için herhangi bir diğer kişi tarafından veya denetleyici tarafından kullanılabilecek makul tüm araçlar dikkate alınmalıdır; koruma esasları, veri öznesinin artık tespit edilebilir olmadığı bir biçimde anonimleşmiş verilere uygulanmayacaktır; madde 27'nin anlamı dahilindeki davranış kuralları, verilerin anonimleşebilmesine ve veri öznesinin tespitinin artık mümkün olmadığı bir biçimde alıkonma biçimlerine dair rehberlik sağlamak için yararlı bir araç olabilir;

(27) Bireylerin korunması, manuel işlemenin yanı sıra verilerin otomatik işlenmesinde de uygulanmalıdır; bu korumanın kapsamı kullanılan tekniklere bağlı olarak geçerli olmamalıdır, aksi takdirde, bu ciddi bir kanun boşluklarından yararlanma riski yaratacaktır; yine de manuel işlemeye dair bu Direktif yapılandırılmamış dosyaları değil yalnızca dosyalama sistemlerini kapsar, özellikle bir dosyalama sisteminin içeriği, kişisel verilere kolay erişime olanak veren bireylere ilişkin özel kriterlere göre yapılandırılmalıdır; madde 2 (c)deki tanım doğrultusunda, kişisel verilerin yapılandırılmış bir

dizisinin bileşenlerini belirlemek için farklı kriterler ve bu tür bir veri dizisine erişimi yöneten farklı kriterler, her bir Üye Devlet tarafından belirlenebilir; özel kriterlere göre yapılandırılmamış kapak sayfalarının yanı sıra dosyalar veya dosya dizileri, hiçbir koşul altında bu Direktifin kapsamına girmeyecektir;

(28) Kişisel verilerin işlenmesi, ilgili bireyler için yasal ve adil olmalıdır; özellikle veriler uygun, ilgili olmalıdır ve işlendikleri amacı aşmamalıdır; bu tür amaçlar açık ve meşru olmalı ve verilerin toplanma zamanında belirlenmelidir; toplama sonrasındaki işleme amaçları, başlangıçta belirtilen amaçlarla uyumsuz olmamalıdır;

(29) Tarihsel, istatistiksel veya bilimsel amaçlarla kişisel verilerin ayrıca işlenmesi, Üye Devletlerin uygun korunma önlemleri sağlaması koşuluyla önceden toplanmış verilerin amaçlarıyla uyumsuz olarak kabul edilmez, bu korunma önlemleri özellikle, herhangi bir özel bireye dair tedbirlerin veya kararların desteklenmesinde verilerin kullanımınına imkan vermemelidir;

(30) Kişisel verilerin işlenmesi, ayrıca veri öznesinin haklarının ve özgürlüklerinin çiğnenmemesi koşuluyla, yasal olması amacıyla, veri öznesinin rızasıyla yürütülmelidir veya veri öznesi hakkında bağlayıcı bir sözleşmenin yerine getirilmesi veya sonuçlandırılması için veya gerçek veya tüzel bir kişinin meşru menfaati için veya resmi otoritenin uygulanması için veya kamu menfaatine yürütülen bir görevin yerine getirilmesi için gerekli olmalıdır; özellikle etkin rekabeti garanti ederken, ilgili menfaatler arasında bir denge sağlamak için, Üye Devletler, şirketlerin veya diğer kuruluşların olağan meşru iş faaliyetleri bağlamında kişisel verilerin kullanılabilme veya üçüncü bir şahsa açıklanma koşullarını belirleyebilirler; benzer şekilde Üye Devletler, örneğin nedenlerini belirtmeksizin ve bedelsiz olarak, hakkındaki verilerin işlenmesine itiraz etmek için bir veri öznesine izin veren hükümlere tabi olan ister siyasi yapıdaki herhangi diğer bir dernek veya vakıf veya yardım kuruluşu tarafından isterse ticari olarak yürütülen pazarlama amaçları için, kişisel verilerin üçüncü bir şahsa açıklanabilme koşullarını belirtebilirler;

(31) Veri öznesinin yaşamı için asıl olan bir menfaati korumak için yapıldığında kişisel verilerin işlenmesi, aynı derecede yasal kabul edilmelidir;

(32) Kamu menfaatinde veya resmi otoritenin uygulamasında yürütülen bir görevi yerine getiren denetleyicinin, bir kamu idaresi veya kamu hukuku veya bir meslek örgütü gibi özel bir kanun tarafından yönetilen başka bir tüzel veya gerçek kişi mi olacağını belirlemek ulusal mevzuata kalmaktadır;

(33) Veri öznesi açık şekilde rıza göstermezse, temel özgürlükleri veya kişisel mahremiyeti ihlal eden yapıdaki veriler işlenmemelidir; ancak, temel özgürlüklerin yerine getirilmesine izin verecek amaçlar için, bazı derneklerin veya vakıfların meşru faaliyetleri esnasında veya mesleki gizlilik hakkındaki yasal bir yükümlülüğe tabi kişiler tarafından bu verilerin sağlık amaçları için kullanılması durumunda; bu yasaklamaya uymama durumu açıkça belirtilmelidir;

(34) Sağlık sigortası sistemindeki hizmetler ve yardımlar için talepleri belirtmede kullanılan prosedürlerin kalitesini ve maliyet etkinliğini temin etmek başta olmak üzere - kamu menfaati için önemli nedenlerle gerekçelendirildiğinde, önemli kamu menfaati gerekçesine dayanması durumunda; bilimsel araştırma ve hükümet istatistikleri halk sağlığı ve sosyal koruma gibi alanlarda, Üye Devletlerin verilerin hassas kategorilerini işleme yasağına uymamasına da izin verilmelidir; ancak bireylerin kişisel gizlilik ve

temel haklarını korumak hususunda özel ve uygun korunma önlemlerini sağlamak, Üye Devletlerin ödevidir;

(35) Ayrıca, resmi olarak tanınan dini derneklerle ilgili veya uluslararası kamu hukuku veya anayasa hukukunda öngörülen amaçları başarmak için resmi makamlar tarafından kişisel verilerin işlenmesi, kamu menfaatinin önemli gerekçeleri üzerine yürütülür;

(36) Belirli Üye Devletlerde, seçim faaliyetleri esnasında demokratik sistemin işlemesi, siyasi partilerin halkın siyasi görüşü hakkındaki verileri derlemesini gerektirir, uygun korunma önlemlerin sağlanması koşuluyla bu tür verilerin işlenmesine önemli kamu menfaati nedeniyle izin verilebilir;

(37) Başta görsel işitsel alan olmak üzere, sanatsal ifade, edebi amaçları için veya gazetecilik amaçları için kişisel verilerin işlenmesi; özellikle, İnsan Hakları ve Temel Özgürlüklerinin Korunması hakkındaki Avrupa Sözleşmesinin 10. maddesinde garanti edildiği gibi, özellikle bilgi alma ve verme hakkı ve bilgilendirme hakkıyla bireylerin temel haklarını uzlaştırmanın gerekli olması durumunda, bu Direktifin bazı hükümlerinin koşullarından muaf tutulmaya yetki vermelidir. Bu yüzden üye Devletler, denetleme makamının yetkisi ve üçüncü ülkelere verilerin aktarılması hakkındaki tedbirlere, veri işlemenin yasallığı hakkındaki genel tedbirlere dair temel haklar arasında denge sağlama amacı için gerekli muafiyetleri ve derogasyonları belirtmelidir;

(38) Verilerin işlenmesinin adil olması için, veri öznesi, işleme faaliyetinin varlığını öğrenecek konumda olmalıdır ve veriler ondan toplandığında, toplama koşullarını dikkate alan doğru ve tam bilgi verilmelidir;

(39) Bazı verilerin işlenmesi, denetleyicinin veri öznesinden doğrudan toplamadığı verileri gerektirir, ayrıca, veri öznesinden veriler toplandığı esnada, ifşa beklenmese bile, veriler üçüncü bir şahsa yasal olarak ifşa edilebilir; tüm bu durumlarda, veri öznesi, veriler kaydedildiğinde veya en geç veriler ilk kez bir üçüncü şahsa ifşa edildiğinde, bilgilendirilmelidir;

(40) Ancak, veri öznesinin önceden bilgili olması durumunda, bu yükümlülüğü uygulamak gereksizdir; ayrıca, açıklama veya kaydetme açık şekilde yasayla sağlanırsa veya veri öznesine bilgi sağlamanın imkansızlığı kanıtlanırsa veya işlemenin tarihsel, istatistiki veya bilimsel amaçlar için olması halinde gerekebilecek aşırı çabayı gerektirmesi halinde bu tür bir yükümlülük olmayacaktır; bu bakımdan, veri öznelerinin sayısı, verilerin yaşı ve kabul edilen herhangi dengeleyici tedbirler dikkate alınmalıdır;

(41) Her kişi, özellikle işlemenin yasallığını ve verilerin doğruluğunu onaylamak için işlenmekte olan ona ait verilere erişim hakkını kullanabilmelidir; aynı nedenlerle, her veri öznesi en azından madde 15 (1)de atıfta bulunulan otomatik kararlar durumunda, ona ilişkin verilerin otomatik işlenmesiyle ilgili mantığı bilme hakkına sahip olmalıdır; bu hak, başta yazılımı koruyan telif hakkını ve ticari sırları veya fikri mülkiyeti ters şekilde etkilememelidir; ancak bu düşünceler, veri öznesinin bilgilendirilmemesine yol açmamalıdır;

(42) Üye Devletler, veri öznesinin menfaati için veya diğerlerinin hak ve özgürlüklerini korumak için bilgiye erişim hakkını sınırlandırabilirler; örneğin, tıbbi verilere erişimin yalnızca bir sağlık uzmanı tarafından elde edilebileceğini belirtebilirler;

(43) Benzer şekilde denetleyicinin bazı yükümlülükleri ve bilgilendirme ve erişim hakları üzerindeki sınırlandırmalar; örneğin, düzenlenen mesleklerdeki etik ihlallerine dair kriminal soruşturmalar,

takibatlar ve davaların yanı sıra bir Üye Devlet veya Birliğin ulusal güvenlik, savunma, kamu güvenliği veya önemli ekonomik veya mali menfaatlerini güvence altına almanın gerektirdiği ölçüde Üye Devletler tarafından uygulanabilir; istisnalar ve sınırlamaların listesi, kamu güvenliği, ekonomik veya mali menfaatler ve suç önlemeye ilişkin en son söz edilen üç alanda gerekli yönetmelik veya izleme, denetim görevlerini içermelidir; bu üç alandaki görevlerin listelenmesi, Devlet güvenlik veya savunma nedenleri için sınırlamaları veya istisnaların meşruiyetini etkilemez;

(44) Üye Devletler, Topluluk hukuku gerekçesiyle, yukarıda atıfta bulunulan amaçların bazısını güvenceye almak için, verilerin kalitesi ve bireyleri bilgilendirme yükümlülüğü, erişim hakkına ilişkin bu Direktifin hükümlerine uymayabilir;

(45) Verilerin, gerçek veya tüzel bir kişinin meşru menfaatleri veya resmi otorite, kamu menfaati gerekçesiyle yasal olarak işlenebileceği durumlarda, herhangi bir veri öznesine, yine de kendisine ait herhangi bir verinin işlenmesine itiraz etmek için özel durumuna ilişkin meşru ve mecburi gerekçelerle izin verilmelidir; bununla birlikte Üye Devletler bunun aksine ulusal hüküm koyabilirler;

(46) Kişisel verilerin işlenmesine dair veri öznelerinin haklarının ve özgürlüklerinin korunması, hem, güvenliği sağlamak ve bu suretle herhangi bir yetkisiz işlemeyi önlemek için işlemenin kendi zamanında hem de işleme sisteminin tasarımı zamanında uygun teknik ve kurumsal tedbirlerin alınmasını gerektirir; bu tedbirlere denetleyicilerin uymasını sağlamak Üye Devletlerin ödevidir, bu tedbirler, korunacak verilerin yapısı ve işlemenin yapısındaki risklere ilişkin uygulamanın maliyetlerini ve durumunu dikkate alarak uygun güvenlik seviyesini sağlamalıdır;

(47) Tek amacı verilerin iletilmesi olan, kişisel verileri içeren bir mesajın bir iletişim aracıyla veya elektronik posta servisiyle iletilmesi durumunda, mesajda belirtilen kişisel verilere dair denetleyici; iletim servislerini sunan kişi yerine, mesajın çıktığı kişi olarak kabul edilecektir; bununla birlikte bu tür servisleri sunanlar, normal olarak, servisin çalışması için gerekli ek kişisel verilerin işlenmesi bakımından denetleyici olarak kabul edilecektir;

(48) Denetleme makamını bilgilendirmeye dönük prosedürler, faaliyetin, bu Direktif kapsamında alınan ulusal tedbirlere uygun olduğunu doğrulama amacı için, herhangi bir işleme faaliyetinin amaçlarının ve ana özelliklerinin açıklanmasını sağlamak üzere tasarlanmıştır;

(49) Uygun olmayan idari formalitelerden kaçınmak için, gerekli bildirim yükümlülüğünden muafiyetler; sınırlarını belirten bir Üye Devlet tarafından alınan bir tedbire uyumlu olması koşuluyla, işlemenin, veri öznelerinin haklarını ve özgürlüklerini olumsuz şekilde etkilemesinin mümkün olmadığı durumlarda, Üye Devlet tarafından koyulabilir; benzer şekilde muafiyet veya basitleştirme, denetleyici tarafından atanan bir kişinin yürütülen işlemenin veri öznelerinin haklarını ve özgürlüklerini olumsuz şekilde etkilemesinin olanaksız olmasını sağladığında, Üye Devletler tarafından koyulabilir; ister denetleyicinin bir çalışanı olsun veya olmasın bu tür bir veri koruma görevlisi tam bağımsızlık içinde işlevlerini yerine getirecek bir konumda olmalıdır;

(50) Muafiyet veya basitleştirme, meşru bir menfaati kanıtlayan bir kişi veya kamu tarafından danışmaya açma ve kamuya bilgi sağlamak için ulusal yasaya göre tek amacı kayıt tutma olan işleme faaliyetleri için öngörülebilir;

(51) Yine de bildirim yükümlülüğünden muafiyet veya basitleştirme denetleyiciyi bu Direktiften kaynaklanan diğer yükümlülüklerinin herhangi birisinden kurtarmayacaktır;

(52) Bu bağlamda, genel olarak yetkili makamlar tarafından *olaydan sonra* doğrulama yeterli bir tedbir olarak kabul edilmelidir;

(53) Ancak bazı işleme faaliyetlerinin, yeni teknolojilerin özel kullanımından dolayı veya bir sözleşme, hak, faydadan bireyleri kapsam dışı tutanlar gibi kendi amaçlarının kapsamı nedeniyle veri öznelerinin hak ve özgürlüklerine özel riskler yaratması olasıdır; Üye Devletler isterlerse mevzuatlarında bu tür riskleri belirtebilirler;

(54) Toplulukta yapılan tüm işlemeye ilişkin olarak; özel riskleri ortaya çıkaran miktar çok sınırlı olmalıdır; Üye Devletler denetleme makamı veya makamla işbirliği içindeki veri koruma görevlisinin, işlenmesinden önce kontrolün yapılmasını sağlamalıdır; bu ön kontrolün ardından, ulusal yasasına göre denetleme makamı, işlemeye dair bir görüş veya bir izin verebilir; bu tür kontrol; ya ulusal parlamentonun bir tedbirin ya da işlemenin yapısını tanımlayan ve uygun korunma önlemlerini belirten bir yasal tedbirin hazırlanmasıyla eş zamanlı olabilir;

(55) Denetleyici veri öznelerinin haklarını gözetmezse, ulusal mevzuat bir yargı yolu sağlamalıdır; yasadışı işlemenin bir sonucu olarak bir kişinin maruz kalabileceği herhangi bir zarar; mücbir sebepler durumunda ya da hatanın veri öznesinin tarafında olduğunu saptadığı durumlarda; zarardan sorumlu olmadığını kanıtlarsa yükümlülükten muaf tutulacak olan denetleyici tarafından tazmin edilmelidir; yaptırımlar, bu Direktif kapsamında alınan ulusal tedbirlere uymayanın kamu veya özel hukuk tarafından yönetilen herhangi bir kişi olduğuna bakılmaksızın uygulanmalıdır;

(56) Kişisel verilerin sınır ötesi dolaşımı, uluslararası ticaretin genişletilmesi için gereklidir, Bu Direktifle Topluluk bünyesinde garanti edilen bireylerin korunması; yeterli koruma seviyesini sağlayan üçüncü ülkelere kişisel verilerin aktarılmasını önlememelidir; üçüncü bir ülke tarafından sağlanan koruma seviyesinin yeterliliği, transfer işlemleri veya transfer işlemini çevreleyen tüm koşulların ışığında değerlendirilmelidir;

(57) Diğer taraftan yeterli ve elverişli koruma seviyesini sağlamayan üçüncü bir ülkeye, kişisel verilerin transferi yasaklanmalıdır;

(58) Transferin, yasayla belirlenen bir kayıttan ve meşru menfaate sahip kamu veya kişiler tarafından danışma için yapıldığı veya örneğin, sosyal güvenlik konularında yetkili servisler arasında veya gümrük veya vergi idareleri arasında verilerin uluslararası transferi durumunda, önemli kamu menfaati korumasının bunu gerektirdiği bir sözleşme veya yasal hak talebine ilişkin transferin gerektiği, veri öznesinin rızasını verdiği bazı durumlarda bu yasaktan muafiyet için önlemler alınmalıdır; bu tür bir transferin kayıttaki mevcut tüm veri kategorilerini veya verilerin tümünü gerektirmediği durumlarda ve kayıt, meşru bir menfaate sahip kişiler tarafından danışılma içinse, transfer yalnızca bu kişilerin talebi üzerine veya bunlar alıcı olacaklarsa yapılmalıdır;

(59) Denetleyicinin, uygun korunma önlemleri sunduğu durumlarda, üçüncü bir ülkede koruma olmayışını tazmin etmek için özel önlemler alınmalıdır; ayrıca Topluluk ve bu tür üçüncü ülkeler arasındaki müzakere prosedürleri için önlem alınmalıdır;

(60) Herhangi bir durumda, üçüncü ülkelere transferler, bu Direktif ve özellikle ilgili 8. maddesi uyarınca, yalnızca Üye Devletler tarafından kabul edilen hükümlere tam uygun şekilde gerçekleştirilebilir;

(61) Üye Devletler ve Komisyon, kendi ilgili yetki alanları içinde, uygulanması için benimsenen ulusal hükümleri gözeterek ve bazı sektörlerde yerine getirilen işlemenin özel karakteristiklerini göz önüne alarak, bu Direktifin uygulanmasını kolaylaştırmak hususunda, davranış kurallarını düzenlemeleri için ticari birlikleri ve ilgili diğer temsilci kuruluşları teşvik etmelidir;

(62) Denetim makamına ilişkin Üye Devletlerdeki tam bağımsız olarak işlevlerini yerine getiren kuruluşlar; kişisel verilerin işlenmesine dair bireylerin korunmasında, zorunlu bir bileşendir;

(63) Bu tür makamlar, özellikle yasal takibata kalkışma yetkisi ve bireylerden şikayet durumlarında inceleme ve müdahale yetkileri dahil olmak üzere kendi görevlerini yerine getirmek için gerekli araçlara sahip olmalıdır; bu tür makamlar, kendi yetki alanlarındaki Üye Devletlerde; işlemenin şeffaflığını sağlamak için yardımcı olmalıdırlar;

(64) Farklı Üye Devletlerdeki makamlar, Avrupa Birliği çapında, koruma kurallarının uygun şekilde gözetilmesini sağlamak için kendi görevlerini yerine getirmede birbirlerini desteklemeye ihtiyaç duyacaklardır;

(65) Topluluk düzeyinde, kişisel verilerin işlenmesine dair Bireylerin Korunması hakkında bir Çalışma Grubu kurulmalıdır ve işlevlerini yerine getirmede tamamen bağımsız olmalıdır; özel yapılarını dikkate alarak, Komisyona tavsiyelerde bulunmalıdır ve özellikle bu Direktif uyarınca kabul edilen ulusal kuralların homojen uygulanmasına katkı sağlamalıdır;

(66) Bu direktif, üçüncü ülkelere verilerin transferine ilişkin olarak, 87/373/EEC4 sayılı Konsey kararında belirtilen şekilde bir prosedürün tesisini ve Komisyon üzerindeki uygulama yetkilerinin verilmesini gerektirir5;

(67) AT Anlaşmasının madde 189 b'sinde öngörülen prosedüre uygun olarak kabul edilen eylemler için tedbirleri uygulamaya dair, Avrupa Parlamentosu, Konsey ve Komisyon arasında geçici bir anlaşma üzerine mutabakata 20 Aralık 1994 tarihinde erişilmiştir;

(68) Bu Direktifte düzenlenen kişisel verilerin işlenmesine dair, kişisel mahremiyet hakkı başta olmak üzere; bireylerin hak ve özgürlüklerinin korunmasına dair prensiplere; özellikle, bu prensiplere dayalı özel kurallarla ilgili belirli sektörlere göre, ilave yapılabilir veya daha açık şekilde anlatılabilir;

(69) Üye Devletlere, önceden devam eden tüm işleme faaliyetlerine, yeni ulusal kuralları kademeli şekilde uygulamak için, bu Direktifin yerini alan ulusal tedbirlerin uygulamaya girdiği yıldan itibaren üç yılı geçemeyen bir süre verilmelidir; maliyet etkin uygulanmasını kolaylaştırmak için, Direktif hükümlerinin bazısıyla mevcut manuel dosyalama sistemlerinin uyumunu sağlamak üzere, bu Direktifin kabul edilme tarihinden 12 yıl sonra biten başka bir süre Üye Devletlere verilecektir; bu tür dosyalama sistemlerinde bulunan veriler bu genişletilmiş geçiş dönemi esnasında manuel olarak işlenir. Bu sistemler, bu işleme sırasındaki hükümlerle uyumlu hale getirilmelidir;

(70) Bu hükümlerin yürürlüğe girmesinden önce bildirilen rıza ve ücrete dayalı sonuçlandırılan bir sözleşmenin yerine getirilmesinde gerekli herhangi bir hassas veri için, bu Direktif uyarınca alınan ulusal

hükümler yürürlüğe girdikten sonra, veri öznesinin sürece devam etmesi için denetleyiciye yine izin vermesine gerek yoktur;

(71) Bu tür düzenleme, kişisel verilerin işlenmesine dair bireylerin korunmasını ilgilendirmediğinde, Bu Direktif, ülkede oturan tüketicilere yönelik pazarlama faaliyetlerini düzenleyen bir üye Devlet yönteminin yerini almaz;

(72) Bu Direktif, bu Direktifte düzenlenen prensipler uygulandığında, dikkate alınması gereken resmi belgelere kamu erişim esaslarına olanak sağlar;

BU DİREKTİFİ KABUL ETMİŞTİR:

BÖLÜM I
GENEL HÜKÜMLER

Madde 1 Direktifin Amacı

(1) Bu Direktife uygun olarak, Üye Devletler, kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini koruyacaktır;

(2) Üye Devletler 1. paragraf kapsamında sağlanan korumayla bağlantılı nedenler için Üye Devletler arasında kişisel verilerin akışını yasaklamayacak ya da engellemeyeceklerdir;

Madde 2 Tanımlar

Bu Direktifin amacı için:

a. "kişisel veri" fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye ("veri öznesi) ilişkin herhangi bir bilgiyi kastedecektir;
b. "kişisel verilerin işlenmesi (işleme)", silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletmeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisini kastedecektir;
c. "kişisel veri dosyalama sistemi (dosyalama sistemi)" ister merkezi ister merkezi olmayan ya da bir işlevsel veya coğrafi tabana dağıtılmış özel kriterlere göre erişilebilir olan herhangi bir yapılandırılmış kişisel veri dizisini kastedecektir;
d. "denetleyici", kişisel verilerin işlenme araçlarını ve amaçlarını tek başına ya da diğerleriyle ortaklaşa belirleyen gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya başka bir kuruluşu kastedecektir; işleme amaçları ve araçları ulusal veya Topluluk hukuku veya yönetmelikleriyle belirlendiğinde, denetleyici veya atanması için özel kriterler, ulusal veya topluluk hukukuyla belirlenebilir;
e. "işleyici", denetleyici adına kişisel verileri işleyen bir gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya diğer bir kuruluşu kastedecektir;
f. "üçüncü şahıs", veri işlemek için yetkilendirilen işleyici veya denetleyicinin doğrudan yetkisi altındaki kişiler ve işleyici, denetleyici,veri öznesi dışındaki herhangi bir gerçek veya tüzel kişi, kamu makamını, devlet dairesini veya başka bir kuruluşu kastedecektir;
g. "alıcı", ister bir üçüncü şahıs olsun ya da olmasın, verilerin açıklandığı bir gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya başka bir kuruluşu kastedecektir; ancak, özel bir soruşturma çerçevesinde verileri alan makamlar alıcı olarak kabul edilmeyecektir;
h. "veri öznesinin rızası", kendisine dair kişisel verilerin işlenmesi için veri öznesinin kabulüne işaret eden, özgürce ve bilgilendirilme yapıldıktan sonra alınan rızayı kastedecektir.

Madde 3 Kapsam

(1) Bu Direktif, bir dosyalama sisteminin parçasını oluşturması istenen veya bir dosyalama sisteminin parçasını oluşturan kişisel verilerin otomatik araçlar dışında işlenmesine ve kısmen veya tamamen otomatik araçlarla kişisel verilerin işlenmesine uygulanacaktır.

(2) Bu Direktif, kişisel verilerin işlenmesine uygulanmayacaktır:

ceza hukuku alanındaki Devlet faaliyetleri ve (işleme faaliyeti Devlet güvenlik konularını ilgilendirdiğinde, Devletin ekonomik refahı dahil olmak üzere) Devlet güvenliği, savunma, kamu güvenliğine ilişkin verilerin işlenmesi için herhangi bir durumda ve Avrupa Birliği Anlaşmasının V ve VI. başlıklarıyla belirtilenler gibi Topluluk hukuku kaspamının dışına düşen bir faaliyet esnasında,

bir gerçek kişi tarafından, tamamen kişisel veya ev içi faaliyeti esnasında.

Madde 4 Uygulanacak ulusal kanun

(1) Her bir Üye Devlet, aşağıdaki durumlarda, kişisel verilerin işlenmesi için bu Direktif uyarınca kabul ettikleri ulusal hükümleri uygulayacaklardır:

a. İşleme, Üye Devletin topraklarındaki denetleyici kuruluşunun faaliyetleri bağlamında yapıldığında; aynı denetleyici, çeşitli Üye Devletlerin toprağında yerleşikse, bu kuruluşların her birinin, uygulanan ulusal mevzuatlarda öngörülen yükümlülüklere uymasını temin edecek gerekli tedbirleri almalıdır;
b. denetleyici Üye Devletin topraklarında yerleşik olmayıp, uluslararası kamu hukukuna göre ulusal hukukun uygulandığı bir yerde bulunuyorsa;
c. denetleyici Topluluk topraklarında yerleşik değilse ve işleme amaçları için, kişisel veriler, bahse konu Üye devlet topraklarında konumlanan otomatik cihazları kullanırsa, bu tür cihazlar yalnızca Topluluk toprağı boyunca iletilme amacı için kullanılmadıkça;

(2) 1 (c) paragrafında atıfta bulunulan koşullarda, denetleyici, denetleyicinin kendisine karşı başlatılabilecek davalara zarar vermeksizin o Üye Devlet toprağında yerleşik bir temsilci atamalıdır.

BÖLÜM II
KİŞİSEL VERİLERİN İŞLENMESİNİN YASALLIĞI HAKKINDAKİ GENEL KURALLAR

Madde 5

Üye Devletler, bu bölüm hükümlerinin sınırları kapsamında, kişisel verileri işlemenin yasal olduğu koşulları daha hassas şekilde belirleyeceklerdir.

I.KISIM
VERİ KALİTESİNE İLİŞKİN PRENSİPLER

Madde 6

(1) Üye Devletler, kişisel verilerin aşağıdaki şekilde olmasını sağlayacaklardır:

a. adil ve yasal olarak işlenmiş;
b. belirli, açık ve meşru amaçlar için toplanmış ve bu amaçlarla uyumsuz biçimde başkaca işlenmemiş. Üye Devletlerin uygun korunma önlemleri sağlaması koşuluyla; tarihsel, istatistiksel veya bilimsel amaçlar için verilerin detaylı işlenmesi; uyumsuz olarak kabul edilmeyecektir;
c. toplandığı ve/veya ayrıca işlendiği amaçlara ilişkin olarak yeterlidir, ilgilidir ve bu amacı aşmaz;
d. doğrudur ve gerektiği yerde güncel tutulur. Toplanma ve sonrasındaki işlenme, silinme veya düzeltilme amaçlarını göz önünde tutarak verilerin yanlış veya eksik olmamasını sağlayacak tüm makul önlemler alınmalıdır;
e. verilerin toplandığı esnada veya sonrasında işlendiği amaçlar için gerekenden daha uzun olmayan süre boyunca, veri öznelerinin tespitine izin veren biçimde tutulur. Üye Devletler, tarihsel, istatistiksel veya bilimsel kullanım amacıyla daha uzun süreli depolanan kişisel veriler için uygun koruma önlemleri alacaktır.

(2) 1. paragrafa uyulmasını sağlamak, denetleyicinin sorumluluğundadır olacaktır.

II.KISIM
VERİ İŞLEMEYİ YASALLAŞTIRMA KRİTERLERİ

Madde 7

Üye Devletler, kişisel verilerin işlenebilmesini yalnızca aşağıdaki koşullar sağlanırsa sağlayacaklardır:

a. Veri öznesi açık, kesin ve net bir biçimde rızasını vermişse veya
b. İşleme, bir sözleşme yapmadan önce veri öznesinin talebi üzerine önlem almak için ya da veri öznesinin taraf olduğu bir sözleşmenin yerine getirilmesi için gerekliyse veya
c. İşleme denetleyicinin konusu olan bir yasal yükümlülüğe uyum için gerekirse, veya
d. (d) İşleme, veri öznesinin hayati menfaatlerini korumak için gerekliyse; veya
e. İşleme, verilerin açıklandığı üçüncü bir şahıs veya denetleyiciye yetki veren kamu makamının uygulamasında veya kamu menfaatine yapılan bir görevin yerine getirilmesi için gerekliyse; veya
f. İşleme, bu tür menfaatlerin, madde 1 (1) kapsamında koruma gerektiren veri öznesinin temel hak ve özgürlükleriyle ilgili menfaatleri çiğnemesi haricinde, verilerin açıklandığı üçüncü şahıs veya şahıslar tarafından ya da denetleyici tarafından takip edilen meşru menfaatlerin amaçları için gerekliyse;

III.KISIM
ÖZEL İŞLEME KATEGORİLERİ

Madde 8 Verilerin özel işleme kategorileri

(1) Üye Devletler, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklayacaktır.

(2.1) paragraf aşağıdaki durumlarda uygulanmayacaktır:

a. veri öznesinin rızasını vermesiyle 1. paragrafta atıfta bulunulan yasağın kaldırılamayacağını Üye Devlet kanunlarının belirtmesi haricinde, bu verilerin işlenmesinde veri öznesi açık rızasını vermişse; veya
b. işlemenin, yeterli korunma önlemleri için sağlanan ulusal kanunla yetkilendirildiği kadarıyla, istihdam kanunu alanında, denetleyicinin yükümlülüklerini ve özel haklarını yerine getirme amacı için gerekli olduğunda; veya
c. işleme, veri öznesinin rızasını vernesinin fiziksel veya yasal olarak elverişsiz olduğu durumda, diğer bir kişinin veya veri öznesinin hayati menfaatlerini korumak için gerekliyse; veya
d. işleme; veri öznelerinin rızası olmaksızın verilerin üçüncü şahıslara açıklanmadığı ve işlemenin yalnızca amaçlarıyla bağlantılı olarak düzenli iletişimde oldukları kişileri veya kuruluş mensuplarını ilgilendirmesi koşuluyla bir vakıf, dernek veya siyasi, felsefi, dini veya ticaret birliği amaçlı başka bir kar amacı gütmeyen kuruluş tarafından uygun teminatlı meşru faaliyetler esnasında yapılırsa, veya
e. işleme, veri öznesi tarafından açıkça halka duyurulan verilere ilişkinse ya da kanuni hakların tesisi, yerine getirilmesi veya savunulması için gerekliyse.

(2.2) Paragraf 1, sağlık hizmetlerinin yönetimi veya bakım veya tedavinin sağlanması, tıbbi teşhis, önleyici tıp amaçları için veri işlemenin gerektiği yerde ve mesleki gizlilik yükümlülüğü için ulusal yetkili kuruluşlar tarafından veya eşdeğer gizlilik yükümlülüğüne tabi diğer bir kişi tarafından saptanan ulusal kanun kapsamında bir sağlık uzman öznesi tarafından bu verilerin işlendiği yerde uygulanmayacaktır.

(2.3) uygun korunma önlemlerinin sağlanmasına tabi olarak, Üye Devletler, önemli kamu menfaati nedenleri için, ya ulusal yasa ya da denetleme makamının kararıyla paragraf 2'de belirtilenlere ek olarak muafiyetler koyabilir.

(2.4) suçlar, adli hükümler veya güvenlik tedbirlerine ilişkin verilerin işlenmesi, yalnızca resmi makamın kontrolü altında yapılabilir veya ulusal yasa kapsamında uygun özel korunma önlemleri sağlanırsa, uygun özel korunma önlemleri sağlayan ulusal hükümler kapsamında Üye Devlet tarafından verilebilecek tadillere tabi olabilir. Ancak, adli hükümlerin tam bir kaydı yalnızca resmi makamın kontrolü altında tutulabilir.

(2.5) Üye Devletler, hukuk davalarındaki kararlar veya idari müeyyidelere ilişkin verilerin de resmi makamın kontrolü altında işlenmesini sağlayabilirler.

(2.6) 4 ve 5. paragraflar için 1. paragraftan tadiller komisyona haber verilecektir.

(2.7) Üye Devletler, ulusal bir tespit numarası veya genel başvurunun diğer belirtecinin işlenebileceği koşulları belirleyecektir.

Madde 9 İfade özgürlüğü ve kişisel verilerin işlenmesi

Üye Devletler, kişisel verilerin ifade özgürlüğünü yöneten kurallarla kişisel gizlilik hakkını uzlaştırmak için gerekirse, yalnızca, edebi veya sanatsal açıklama amacı veya gazetecilik amaçları için kişisel verilerin işlenmesinde Kısım IV ve Kısım VI, bu Bölümün hükümlerinden muafiyetler veya derogasyonlar sağlayacaktır.

IV.KISIM
VERİ ÖZNESİNE VERİLECEK BİLGİLER

Madde 10 Veri öznesinden verilerin toplanma durumlarında bilgilendirme

Üye Devletler, önceden mevcut olması haricinde, kendine dair bilgilerin toplandığı bir veri öznesine, denetleyici veya temsilcisinin en azından aşağıdaki bilgileri vermesini sağlamalıdır:

a. Denetleyici ve varsa temsilcisinin kimliği;
b. Kastedilen veri işleme amaçları;
c. Aşağıdakiler gibi herhangi bir başka bilgi;
   - verilerin alıcıları veya alıcı kategorileri,
   - yanıt vermemenin olası sonuçlarının yanı sıra soruların yanıtlarının zorunlu veya gönüllü olup olmadığı,
   - (özneyle) ilgili verileri düzeltme hakkının ve verilere erişim hakkının olması,

(denetleyici veya temsilcisi) bu tür başka bilgilendirmenin gerekli olmasına göre, verilerin toplanmasındaki özel koşulları göz önünde bulundurarak veri öznesine ilişkin adil işlemeyi garanti etmelidirler.

Madde 11 Verilerin veri öznesinden elde edilmediğinde bilgilendirme

Veriler veri öznesinden elde edilmediğinde, Üye Devletler, (veri öznesinin bu bilgilere) önceden sahip olması hariç, kişisel verilerin kaydının yapılması esnasında ya da üçüncü bir şahsa ifşa öngörüldüğünde, verilerin ilk ifşa zamanından önce, denetleyici veya temsilcisinin en azından aşağıdaki bilgileri veri öznesine vermesini sağlayacaktır:

a. Denetleyicinin ve varsa temsilcisinin kimliği;
b. İşlemenin amaçları;
c. Aşağıdakiler gibi herhangi bir başka bilgi;
   - verilerin alıcıları veya alıcı kategorileri,
   - yanıt vermemenin olası sonuçlarının yanı sıra soruların yanıtlarının zorunlu veya gönüllü olup olmadığı,
   - (özneyle) ilgili verileri düzeltme hakkı ve verilere (kendisinin) erişim hakkının olması,

(denetleyici veya temsilcisi) bu tür başka bilgilendirmenin gerekli olmasına göre, verilerin toplanmasındaki özel koşulları göz önünde bulundurarak veri öznesine ilişkin adil işlemeyi garanti etmelidirler.

Kayıt veya ifşa açıkça yasayla belirtilirse ya da aşırı bir çaba gerektirecek ya da imkansızlığı kanıtlanan verilerin sağlanması için, tarihsel veya bilimsel araştırma amaçları için veya istatistiksel amaçlar için işleme durumunda; Paragraf 1 uygulanmayacaktır. Bu durumlarda, Üye Devletler uygun korunma önlemleri sağlayacaktır.

V.KISIM
VERİ ÖZNELERİNİN VERİLERE ERİŞME HAKKI

Madde 12 Erişim hakkı

Üye Devletler, her veri öznesinin denetleyiciden (aşağıdakileri) temin etme hakkını garanti edecektir:

a. aşırı gecikme veya masraf olmaksızın ve makul aralıklarla, sınırlama olmaksızın:

—kendisine dair verilerin işlenip işlenmeyeceği hususunda onay ve en azından, verilerin açıklandığı alıcı kategorileri veya alıcıları ve ilgili verilerin kategorileri, işleme amaçları hususunda bilgi,

—kaynakları hususunda herhangi bir mevcut bilginin ve işleme tabi tutulan verilerin anlaşılır biçimde ona iletilmesi,

—en azından madde 15 (1)'de atıfta bulunulan otomatik kararlar durumunda, kendisine ilişkin verilerin otomatik işlenmesiyle ilgili mantık bilgisi;

b. Özellikle verinin eksik veya yanlış yapısı yüzünden, bu Direktifin hükümlerine uymayan işlemede, verilerin engellenmesi veya silinmesi, uygun olarak düzeltilmesi;
c. Bunun imkansız olduğu gösterilmezse veya orantısız çabayı gerektirmezse, (b) bendine uygun olarak yapılan herhangi bir düzeltme, silme veya engelleme hakkında, verilerin açıklandığı üçüncü şahıslara bildirim.

VI.KISIM
MUAFİYETLER VE SINIRLAMALAR

Madde 13 Muafiyetler ve sınırlamalar

(1) Bu tür bir sınırlama, aşağıdakileri sağlamak için gerekli tedbirleri oluşturduğunda, Üye Devletler, 6 (1), 10, 11 (1), 12 ve 21 maddelerinde belirtilen hak ve yükümlülüklerin kapsamını sınırlandıracak yasal tedbirleri kabul edebilirler:

a. ulusal güvenlik;
b. savunma;
c. kamu güvenliği;
d. düzenlenmiş meslekler için etik ihlallerinin veya ceza gerektiren suçların önlenmesi, incelenmesi, tespiti ve kovuşturulması;
e. parasal, bütçe ve vergilendirme konuları dahil olmak üzere, Avrupa Birliği'nin veya bir Üye Devletin önemli bir ekonomik veya mali menfaati;
f. c), (d) ve (e)'de atıfta bulunulan durumlarda, resmi makamın yürütmesiyle ara sıra da olsa bağlantılı düzenleyici fonksiyon veya izleme, denetim;
g. diğerlerinin hak ve özgürlüklerinin veya veri öznesinin korunması.

(2) Üye Devletler, yeterli yasal korunma önlemlerine tabi olarak özellikle veriler herhangi özel bir bireye dair kararlar veya tedbirler almak için kullanılmadığında, veri öznesinin gizlilik hakkını ihlal riski açıkça yoksa, veriler yalnızca bilimsel araştırma amacı için işlendiğinde veya yalnızca istatistik yaratma amacı için gerekli dönemi aşmayan bir süre için kişisel formda tutulduğunda, madde 12'de belirtilen hakları bir yasama tedbiriyle sınırlandırabilir.

VII.KISIM
VERİ ÖZNESİNİN İTİRAZ HAKKI

Madde 14 Veri öznesinin itiraz hakkı

Üye Devletler aşağıdaki hakları veri öznesine vereceklerdir:

a. En azından madde 7 (e) ve (f)'de atıfta bulunulan durumlarda, ulusal mevzuat tarafından aksinin belirtilmesi haricinde, kendisine dair verilerin işlenmesinde, özel durumuna ilişkin zorlayıcı kanuni gerekçelere her zaman itiraz etmek. Gerekçeli bir itiraz olduğunda, denetleyici tarafından başlatılan işleme, artık bu verileri kapsamayabilir;
b. Denetleyicinin doğrudan pazarlama amaçları için işlenmesini öngördüğü, kendine ait kişisel verilerin işlenmesine ücretsiz ve istek üzerine itiraz etme (hakkı) veya kişisel veriler üçüncü şahıslara ilk kez ifşa edilmeden veya doğrudan pazarlama amaçları için üçüncü şahıslar adına kullanılmadan önce bilgilendirilme (hakkı) ve bu tür ifşalara veya kullanımlara ücretsiz itiraz hakkının açık şekilde sunulması;

Üye Devletler, (b)'nin ilk alt paragrafında atıfta bulunulan hakkın varlığından veri öznelerinin haberdar olmasını temin etmek için gerekli tedbirleri alacaklardır.

Madde 15 Otomatik bireysel kararlar

(1) Üye Devletler, her kişiye, işte performans, kredibilite, güvenilirlik, tutum v.b gibi kendisine ilişkin bazı kişisel yönleri değerlendirmek için yalnızca verilerin otomatik işlenmesine dayalı ve onu önemli derecede etkileyen veya ona ilişkin yasal etkiler üreten bir karara tabi kalmama hakkı verecektir.

(2) Bu Direktifin diğer maddelerine tabi olarak Üye Devletler şayet karar aşağıdaki şekilde alındı veya yetki veriyorsa, 1. paragrafta atıfta bulunulan türde bir karara bir kişinin tabi olabilmesini sağlayacaklardır:

a. kendi görüşünü belirtmesine izin veren düzenlemeler gibi meşru menfaatlerini güvenceye alacak uygun tedbirler olduğunda ya da veri öznesi tarafından sunulan sözleşmenin yapılması veya yerine getirilme talebinin karşılanması koşuluyla bir sözleşmenin yapılması veya yerine getirilmesi esnasında alınırsa veya;
b. öznenin meşru menfaatlerini güvenceye alacak tedbirleri de belirten bir yasa tarafından yetkilendirilirse.

VIII.KISIM
İŞLEMENİN GİZLİLİĞİ VE GÜVENLİĞİ

Madde 16 İşlemenin gizliliği

Kişisel verilere erişme hakkı olan işleyicinin kendisi dahil olmak üzere, işleyicinin veya denetleyicinin yetkisi altındaki herhangi bir kişi, bunu yapması kanun tarafından istenmezse, denetleyicinin talimatı haricinde verileri işlememelidir.

Madde 17 İşlemenin güvenliği

(1) Üye Devletler, özellikle işlemenin bir ağ üzerinde verilerin iletilmesini gerektirdiğinde ve işlemenin tüm diğer yasa dışı biçimlerine karşı, yetkisiz açıklama veya erişim, değiştirme, kazara kayıp veya kazara veya yasa

dışı tahribe karşı kişisel verileri korumak için gereken uygun teknik ve kurumsal tedbirleri, denetleyicinin uygulamasını sağlayacaklardır.

Bu tür tedbirler, uygulamalarının durum ve maliyetini dikkate alarak, korunacak verinin yapısına ve işleme tarafından sunulan risklere uygun seviyede güvenlik sağlayacaktır.

(2) Üye Devletler, işleme kendi adına yürütüldüğünde, denetleyicinin yürütülecek işlemeyi yöneten teknik güvenlik tedbirlerine ve kurumsal tedbirlere dair yeterli garantiler sağlayan bir işleyiciyi seçmesini ve bu tedbirlerle uyum sağlamasını temin edecektir.

(3) İşleyici vasıtasıyla işlemenin yapılması özellikle aşağıdakileri şart koşan ve işleyiciyi denetleyiciye bağlayan yasal belge veya bir sözleşme ile yönetilmelidir:

- işleyici yalnızca denetleyiciden gelen talimatlara göre hareket edecektir.
- işleyicinin yerleşik olduğu Üye Devlet kanunuyla tanımlandığı şekilde, 1. paragrafta düzenlenen yükümlülükler işleyicinin de ödevi olacaktır.

(4) Paragraf 1'de atıfta bulunulan tedbirlere dair koşullara ve veri korunmasına ilişkin yasal belge veya sözleşmenin parçaları, kanıtı tutma amaçları için yazılı veya eşdeğer diğer bir biçimde olacaktır.

IX.KISIM
BİLDİRİM

Madde 18 Denetleme makamına bildirimde bulunma yükümlülüğü

1. Üye Devletler, kısmen veya tamamen otomatik işleme faaliyeti veya tek amaç veya ilgili çeşitli amaçlara hizmet etmesi istenen bu tür bir dizi faaliyeti yürütmeden önce denetleyici ve varsa temsilcisinin, madde 28'de atıfta bulunulan denetleme makamına bildirimde bulunmasını sağlayacaklardır.

2. Üye Devletler, yalnızca aşağıdaki durumlarda ve aşağıdaki koşullarda bildirimden muafiyeti veya bildirimin basitleştirilmesini sağlayabilirler:

- veri öznelerinin haklarını ve özgürlüklerini olumsuz şekilde etkileyecek, işlenecek verileri muhtemelen dikkate almayan işleme faaliyeti kategorileri için, depolanacak veriler süre uzunluğu ve verilerin ifşa edileceği alıcılar veya alıcı kategorileri, veri öznesi kategorisi veya kategorileri, işlemeye tabi veri kategorileri veya veriler, işleme amaçlarını belirtirler, ve/veya;

- denetleyici, kendisini yöneten ulusal kanunla uyumlu olarak özellikle aşağıdakilerden sorumlu bir kişisel veri koruma görevlisi atar;

- bu Direktif uyarınca, alınan ulusal hükümlerin bağımsız şekilde dahili uygulamasını sağlama;

- madde 21(2)'de atıfta bulunulan bilgilendirme maddelerini içeren şekilde, denetleyici tarafından yürütülen işleme faaliyetlerinin kaydını tutma;

- böylece, veri öznelerinin hak ve özgürlüklerinin, işleme faaliyetleri tarafından olumsuz şekilde etkilenmesinin olanaksız olmasını sağlama.

3. Üye Devletler, bir meşru menfaat gösteren herhangi bir kişi tarafından veya genel olarak kamu tarafından danışmaya açık olan ve kamuya bilgi sağlamak amaçlı kanunlara veya yönetmeliklere göre tek amacı bir kayıt tutma olan işlemeye 1. paragrafın uygulanmamasını sağlayabilir.

4. Üye Devletler, madde 8(2)(d)'de atıfta bulunulan işleme faaliyetleri durumunda, bildirimin basitleştirilmesini veya bildirimde bulunma yükümlülüğünden muafiyeti sağlayabilirler.

5. Üye Devletler, kişisel verileri kapsayan belirli veya tüm otomatik olmayan işleme faaliyetlerinin bildirilmesini şart koşabilirler ya da bu işleme faaliyetlerinin basitleştirilmiş bildirime tabi olmasını belirtebilirler.

Madde 19 Bildirim içerikleri

1. Üye Devletler, bildirimde verilecek bilgileri belirteceklerdir. Bunlar en azından aşağıdakileri içerecektir:

   a. Denetleyici ve varsa temsilcisinin adı ve adresi;
   b. İşlemenin amacı veya amaçları;
   c. Bunlara ilişkin veri kategorileri veya verinin ve özne verisinin kategorileri veya kategorisinin tanımı;
   d. Verilerin açıklanabileceği alıcılar veya alıcı kategorileri;
   e. Üçüncü ülkelere önerilen veri transferleri;
   f. Veri güvenliğini sağlamak üzere madde 17 uyarınca alınan tedbirlerin uygunluğunun sağlanması için bir ön değerlendirmeye olanak sağlayan genel bir tanım;

2. Üye Devletler paragraf 1'de atıf yapılan bilgileri etkileyen herhangi bir değişikliğin denetleme makamına bildirilmesine dönük prosedürleri belirletecektir.

Madde 20 Ön kontrol

1. Üye Devletler, veri öznelerinin haklarına ve özgürlüklerine özel riskler sunması, olası işleme faaliyetlerini belirleyecektir ve bu işleme faaliyetlerinin başlatılmasından önce incelenmesini kontrol edecektir.
2. Bu tür ön kontroller, şüphe durumunda denetim makamına danışması gereken bir veri koruma görevlisi tarafından veya denetleyiciden bir bildirimin alınmasını takiben denetleme makamı tarafından yerine getirilecektir.
3. Üye Devletler ya ulusal parlamentonun bir tedbiri ya da işlemenin yapısını tanımlayan ve uygun korunma önlemlerini belirten bu tür bir yasama tedbirine dayalı bir tedbirin hazırlanması bağlamında, bu tür kontrolleri de yapabilir.

Madde 21 İşleme faaliyetlerinin duyurulması

1. Üye Devletler, işleme faaliyetlerinin duyurulmasını temin etmek için tedbirler alacaktır.
2. Üye Devletler, madde 18'e uygun olarak, bildirilen işleme faaliyetlerinin bir kaydının denetleme makamı tarafından tutulmasını sağlayacaktır.

   Kayıt, en azından madde 19 (1) (a) (e) de listelenen bilgileri içerecektir. Kayıt herhangi bir kişi tarafından denetlenebilir.

3. Üye Devletler, bildirime tabi olmayan işleme faaliyetlerine ilişkin olarak, Üye Devletler tarafından atanan denetleyicilerin veya diğer bir kuruluşun, talep üzerine herhandi bir kişiye uygun biçimde en azından madde 19 (1) (a) (e)de atıfta bulunulan bilgileri sağlamasını temin edecektir.

   Üye Devletler ya meşru menfaat kanıtını temin edebilen herhangi bir kişi tarafından ya da genel olarak kamu tarafından danışmaya açık olan ve kamuya bilgi sağlaması kastedilen yönetmeliklere veya yasalara göre; tek amacı bir kayıt tutulması olan işlemeye bu hükmün uygulanmamasını sağlayabilir.

BÖLÜM III
YARGI YOLLARI, SORUMLULUK VE MÜEYYİDELER

Madde 22 Yargı yolları

Yargı makamına başvurudan önce, madde 28'de atıfta bulunulan denetleme makamı öncesinde, diğerlerine ilaveten koyulabilecek hüküm için herhangi bir idari çözüme zarar vermeksizin, Üye Devletler, söz konusu işlemeye uygulanan ulusal kanun tarafından garanti edilen hakların herhangi bir ihlali için bir yargı yolunu, her kişinin hakkı olarak sağlayacaktır.

Madde 23 Sorumluluk

1. Üye Devletler, bu Direktif uyarınca kabul edilen ulusal hükümlerle uyumsuz herhangi bir işlemenin veya yasadışı bir işleme faaliyetinin sonucu olarak zarara uğrayan herhangi bir kişinin, uğradığı zarar için denetleyiciden tazminat almaya hak kazanmasını sağlayacaktır.
2. Denetleyici, zarara yol açan olayda sorumlu olmadığını kanıtlarsa, kısmen ya da tamamen bu yükümlülükten muaf tutulabilir.

Madde 24 Müeyyideler

Üye Devletler, bu Direktifin hükümlerinin tam uygulanmasını sağlayacak uygun tedbirleri kabul edecektir ve özellikle, bu direktif uyarınca kabul edilen hükümlerin ihlali durumunda uygulanacak müeyyideleri koyacaktır.

BÖLÜM IV
KİŞİSEL VERİLERİN ÜÇÜNCÜ ÜLKELERE TRANSFERİ

Madde 25 Prensipler

1. Üye Devletler, bu Direktifin diğer hükümleri uyarınca benimsenen ulusal hükümlere uyuma zarar vermeksizin, yalnızca söz konusu üçüncü ülke yeterli koruma seviyesi sağlarsa, transfer sonrası işleme için istenen veya işlemeye tabi olan kişisel verilerin bir üçüncü ülkeye transferinin gerçekleşebilmesini sağlayacaktır.
2. Bir üçüncü ülke tarafından sağlanan koruma seviyesinin yeterliliği, veri transfer faaliyetlerinin dizisinin veya bir veri transfer faaliyetini çevreleyen tüm koşulların ışığında değerlendirilecektir. O ülkeyle uyumlu meslek kuralları ve güvenlik tedbirleri ve söz konusu üçüncü ülkedeki yürülükte olan hem genel hem sektörel yasa hükümleri, son varış ülkesi ve menşe ülke, önerilen faaliyet veya faaliyetlerin süresi ve amacı, verilerin yapısına özel önem verilecektir.
3. Üye Devletler ve Komisyon, 2. paragrafın anlamı dahilinde yeterli koruma seviyesini bir üçüncü ülkenin sağlamadığını düşündükleri durumlarda birbirlerini bilgilendireceklerdir.
4. Komisyon, bu maddenin 2. paragrafının anlamında, bir üçüncü ülkenin yeterli koruma seviyesini sağlamadığını madde 31 (2) kapsamında sağlanan prosedure göre tespit ederse, Üye Devletler, söz konusu üçüncü ülkeye aynı tipte verilerin herhangi bir transferini önlemek için gerekli önlemleri alacaklardır.
5. Komisyon, uygun bir zamanda, paragraf 4 uyarınca sağlanan bulgudan kaynaklanan durumu çözmek amacıyla müzakerelere başlayacaktır.

6. Komisyon, madde 31 (2)'de atıfta bulunulan prosedüre uygun olarak; bireylerin temel haklarının ve özel yaşamlarının korunması için, özellikle paragraf 5'te atıfta bulunulan müzakerelerin sonuçlanması üzerine, giriştiği uluslararası taahhütler veya kendi yerel yasası nedeniyle, bu maddenin 2. paragrafı anlamı dahilinde üçüncü bir ülkenin yeterli bir koruma seviyesini temin etmesini isteyebilir.

   Üye Devletler, Komisyonun kararıyla uyum sağlamak için gerekli tedbirleri alacaktır.

Madde 26 İstisnalar

1. Madde 25'den derogasyon (uygulama dışı tutma) yoluyla ve özel durumları yöneten iç hukukun aksini belirtmesi haricinde, Üye Devletler, aşağıdaki koşullarda madde 25 (2)'nin anlamı dahilinde yeterli koruma seviyesini sağlamayan üçüncü bir ülkeye kişisel verilerin transfer dizisini veya transferinin yapılabilmesini sağlayacaktır:
   a. Veri öznesi önerilen transfer için açık şekilde rızasını vermişse veya
   b. Veri öznesinin talebine yanıt olarak alınan ön sözleşme tedbirlerinin uygulanması veya denetleyici ve veri öznesi arasındaki bir sözleşmenin yerine getirilmesi için transfer gerekliyse; veya
   c. Üçüncü bir şahıs ve denetleyici arasında veri öznesinin menfaatine sonuçlanan bir sözleşmenin yerine getirilmesi veya sonuçlandırılması için transfer gerekliyse, veya
   d. Transfer; kanuni hakların tesisi, işletilmesi veya savunulması için veya önemli kamu menfaati zemininde yasal olarak gerekliyse veya zorunluysa, veya
   e. Veri öznesinin hayati menfaatlerinin korunması için transfer gerekirse, veya
   f. Özel durumda yapılan konsültasyon için kanunda öngörülen koşullar ölçüsünde, bir meşru menfaat gösteren herhangi bir kişi tarafından veya genel olarak kamu tarafından danışmaya açık olan ve kamuya bilgi sağlamak amaçlı kanunlar veya yönetmeliklere göre transfer bir kayıttan sağlanırsa.
2. Paragraf 1'e zarar vermeksizin, bir Üye Devlet, ilgili hakların işletilmesine dair ve bireylerin temel hak ve özgürlükleri ve kişisel mahremiyet hakkının korunmasına ilişkin anlam dahilinde, yeterli koruma seviyesini sağlamayan üçüncü bir ülkeye kişisel veri transferler dizisine veya bir transferine izin verebilir, bu tür korunma önlemleri özellikle uygun sözleşme maddelerinden kaynaklanabilir.
3. Üye Devlet, paragraf 2 uyarınca verdiği izinlerden Üye Devletleri ve Komisyonu haberdar edecektir.

   Bir Üye Devlet veya Komisyon, bireylerin temel hakları ve özgürlükleri ve mahremiyetinin korunmasını gerektiren gerekçeli dayanaklara itiraz ederse, Komisyon, madde 31 (2)'de belirtilen prosedüre göre uygun tedbirleri alacaktır.

   Üye Devletler Komisyonun kararına uymak için gerekli tedbirleri alacaklardır.

4. Madde 31 (2)'de atıfta bulunulan prosedüre uygun olarak, Komisyon, bazı standart sözleşme maddelerinin paragraf 2'nin gerektirdiği şekilde yeterli teminat sunmasına karar verirse, Üye Devletler, Komisyon kararına uymak için gerekli tedbirleri alacaklardır.

BÖLÜM V
DAVRANIŞ KURALLARI

Madde 27

1. Üye Devletler ve Komisyon, çeşitli sektörlerin özel niteliklerini dikkate alarak, bu Direktif uyarınca Üye Devletler tarafından benimsenen ulusal hükümlerin doğru uygulanmasına katkı sağlamak için planlanan davranış kurallarını düzenlemeye teşvik edecektir.
2. Üye Devletler, mevcut ulusal kodları tadil etme veya genişletme niyetine sahip veya taslak ulusal kodları hazırlamış denetleyicilerin diğer kategorilerini temsil eden diğer kuruluşlar ve ticari kurumların, davranış kurallarını ulusal makamın görüşüne sunabilmesi için önlem alacaktır.

   Üye Devletler, sunulan taslakların, bu Direktif uyarınca kabul edilen ulusal hükümlerle uyumlu olup olmadığını ulusal makamın belirlemesi için önlem alacaktır. Komisyon, taslağı uygun görürse, ulusal makam, kendi temsilcilerinin veya veri öznelerinin görüşlerini isteyecektir.

3. Taslak Topluluk kodları ve mevcut Topluluk kodlarının uzantıları veya düzeltmeleri, madde 29'da atıfta bulunulan çalışma grubuna sunulabilir. Bu çalışma grubu diğer şeyler arasında, sunulan taslağın, bu Direktif uyarınca kabul edilen ulusal hükümlere uygun olup olmadığını belirleyecektir. Uygun bulursa, (ulusal) makam, veri öznelerinin ve kendi temsilcilerinin görüşlerini isteyecektir. Komisyon, Çalışma Grubu tarafından onaylanmış kuralların uygun şekilde tanıtımını sağlayabilir.

BÖLÜM VI
KİŞİSEL VERİLERİN İŞLENMESİNE DAİR BİREYLERİN KORUNMASI HAKKINDAKİ ÇALIŞMA GRUBU VE DENETLEME MAKAMI

Madde 28 Denetleme makamı

1. Her bir Üye Devlet, , bu Direktif uyarınca Üye Devletler tarafından kabul edilen hükümlerin kendi ülkesindeki uygulamasını izlemekten, bir veya daha fazla kamu makamının sorumlu olmasını sağlayacaktır.

   Bu makamlar, onlara tevdi edilen işlevleri yerine getirmede tam bağımsız olarak hareket edeceklerdir.

2. Her bir Üye Devlet, kişisel verilerin işlenmesine dair bireylerin hak ve özgürlüklerinin korunmasına ilişkin idari tedbirleri veya yönetmelikleri hazırlarken, denetim makamına danışılmasını sağlayacaktır.
3. Her bir makama özellikle sağlanacaktır:

   — denetim görevlerinin yerine getirilmesi için gerekli tüm bilgileri toplama yetkileri ve işleme faaliyetlerinin konusunu oluşturan verilere erişim yetkileri gibi araştırma yetkileri;

   — örneğin ulusal parlamentolar veya diğer siyasi kuruluşlara konuyu havale etme veya denetleyiciye ihtar verme veya uyarma, işleme üzerinde geçici veya kesin yasaklama koyma, verilerin yok edilmesini veya silinmesini, engellenmesini emretme, bu tür görüşlerin uygun şekilde yayınlanmasını sağlama ve madde 20'e uygun olarak işleme faaliyetlerinin yerine getirilmesinden önce görüş bildirme gibi etkin müdahale yetkileri;

— Bu Direktif uyarınca kabul edilen ulusal hükümler ihlal edildiğinde veya bu ihlalleri yargı makamlarının dikkatine sunma için kanuni kovuşturmaya girişme yetkisi.

Denetleme makamının şikayetlere yol açan kararları; mahkemelerde temyiz edilebilir.

4. Her bir denetim makamı, kişisel verilerin işlenmesine dair hak ve özgürlüklerin korunmasına ilişkin o kişiyi temsil eden bir dernek veya herhangi bir kişi tarafından arzedilen iddiaları dinleyecektir.

   Her bir denetim makamı, özellikle, bu Direktifin 13. maddesi uyarınca kabul edilen ulusal hükümler uygulandığında, herhangi bir kişi tarafından arz edilen veri işlemenin yasallığı hakkındaki kontroller için iddiaları dinleyecektir. Kişi, bir kontrolün yapıldığından her halükarda bilgilendirilecektir.

5. Her denetleme makamı, faaliyetleri hakkında düzenli aralıklarla bir rapor hazırlayacaktır. Rapor, kamuya açıklanacaktır.
6. Her denetleme makamı, sözkonusu işlemeye uygulanan ulusal kanun her ne olursa olsun, paragraf 3'e uygun olarak verilen yetkileri kendi Üye Devletinin toprağında uygulamaya yetkilidir. Her bir makamdan, diğer bir Üye Devletin makamı ile yetkilerini uygulaması istenebilir.

   Denetleme makamları, özellikle tüm yararlı bilgileri takas ederek, kendi görevlerini yerine getirmek için gerekli ölçüde birbirleriyle iş birliği yapacaklardır.

7. Üye Devletler, görevlerinin bitiminden sonra bile, denetleme makamının personellerinin ve mensuplarının, eriştikleri gizli bilgilere dair mesleki gizlilik görevine tabi olmalarını sağlayacaktır.

Madde 29 Kişisel Verilerin İşlenmesine dair Bireylerin Korunması Hakkındaki Çalışma Grubu

1. Bundan böyle "Çalışma Grubu" denilecek olan, Kişisel Verilerin İşlenmesine dair Bireylerin Korunması hakkında bir çalışma grubu, bu belgeyle kurulmaktadır.

   Danışma statüsüne sahip olacak ve bağımsız olarak hareket edecektir.

2. Çalışma Grubu, Komisyon'un bir temsilcisi ve Topluluk kurumları ve kuruluşları için kurulan makamların veya makamın birer temsilcisi ve her bir Üye Devlet tarafından atanan denetleme makamı veya makamlarının birer temsilcisinden oluşacaktır.

   Çalışma Grubunun her bir üyesi, temsil ettikleri makam veya makamlar, kurumlar tarafından atanacaklardır. Bir Üye Devlet birden fazla denetleme makamı atamışsa, bunlar ortak bir temsilci atayacaklardır. Aynısı, Topluluk kurum ve kuruluşları için saptanan makamlara uygulanacaktır.

3. Çalışma Grubu, denetleme makamları temsilcilerinin salt (kendi) çoğunluğuyla kararlar alacaktır.
4. Çalışma Grubu, başkanını seçer. Başkanın görev süresi iki yıl olacaktır. Başkan yeniden seçilebilecektir.
5. Çalışma Grubunun sekreteryası Komisyon tarafından sağlanacaktır.
6. Çalışma Grubu, kendi prosedür kurallarını kabul edecektir.
7. Çalışma Grubu, ya Komisyon'un talebi veya denetleme makamının bir temsilcisinin talebi üzerine veya kendi insiyatifiyle, başkanı tarafından gündemine getirilen maddeleri ele alacaktır.

Madde 30

1. Çalışma Grubu:
   a. Bu tür tedbirlerin düzenli uygulanmasına katkı sağlamak için bu Direktif kapsamında benimsenen ulusal tedbirlerin uygulanmasını kapsayan herhangi bir sorunu inceleyecektir;
   b. Topluluktaki ve üçüncü ülkelerdeki koruma seviyesi hakkında Komisyon'a görüş verecektir;
   c. Kişisel verilerin işlenmesine dair gerçek kişilerin hak ve özgürlüklerini güvenceye alacak ek veya özel tedbirler hakkında ve bu tür hak ve özgürlükleri etkileyen diğer önerilmiş Topluluk tedbirleri hakkında, bu Direktifin herhangi bir önerilen tadili üzerinde Komisyona tavsiyede bulunacaktır;
   d. Topluluk seviyesinde hazırlanan davranış kuralları hakkında görüş verecektir.
2. Çalışma Grubu, Topluluktaki kişisel verilerin işlenmesine dair kişilerin korunmasında eşdeğerliği muhtemelen etkileyecek uyuşmazlıkların Üye Devletlerin uygulamalarından ya da kanunlarından kaynaklandığını saptarsa, bu doğrultuda Komisyon'u bilgilendirecektir.
3. Çalışma Grubu kendi insiyatifiyle, Toplulukta kişisel verilerin işlenmesine dair kişilerin korunmasına ilişkin tüm konularda tavsiyelerde bulunabilir.
4. Çalışma Grubunun fikirleri ve tavsiyeleri, madde 31'de atıfta bulunulan komiteye ve Komisyon'a iletilecektir.
5. Komisyon, görüş ve tavsiyelerine yanıt olarak aldığı önlemleri Çalışma Grubu'na bildirecektir. Bunu Avrupa Parlamentosu ve Konseyi'ne de iletilecek bir raporla yapacaktır. Rapor kamuya açık olacaktır.
6. Çalışma Grubu, Komisyon, Avrupa Parlamentosu ve Konseyi'ne iletilecek olan üçüncü ülkelerde ve topluluktaki kişisel verilerin işlenmesine dair gerçek kişilerin korunmasına dair durum hakkında bir yıllık rapor hazırlayacaktır. Rapor halka duyurulacaktır.

BÖLÜM VII
TEDBİRLERİ UYGULAYAN TOPLULUK

Madde 31

1. Komisyon bir komite tarafından desteklenecektir.
2. Bu maddeye atıf yapıldığında, 1999/468/EC (1) sayılı kararın 4 ve 7. maddeleri, ilgili 8. maddenin hükümleri gözönünde bulundurularak uygulanacaktır.
   1999/468/EC sayılı kararın 4(3) maddesinde belirtilen dönem, üç ay olacaktır.
3. Komite kendi prosedür kurallarını kabul edecektir.

Madde 32 Nihai Hükümler

1. Üye Devletler, bu Direktifle uyum sağlamak için gerekli idari hükümleri, yasaları ve yönetmelikleri kabul edilme tarihinden itibaren en geç üç yıllık dönemin bitimine kadar yürürlüğe koyacaklardır.

   Üye Devletler bu kararları kabul ettiğinde, bunlar, bu Direktife bir atıfı içerecektir veya kendi resmi yayınları dolayısıyla bu tür bir atıf eşlik edecektir. Bu tür referans yapma yöntemleri, Üye Devletler tarafından öngörülecektir.

2. Üye Devletler, bu Direktif uyarınca kabul edilen ulusal hükümlerin yürürlüğe girdiği tarihte devam eden işlemenin; bu yürürlük tarihinden itibaren üç yıl içinde, bu hükümlerle uygun hale getirilmesini temin edeceklerdir.

Önceki alt paragraftan derogasyon yoluyla, Üye Devletler, bu Direktifin uygulanmasına ilişkin benimsenen ulusal hükümlerin yürürlüğe koyulduğu tarihte manuel dosyalama sisteminde tutulan verilerin işlenmesinin kabul tarihinden itibaren

12 yıl içinde, bu Direktifin 6, 7 ve 8. maddelerine uyumlu hale getirilmesini sağlayabilirler. Ancak, Üye Devletler, denetleyici tarafından izlenen meşru amaçlarla uyumsuz bir biçimde depolanan veya eksik, yanlış olan verilerin engellenmesi veya silinmesi, düzeltilmesi ve elde etme hakkını, özellikle erişim hakkını yerine getirme zamanında ve talebi üzerine veri öznesine vereceklerdir.

3. Paragraf 2'den derogasyon yoluyla, Üye Devletler, uygun korunma önlemlerine tabii olarak, yalnızca, tarihsel araştırma amacıyla tutulan verilerin bu Direktifin 6, 7 ve 8. Maddesine uyumlu hale getirilmesine gerek olmadığını belirtebilirler.
4. Üye Devletler, bu Direktifle kapsanan alanda kabul ettikleri iç hukuk hükümlerinin metnini Komisyona iletecektir.

Madde 33

Komisyon, gerekirse, tadiller için uygun önerileri raporuna ekleyerek, bu Direktifin uygulanması hakkında madde 326 de atıfta bulunulan tarihin 3 yıl öncesinden başlayarak düzenli aralıklarla Avrupa Parlamentosu ve Konseye rapor sunacaktır. Rapor halka duyurulacaktır.

Komisyon, özellikle, gerçek kişilere ilişkin ses ve görüntü verilerinin işlenmesinde bu Direktifin uygulanmasını inceleyecektir ve bilgi toplumundaki ilerleme durumunun ışığında ve bilgi teknolojisindeki gelişmeleri dikkate alarak gerekeceği kanıtlanan herhangi uygun önerileri sunacaktır.

Madde 34

Bu Direktif Üye Devletlere hitap etmektedir.

6 Komisyona verilen uygulama yetkilerinin yerine getirilme prosedürlerini belirten 1999/468/EC sayı ve 28 Haziran 1999 tarihli Konsey Kararı (OJ L 184, 17.7.1999, sayfa:23)

2000/C AVRUPA BİRLİĞİ TEMEL HAKLAR ŞARTININ İLGİLİ HÜKÜMLERİ

***Düzenlemenin orijinal ismi**: Charter of Fundamental Rights of the European Union*
***Düzenlemenin künyesi**: 2000/C 364/01*
***Düzenlemenin orijinal metni için**:*
http://www.europarl.europa.eu/charter/pdf/text_en.pdf (Son erişim tarihi: 16.04.2016)

Article 8 Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

2002/58/EC SAYILI ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN İŞLENMESİ VE ÖZEL HAYATIN GİZLİLİĞİNİN KORUNMASINA İLİŞKİN DİREKTİF

> ***Düzenlemenin orijinal ismi:*** *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*
> ***Düzenlemenin künyesi:*** *32002L0058 Official Journal L 201 , 31/07/2002 P. 0037 – 0047*
> ***Düzenlemenin orijinal metni için:***
> *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058 (Son erişim tarihi: 16.04.2016)*
> ***Not:*** *Bu Direktif, 97/66/EC Sayılı Telekomünikasyon Alanında Kişisel Verilerine İşlenmesi Ve Özel Hayatın Korunmasına İlişkin Direktifi yürürlükten Kaldırmıştır.*

BAŞLANGIÇ

Directive 2002/58/EC of the European Parliament and of the Council

of 12 July 2002

concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Having consulted the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.

(4) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(5) translated the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector. Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.

(5) New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.

(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

(8) Legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the electronic communication sector, should be harmonised in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered.

(9) The Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible.

(10) In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(12) Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.

(13) The contractual relation between a subscriber and a service provider may entail a periodic or a one-off payment for the service provided or to be provided. Prepaid cards are also considered as a contract.

(14) Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

(15) A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.

(16) Information that is part of a broadcasting service provided over a public communications network is intended for a potentially unlimited audience and does not constitute a communication in the sense of this Directive. However, in cases where the individual subscriber or user receiving such information can be identified, for example with video-on-demand services, the information conveyed is covered within the meaning of a communication for the purposes of this Directive.

(17) For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given

specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website.

(18) Value added services may, for example, consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information.

(19) The application of certain requirements relating to presentation and restriction of calling and connected line identification and to automatic call forwarding to subscriber lines connected to analogue exchanges should not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort. It is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission.

(20) Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC.

(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.

(22) The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.

(23) Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should

be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged.

(24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.

(25) However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

(26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services or for the provision of value added services should also be erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.

(27) The exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service that is provided. For instance for a voice telephony call the transmission will be completed as soon as either of

the users terminates the connection. For electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider.

(28) The obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication does not conflict with such procedures on the Internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services.

(29) The service provider may process traffic data relating to subscribers and users where necessary in individual cases in order to detect technical failure or errors in the transmission of communications. Traffic data necessary for billing purposes may also be processed by the provider in order to detect and stop fraud consisting of unpaid use of the electronic communications service.

(30) Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required.

(31) Whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it.

(32) Where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in Directive 95/46/EC. Where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data.

(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card. To the same end, Member States may ask the operators to offer their subscribers a different type of detailed bill in which a certain number of digits of the called number have been deleted.

(34) It is necessary, as regards calling line identification, to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. There is justification for overriding the elimination of calling line

identification presentation in specific cases. Certain subscribers, in particular help lines and similar organisations, have an interest in guaranteeing the anonymity of their callers. It is necessary, as regards connected line identification, to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls. The providers of publicly available electronic communications services should inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification as well as the privacy options which are available. This will allow the subscribers to make an informed choice about the privacy facilities they may want to use. The privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available electronic communications service.

(35) In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent. Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge.

(36) Member States may restrict the users' and subscribers' rights to privacy with regard to calling line identification where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services to carry out their tasks as effectively as possible. For these purposes, Member States may adopt specific provisions to entitle providers of electronic communications services to provide access to calling line identification and location data without the prior consent of the users or subscribers concerned.

(37) Safeguards should be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others. Moreover, in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available electronic communications service.

(38) Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.

(39) The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the

data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.

(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

(41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

(42) Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls. Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.

(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

(44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this Directive.

(45) This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce)(6) are fully applicable.

(46) The functionalities for the provision of electronic communications services may be integrated in the network or in any part of the terminal equipment of the user, including the software. The protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service and of the distribution of the necessary functionalities between these components. Directive 95/46/EC covers any form of processing of personal data regardless of the technology used. The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way. It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected. The adoption of such measures in accordance with Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity(7) will ensure that the introduction of technical features of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market.

(47) Where the rights of the users and subscribers are not respected, national legislation should provide for judicial remedies. Penalties should be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.

(48) It is useful, in the field of application of this Directive, to draw on the experience of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data composed of representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC.

(49) To facilitate compliance with the provisions of this Directive, certain specific arrangements are needed for processing of data already under way on the date that national implementing legislation pursuant to this Directive enters into force,

HAVE ADOPTED THIS DIRECTIVE:

MADDELER

Article 1 Scope and aim

1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to

activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 2 Definitions

Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)(8) shall apply.

The following definitions shall also apply:

(a) "user" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

(b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

(d) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

(e) "call" means a connection established by means of a publicly available telephone service allowing two-way communication in real time;

(f) "consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;

(g) "value added service" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;

(h) "electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Article 3 Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.

2. Articles 8, 10 and 11 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.

3. Cases where it would be technically impossible or require a disproportionate economic effort to fulfil the requirements of Articles 8, 10 and 11 shall be notified to the Commission by the Member States.

Article 4 Security

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Article 5 Confidentiality of the communications

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Article 6 Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 7 Itemised billing

1. Subscribers shall have the right to receive non-itemised bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.

Article 8 Presentation and restriction of calling and connected line identification

1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.

5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 9 Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

Article 10 Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

(a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service;

(b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

Article 11 Automatic call forwarding

Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.

Article 12 Directories of subscribers

1. Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

2. Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

Article 13 Unsolicited communications

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

Article 14 Technical features and standardisation

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services(9).

3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications(10).

Article 15 Application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

Article 16 Transitional arrangements

1. Article 12 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this Directive enter into force.

2. Where the personal data of subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the provisions of Directive 95/46/EC and of Article 11 of Directive 97/66/EC before the national provisions adopted in pursuance of this Directive enter into force, the

personal data of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received complete information about purposes and options in accordance with Article 12 of this Directive.

Article 17 Transposition

1. Before 31 October 2003 Member States shall bring into force the provisions necessary to comply with this Directive. They shall forthwith inform the Commission thereof.

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

Article 18 Review

The Commission shall submit to the European Parliament and the Council, not later than three years after the date referred to in Article 17(1), a report on the application of this Directive and its impact on economic operators and consumers, in particular as regards the provisions on unsolicited communications, taking into account the international environment. For this purpose, the Commission may request information from the Member States, which shall be supplied without undue delay. Where appropriate, the Commission shall submit proposals to amend this Directive, taking account of the results of that report, any changes in the sector and any other proposal it may deem necessary in order to improve the effectiveness of this Directive.

Article 19 Repeal

Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1).

References made to the repealed Directive shall be construed as being made to this Directive.

Article 20 Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 21 Addressees

This Directive is addressed to the Member States.

Done at Brussels, 12 July 2002.

For the European Parliament

The President

P. Cox

For the Council

The President

T. Pedersen

(1) OJ C 365 E, 19.12.2000, p. 223.

(2) OJ C 123, 25.4.2001, p. 53.

(3) Opinion of the European Parliament of 13 November 2001 (not yet published in the Official Journal), Council Common Position of 28 January 2002 (OJ C 113 E, 14.5.2002, p. 39) and Decision of the European Parliament of 30 May 2002 (not yet published in the Official Journal). Council Decision of 25 June 2002.

(4) OJ L 281, 23.11.1995, p. 31.

(5) OJ L 24, 30.1.1998, p. 1.

(6) OJ L 178, 17.7.2000, p. 1.

(7) OJ L 91, 7.4.1999, p. 10.

(8) OJ L 108, 24.4.2002, p. 33.

(9) OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

(10) OJ L 36, 7.2.1987, p. 31. Decision as last amended by the 1994 Act of Accession.

2006/24/EC SAYILI KAMUYA AÇIK HABERLEŞME HİZMETLERİ VEYA KAMU HABERLEŞME ŞEBEKESİ İLE BAĞLANTILI OLARAK ÜRETİLEN VEYA İŞLENEN VERİLERİN SAKLANMASINA İLİŞKİN AVRUPA PARLAMENTOSU VE AVRUPA KONSEYİ DİREKTİF

> *15.03.2006 tarih ve 2006/24/EC sayılı "**Kamuya Açık Haberleşme Hizmetleri veya Kamu Haberleşme Şebekesi ile Bağlantılı Olarak Üretilen veya İşlenen Verilerin Saklanmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi**" için bkz.*
> *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF*
> *(Son erişim tarihi: 16.04.2016)*

2007/228 AVRUPA TOPLULUKLARI KOMİSYONU BİLDİRİSİ

> *02.05.2007 tarih ve 2007/228 sayılı **Avrupa Toplulukları Komisyonu Bildirisi** için bkz.*
> *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52007DC0228*
> *(Son erişim tarihi: 16.04.2016)*

2016 AVRUPA BİRLİĞİ GENEL VERİ KORUMA REGÜLASYONU

Düzenlemenin orijinal ismi: *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**)*

Düzenlemenin künyesi: */* COM/2012/011 final - 2012/0011 (COD) */ Brussels, 6 April 2016 (OR. en) 5419/16 (06.04.2016 tarihinde Avrupa Parlamentosu'nda kabul edilen sürüm. 25 Mayıs 2018 tarihinde yürürlüğe girecektir.)*

Düzenlemenin orijinal metni için:

http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1460910824051&uri=CONSIL:ST_5419_2016_INIT (HTML) (Son erişim tarihi: 16.04.2016)

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&qid=1460910824051&from=EN (PDF) (Son erişim tarihi: 16.04.2016)

BAŞLANGIÇ

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee , Having regard to the opinion of the Committee of the Regions ,

Acting in accordance with the ordinary legislative procedure ,

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council[4] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications,the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with

the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC[5].

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council[6] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial

---

[5] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

[6] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/… of the European Parliament and of the Council[7]. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/… with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.
With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council[8], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether

---

[7] Directive (EU) 2016/… of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (OJ L …).

[8] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools

and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council[9] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing

[9] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of

the data subject prior to entering into a contract.

(41) Where this Regulation refers to a legal basis or a legislative measure , this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union ('Court of Justice') and the European Court of Human Rights.

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC[10] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and

[10] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

man-made disasters.

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the

principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and

cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or

out-of-court procedure.

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including

limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council[11], namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down in constitutional law or international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order

---

[11] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However,

decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated

decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.

(73) Restrictions concerning specific principles and concerning the rights of information, access to and rectification or erasure of personal data and on the right to data portability, the right to object, decisions based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75) The risk to the rights and freedoms of natural persons , of varying likelihood and severity, may result from personal data processing which could lead to physical, material or

non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the

processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or the processor to act on its behalf with regard to their obligations under this Regulation. The designation of such representative does not affect the responsibility and liability of the controller or the processor under this Regulation. Such representative should perform its tasks according to the mandate received from the controller or processor, including to cooperate with the competent supervisory authorities on any action taken in ensuring compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the

subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the stateof the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should

describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

(100) In order to enhance transparency and compliance with this Regulation, the establishment of certification

mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism

of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council[12] as established under this Regulation, to the European Parliament and to the Council.

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative

---

[12] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient

preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment

of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one

Member State and on what constitutes a relevant and reasoned objection.

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorites concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under.

Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation.

The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

(131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise

of its powers under the Treaties.

(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle with a two-third majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded.A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial

remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

(143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concernedwhich wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation.

Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down by Article 263 TFEU.

(144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly

interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council[13] should not prejudice the application of such specific rules.

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriateprocedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for fixing the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory

[13] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

authorities or of other penalties under this Regulation.

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanor procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council[14] leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

(155) Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of

---

[14] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of

the data subject, the general rules of this Regulation should apply in view of those measures.

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council[15] should apply.

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council[16] provides further specifications on statistical confidentiality for European statistics.

(164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.

(165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

(166) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

---

[15] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

[16] Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

(169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

(170) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012[17].

(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council[18], including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,

HAVE ADOPTED THIS REGULATION:

[17] OJ C 192, 30.6.2012, p. 7.

[18] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

CHAPTER I
GENERAL PROVISIONS

Article 1 Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2 Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3 Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4 Definitions

For the purposes of this Regulation:

1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2. 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

4. 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

5. 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

6. 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

7. 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

8. 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

10. 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

11. 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

12. 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

13. 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

14. 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

15. 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

16. 'main establishment' means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

17. 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

18. 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

19. 'group of undertakings' means a controlling undertaking and its controlled undertakings;

20. 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

21. 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

22. 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

23. 'cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

24. 'relevant and reasoned objection' means an objection as to whether there is an infringement of this Regulation or not, or whether the envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

25. 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[19];

26. 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II
PRINCIPLES

Article 5 Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

---

[19] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6 Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair

processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the

Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7 Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8 Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where

the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9 Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data

protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10 Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11 Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III
RIGHTS OF THE DATA SUBJECT

SECTION 1
TRANSPARENCY AND MODALITIES

Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

SECTION 2
INFORMATION AND ACCESS TO PERSONAL DATA

Article 13 Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14 Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, if any, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, where applicable;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing

with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15 Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

SECTION 3
RECTIFICATION AND ERASURE

Article 16 Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her . Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17 Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18 Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Articles 16, 17(1) and 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20 Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

SECTION 4
RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING

Article 21 Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22 Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

SECTION 5
RESTRICTIONS

Article 23 Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12

to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a), (b), (c), (d), (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER IV
CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

Article 24 Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25 Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26 Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union

or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27 Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. This obligation shall not apply to:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

3. The representative shall be established in one of those Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28 Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29 Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30 Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31 Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

SECTION 2
SECURITY OF PERSONAL DATA

Article 32 Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33 Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34 Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

SECTION 3
DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Article 35 Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36 Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

SECTION 4
DATA PROTECTION OFFICER

Article 37 Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38 Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39 Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

SECTION 5
CODES OF CONDUCT AND CERTIFICATION

Article 40 Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41 Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42 Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43 Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council[20] in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with paragraph 1 only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

[20] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30)

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 44 General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45 Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an

international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46 Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of

Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47 Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred under point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48 Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a

Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49 Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Articles 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation pursuant to points (a) to (g) of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph and the second subparagraph of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50 International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 51 Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by … [*two years from the date of entry into force of this Regulation*] at the latest and, without delay, any subsequent amendment affecting them.

Article 52 Independence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53 General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

- their parliament;
- their government;
- their head of State; or
- an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 54 Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

(a) the establishment of each supervisory authority;

(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(c) the rules and procedures for the appointment of the member or members of each supervisory authority;

(d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after … [*the date of entry into force of this Regulation*], part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

SECTION 2
COMPETENCE, TASKS AND POWERS

Article 55 Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of points (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56 Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure

provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57 Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40 and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1, by measures such as a complaint submission form which may also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58 Powers

1. Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Articles 17(2) and 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59 Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2).

Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

CHAPTER VII
COOPERATION AND CONSISTENCY

SECTION 1
COOPERATION

Article 60 Cooperation between the lead supervisory authority and other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion it is not relevant and reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61 Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a requestpursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62 Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff from the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56 (1) or 56(4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

SECTION 2
CONSISTENCY

Article 63 Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64 Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

(a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

(b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

(c) aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);

(d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and Article 28(8);

(e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

(f) aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

(a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

(b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall within two weeks after receiving the opinion, electronically communicate to the Chair of the Board whether it maintains or will amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Article 65 Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-third majority of the members of the Board. This period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published

on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66 Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Articles 64(3) and 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Article 67 Exchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

SECTION 3
EUROPEAN DATA PROTECTION BOARD

Article 68 European Data Protection Board

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.

2. The Board shall be represented by its Chair.

3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.

5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69 Independence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Article 70 Tasks of the Board

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

(a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

(b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17 (2);

(e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

(i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the fixing of administrative fines pursuant to Articles 83;

(l) review the practical application of the guidelines, recommendations and best practices referred to in point (e) and (f);

(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r) provide the Commission with an opinion on the the icons referred to in Article 12(7);

(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation

no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71 Reports

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72 Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The Board shall adopt its own rules of procedure by a two-third majority of its members and organise its own operational arrangements.

Article 73 Chair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Article 74 Tasks of the Chair

1. The Chair shall have the following tasks:

(a) to convene the meetings of the Board and prepare its agenda;

(b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;

(c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Article 75 Secretariat

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.

5. The secretariat shall provide analytical, administrative and logistical support to the Board.

6. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the Board;

(b) communication between the members of the Board, its Chair and the Commission;

(c) communication with other institutions and the public;

(d) the use of electronic means for the internal and external communication;

(e) the translation of relevant information;

(f) the preparation and follow-up of the meetings of the Board;

(g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Article 76 Confidentiality

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council[21].

CHAPTER VIII
REMEDIES, LIABILITY AND PENALTIES

Article 77 Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringment if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78 Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Article 55 and Article 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

---

[21] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79 Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Article 80 Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a

Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Article 81 Suspension of proceedings

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 82 Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83 General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) in case measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringments of the following provisions shall, in acccordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted unter Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in acccordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by … [*two years from the date of entry into force of this Regulation*] and, without delay, any subsequent amendment law or amendment affecting them.

Article 84 Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by … [*two years from the date of entry into force of this Regulation*] and, without delay, any subsequent amendment affecting them.

CHAPTER IX
PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS

Article 85 Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86 Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87 Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88 Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer

of personal data within a group of undertakings, or a group of entreprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by … [*two years from the date of entry into force of this Regulation*] and, without delay, any subsequent amendment affecting them.

Article 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90 Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result ofor has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by … [*two years from the date of entry into force of this Regulation*] and, without delay, any subsequent amendment affecting them.

Article 91 Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X
DELEGATED ACTS AND IMPLEMENTING ACTS

Article 92 Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from … [*the date of entry into force of this Regulation*].

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 93 Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI
FINAL PROVISIONS

Article 94 Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from … [*two years from the date of entry into force of this Regulation*].

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95 Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Article 96 Relationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to … [*the date of entry into force of this Regulation*], and which are in accordance with Union law applicable prior to … [*the date of entry into force of this Regulation*], shall remain in force until amended, replaced or revoked.

Article 97 Commission reports

1. By … [*4 years after the date of entry into force of this Regulation*] and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

(a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

(b) Chapter VII on cooperation and consistency.

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

Article 98 Review of other Union legal acts on data protection

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 99 Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union.*

2. It shall apply from … [*two years from the date of entry into force of this Regulation*].

This Regulation shall be binding in its entirety and directly applicable in all Member States. Done at …,

For the European Parliament	*For the Council*
The President	*The President*

§ TÜRKİYE'DEKİ DÜZENLEMELER

TÜRKİYE CUMHURİYETİ 1982 ANAYASASININ İLGİLİ HÜKÜMLERİ

> ***Künye**: 18.10.1982 tarihli 2709 sayılı Kanun.*
> *(09.11.1982 tarihli 17863 sayılı Mükerrer Resmi Gazete)*
> ***Tam metin için:***
> *http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf 19.03.16*

Madde 20 (A. Özel hayatın gizliliği)

Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Üçüncü cümle mülga: 3/10/2001-4709/5 md.) (Değişik: 3/10/2001-4709/5 md.) Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

Madde 22 (C. Haberleşme hürriyeti)

(Değişik: 3/10/2001-4709/7 md.)

Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

Istisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU

Künye: *24.03.2016 tarihli 6698 sayılı Kanun.*
(07.04.2016 tarihli 29677 sayılı Resmi Gazete)
Mevzuat.gov.tr:
http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf 08.04.2016

BİRİNCİ BÖLÜM
Amaç, Kapsam ve Tanımlar

MADDE 1- Amaç

(1) Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.

MADDE 2- Kapsam

(1) Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.

MADDE 3- Tanımlar

(1) Bu Kanunun uygulanmasında;

a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

b) Anonim hâle getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,

c) Başkan: Kişisel Verileri Koruma Kurumu Başkanını,

ç) İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

f) Kurul: Kişisel Verileri Koruma Kurulunu,

g) Kurum: Kişisel Verileri Koruma Kurumunu,

ğ) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

h) Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

ı) Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ifade eder.

İKİNCİ BÖLÜM
Kişisel Verilerin İşlenmesi

MADDE 4- Genel ilkeler

(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

MADDE 5- Kişisel verilerin işlenme şartları

(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

MADDE 6- Özel nitelikli kişisel verilerin işlenme şartları

(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

MADDE 7- Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi

(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

(2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.

(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.

MADDE 8- Kişisel verilerin aktarılması

(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.

(2) Kişisel veriler;

a) 5 inci maddenin ikinci fıkrasında,

b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında,

belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.

(3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

MADDE 9- Kişisel verilerin yurt dışına aktarılması

(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.

(2) Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;

a) Yeterli korumanın bulunması,

b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması,

kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

(3) Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.

(4) Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine;

a) Türkiye'nin taraf olduğu uluslararası sözleşmeleri,

b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,

c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,

ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,

d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri,

değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.

(5) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.

(6) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

ÜÇÜNCÜ BÖLÜM
Haklar ve Yükümlülükler

MADDE 10- Veri sorumlusunun aydınlatma yükümlülüğü

(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;

a) Veri sorumlusunun ve varsa temsilcisinin kimliği,

b) Kişisel verilerin hangi amaçla işleneceği,

c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,

ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,

d) 11 inci maddede sayılan diğer hakları,

konusunda bilgi vermekle yükümlüdür.

MADDE 11- İlgili kişinin hakları

(1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme,

haklarına sahiptir.

MADDE 12- Veri güvenliğine ilişkin yükümlülükler

(1) Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

(4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

DÖRDÜNCÜ BÖLÜM
Başvuru, Şikâyet ve Veri Sorumluları Sicili

MADDE 13- Veri sorumlusuna başvuru

(1) İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir.

(2) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifedeki ücret alınabilir.

(3) Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusunca gereği yerine getirilir. Başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir.

MADDE 14- Kurula şikâyet

(1) Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir.

(2) 13 üncü madde uyarınca başvuru yolu tüketilmeden şikâyet yoluna başvurulamaz.

(3) Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır.

MADDE 15- Şikâyet üzerine veya resen incelemenin usul ve esasları

(1) Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar.

(2) 1/11/1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde belirtilen şartları taşımayan ihbar veya şikâyetler incelemeye alınmaz.

(3) Devlet sırrı niteliğindeki bilgi ve belgeler hariç; veri sorumlusu, Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır.

(4) Şikâyet üzerine Kurul, talebi inceleyerek ilgililere bir cevap verir. Şikâyet tarihinden itibaren altmış gün içinde cevap verilmezse talep reddedilmiş sayılır.

(5) Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir.

(6) Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin yaygın olduğunun tespit edilmesi hâlinde Kurul, bu konuda ilke kararı alır ve bu kararı yayımlar. Kurul, ilke kararı almadan önce ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşlerini de alabilir.

(7) Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verebilir.

MADDE 16- Veri Sorumluları Sicili

(1) Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulur.

(2) Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.

(3) Veri Sorumluları Siciline kayıt başvurusu aşağıdaki hususları içeren bir bildirimle yapılır:

a) Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri.

b) Kişisel verilerin hangi amaçla işleneceği.

c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar.

ç) Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları.

d) Yabancı ülkelere aktarımı öngörülen kişisel veriler.

e) Kişisel veri güvenliğine ilişkin alınan tedbirler.

f) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

(4) Üçüncü fıkra uyarınca verilen bilgilerde meydana gelen değişiklikler derhâl Başkanlığa bildirilir.

(5) Veri Sorumluları Siciline ilişkin diğer usul ve esaslar yönetmelikle düzenlenir.

BEŞİNCİ BÖLÜM
Suçlar ve Kabahatler

MADDE 17- Suçlar

(1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.

(2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.

MADDE 18- Kabahatler

(1) Bu Kanunun;

a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,

b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,

c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,

ç) 16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar,

idari para cezası verilir.

(2) Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır.

(3) Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir.

ALTINCI BÖLÜM
Kişisel Verileri Koruma Kurumu ve Teşkilat

MADDE 19- Kişisel Verileri Koruma Kurumu

(1) Bu Kanunla verilen görevleri yerine getirmek üzere, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumu kurulmuştur.

(2) Kurum Başbakanlıkla ilişkilidir.

(3) Kurumun merkezi Ankara'dadır.

(4) Kurum, Kurul ve Başkanlıktan oluşur. Kurumun karar organı Kuruldur.

MADDE 20- Kurumun görevleri

(1) Kurumun görevleri şunlardır:

a) Görev alanı itibarıyla, uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak.

b) İhtiyaç duyulması hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak.

c) Kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda uluslararası kuruluşlarla iş birliği yapmak, toplantılara katılmak.

ç) Yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna ve Başbakanlığa sunmak.

d) Kanunlarla verilen diğer görevleri yerine getirmek.

MADDE 21- Kişisel Verileri Koruma Kurulu

(1) Kurul, bu Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz.

(2) Kurul, dokuz üyeden oluşur. Kurulun beş üyesi Türkiye Büyük Millet Meclisi, iki üyesi Cumhurbaşkanı, iki üyesi Bakanlar Kurulu tarafından seçilir.

(3) Kurula üye olabilmek için aşağıdaki şartlar aranır:

a) Kurumun görev alanındaki konularda bilgi ve deneyim sahibi olmak.

b) 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun 48 inci maddesinin birinci fıkrasının (A) bendinin (1), (4), (5), (6) ve (7) numaralı alt bentlerinde belirtilen nitelikleri taşımak.

c) Herhangi bir siyasi parti üyesi olmamak.

ç) En az dört yıllık lisans düzeyinde yükseköğrenim görmüş olmak.

d) Kamu kurum ve kuruluşlarında, uluslararası kuruluşlarda, sivil toplum kuruluşlarında veya kamu kurumu niteliğindeki meslek kuruluşlarında ya da özel sektörde toplamda en az on yıl çalışmış olmak.

(4) Kurul üyeliğine seçileceklerin muvafakatleri aranır. Üye seçiminde, Kurumun görev alanına giren konularda bilgi ve deneyimi bulunanların çoğulcu bir şekilde temsiline özen gösterilir.

(5) Türkiye Büyük Millet Meclisi, Kurula üye seçimini aşağıdaki usulle yapar:

a) Seçim için, siyasi parti gruplarının üye sayısı oranında belirlenecek üye sayısının ikişer katı aday gösterilir ve Kurul üyeleri bu adaylar arasından her siyasi parti grubuna düşen üye sayısı esas alınmak suretiyle Türkiye Büyük Millet Meclisi Genel Kurulunca seçilir. Ancak, siyasi parti gruplarında, Türkiye Büyük Millet Meclisinde yapılacak seçimlerde kime oy kullanılacağına dair görüşme yapılamaz ve karar alınamaz.

b) Kurul üyelerinin seçimi, adayların belirlenerek ilanından sonra on gün içinde yapılır. Siyasi parti grupları tarafından gösterilen adaylar için ayrı ayrı listeler hâlinde birleşik oy pusulası düzenlenir. Adayların adlarının karşısındaki özel yer işaretlenmek suretiyle oy kullanılır. Siyasi parti gruplarının ikinci fıkraya göre belirlenen kontenjanlarından Kurula seçilecek üyelerin sayısından fazla verilen oylar geçersiz sayılır.

c) Karar yeter sayısı olmak şartıyla seçimde en çok oyu alan boş üyelik sayısı kadar aday seçilmiş olur.

ç) Üyelerin görev sürelerinin bitiminden iki ay önce; üyeliklerde herhangi bir sebeple boşalma olması hâlinde, boşalma tarihinden veya boşalma tarihinde Türkiye Büyük Millet Meclisi tatilde ise tatilin bitiminden itibaren bir ay içinde aynı usulle seçim yapılır. Bu seçimlerde, boşalan üyeliklerin siyasi parti gruplarına dağılımı, ilk

seçimde siyasi parti grupları kontenjanından seçilen üye sayısı ve siyasi parti gruplarının hâlihazırdaki oranı dikkate alınmak suretiyle yapılır.

(6) Cumhurbaşkanı veya Bakanlar Kurulu tarafından seçilen üyelerden birinin görev süresinin bitiminden kırk beş gün önce veya herhangi bir sebeple görevin sona ermesi hâlinde durum, on beş gün içinde Kurum tarafından, Cumhurbaşkanlığına veya Bakanlar Kuruluna sunulmak üzere Başbakanlığa bildirilir. Üyelerin görev süresinin dolmasına bir ay kala yeni üye seçimi yapılır. Bu üyeliklerde, görev süresi dolmadan herhangi bir sebeple boşalma olması hâlinde ise bildirimden itibaren on beş gün içinde seçim yapılır.

(7) Kurul, üyeleri arasından Başkan ve İkinci Başkanı seçer. Kurulun Başkanı, Kurumun da başkanıdır.

(8) Kurul üyelerinin görev süresi dört yıldır. Süresi biten üye yeniden seçilebilir. Görev süresi dolmadan herhangi bir sebeple görevi sona eren üyenin yerine seçilen kişi, yerine seçildiği üyenin kalan süresini tamamlar.

(9) Seçilen üyeler Yargıtay Birinci Başkanlık Kurulu huzurunda "Görevimi Anayasaya ve kanunlara uygun olarak, tam bir tarafsızlık, dürüstlük, hakkaniyet ve adalet anlayışı içinde yerine getireceğime, namusum ve şerefim üzerine yemin ederim." şeklinde yemin ederler. Yargıtaya yemin için yapılan başvuru acele işlerden sayılır.

(10) Kurul üyeleri özel bir kanuna dayanmadıkça, Kuruldaki resmî görevlerinin yürütülmesi dışında resmî veya özel hiçbir görev alamaz, dernek, vakıf, kooperatif ve benzeri yerlerde yöneticilik yapamaz, ticaretle uğraşamaz, serbest meslek faaliyetinde bulunamaz, hakemlik ve bilirkişilik yapamazlar. Ancak, Kurul üyeleri, asli görevlerini aksatmayacak şekilde bilimsel amaçlı yayın yapabilir, ders ve konferans verebilir ve bunlardan doğacak telif hakları ile ders ve konferans ücretlerini alabilirler.

(11) Üyelerin görevleri sebebiyle işledikleri iddia edilen suçlara ilişkin soruşturmalar 2/12/1999 tarihli ve 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanuna göre yapılır ve bunlar hakkında soruşturma izni Başbakan tarafından verilir.

(12) Kurul üyeleri hakkında yapılacak disiplin soruşturması ve kovuşturmasında 657 sayılı Kanun hükümleri uygulanır.

(13) Kurul üyelerinin süreleri dolmadan herhangi bir nedenle görevlerine son verilemez. Kurul üyelerinin;

a) Seçilmek için gereken şartları taşımadıklarının sonradan anlaşılması,

b) Görevleriyle ilgili olarak işledikleri suçlardan dolayı haklarında verilen mahkûmiyet kararının kesinleşmesi,

c) Görevlerini yerine getiremeyeceklerinin sağlık kurulu raporuyla kesin olarak tespit edilmesi,

ç) Görevlerine izinsiz, mazeretsiz ve kesintisiz olarak on beş gün ya da bir yılda toplam otuz gün süreyle devam etmediklerinin tespit edilmesi,

d) Bir ay içinde izinsiz ve mazeretsiz olarak toplam üç, bir yıl içinde toplam on Kurul toplantısına katılmadıklarının tespit edilmesi,

hâllerinde Kurul kararıyla üyelikleri sona erer.

(14) Kurul üyeliğine seçilenlerin Kurulda görev yaptıkları sürece önceki görevleri ile olan ilişikleri kesilir. Kamu görevlisi iken üyeliğe seçilenler, memuriyete giriş şartlarını kaybetmemeleri kaydıyla, görev sürelerinin sona ermesi veya görevden ayrılma isteğinde bulunmaları ve otuz gün içinde eski kurumlarına başvurmaları durumunda atamaya yetkili makam tarafından bir ay içinde mükteseplerine uygun bir kadroya atanır. Atama gerçekleşinceye kadar, bunların almakta oldukları her türlü ödemelerin Kurum tarafından ödenmesine devam olunur. Bir kamu kurumunda çalışmayanlardan üyeliğe seçilip yukarıda belirtilen şekilde görevi sona erenlere herhangi bir görev veya işe başlayıncaya kadar, almakta oldukları her türlü ödemeler Kurum tarafından ödenmeye devam edilir ve bu şekilde üyeliği sona erenlere Kurum tarafından yapılacak ödeme üç ayı geçemez. Bunların Kurumda geçirdiği süreler, özlük ve diğer hakları açısından önceki kurum veya kuruluşlarında geçirilmiş sayılır.

MADDE 22- Kurulun görev ve yetkileri

(1) Kurulun görev ve yetkileri şunlardır:

a) Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak.

b) Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak.

c) Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak.

ç) Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek.

d) Veri Sorumluları Sicilinin tutulmasını sağlamak.

e) Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak.

f) Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak.

g) Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak.

ğ) Bu Kanunda öngörülen idari yaptırımlara karar vermek.

h) Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek.

ı) Kurumun; stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemek.

i) Kurumun stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamak.

j) Kurumun performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında hazırlanan rapor taslaklarını onaylamak ve yayımlamak.

k) Taşınmaz alımı, satımı ve kiralanması konularındaki önerileri görüşüp karara bağlamak.

l) Kanunlarla verilen diğer görevleri yerine getirmek.

MADDE 23- Kurulun çalışma esasları

(1) Kurulun toplantı günlerini ve gündemini Başkan belirler. Başkan gereken hâllerde Kurulu olağanüstü toplantıya çağırabilir.

(2) Kurul, başkan dâhil en az altı üye ile toplanır ve üye tam sayısının salt çoğunluğuyla karar alır. Kurul üyeleri çekimser oy kullanamaz.

(3) Kurul üyeleri; kendilerini, üçüncü dereceye kadar kan ve ikinci dereceye kadar kayın hısımlarını, evlatlıklarını ve aralarındaki evlilik bağı kalkmış olsa bile eşlerini ilgilendiren konularla ilgili toplantı ve oylamaya katılamaz.

(4) Kurul üyeleri çalışmaları sırasında ilgililere ve üçüncü kişilere ait öğrendikleri sırları bu konuda kanunen yetkili kılınan mercilerden başkasına açıklayamazlar ve kendi yararlarına kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) Kurulda görüşülen işler tutanağa bağlanır. Kararlar ve varsa karşı oy gerekçeleri karar tarihinden itibaren en geç on beş gün içinde yazılır. Kurul, gerekli gördüğü kararları kamuoyuna duyurur.

(6) Aksi kararlaştırılmadıkça, Kurul toplantılarındaki görüşmeler gizlidir.

(7) Kurulun çalışma usul ve esasları ile kararların yazımı ve diğer hususlar yönetmelikle düzenlenir.

MADDE 24- Başkan

(1) Başkan, Kurul ve Kurumun başkanı sıfatıyla Kurumun en üst amiri olup Kurum hizmetlerini mevzuata, Kurumun amaç ve politikalarına, stratejik planına, performans ölçütlerine ve hizmet kalite standartlarına uygun olarak düzenler, yürütür ve hizmet birimleri arasında koordinasyonu sağlar.

(2) Başkan, Kurumun genel yönetim ve temsilinden sorumludur. Bu sorumluluk, Kurum çalışmalarının düzenlenmesi, yürütülmesi, denetlenmesi, değerlendirilmesi ve gerektiğinde kamuoyuna duyurulması görev ve yetkilerini kapsar.

(3) Başkanın görevleri şunlardır:

a) Kurul toplantılarını idare etmek.

b) Kurul kararlarının tebliğini ve Kurulca gerekli görülenlerin kamuoyuna duyurulmasını sağlamak ve uygulanmalarını izlemek.

c) Başkan Yardımcısını, daire başkanlarını ve Kurum personelini atamak.

ç) Hizmet birimlerinden gelen önerilere son şeklini vererek Kurula sunmak.

d) Stratejik planın uygulanmasını sağlamak, hizmet kalite standartları doğrultusunda insan kaynakları ve çalışma politikalarını oluşturmak.

e) Belirlenen stratejilere, yıllık amaç ve hedeflere uygun olarak Kurumun yıllık bütçesi ile mali tablolarını hazırlamak.

f) Kurul ve hizmet birimlerinin uyumlu, verimli, disiplinli ve düzenli bir biçimde çalışması amacıyla koordinasyonu sağlamak.

g) Kurumun diğer kuruluşlarla ilişkilerini yürütmek.

ğ) Kurum Başkanı adına imzaya yetkili personelin görev ve yetki alanını belirlemek.

h) Kurumun yönetim ve işleyişine ilişkin diğer görevleri yerine getirmek.

(4) Kurum Başkanının yokluğunda İkinci Başkan, Başkana vekalet eder.

MADDE 25- Başkanlığın oluşumu ve görevleri

(1) Başkanlık; Başkan Yardımcısı ve hizmet birimlerinden oluşur. Başkanlık, dördüncü fıkrada sayılan görevleri daire başkanlıkları şeklinde teşkilatlanan hizmet birimleri aracılığıyla yerine getirir. Daire başkanlıklarının sayısı yediyi geçemez.

(2) Başkan tarafından, Kuruma ilişkin görevlerinde yardımcı olmak üzere bir Başkan Yardımcısı atanır.

(3) Başkan Yardımcısı ve daire başkanları; en az dört yıllık yükseköğretim kurumu mezunu, on yıl süreyle kamu hizmetinde bulunan kişiler arasından Başkan tarafından atanır.

(4) Başkanlığın görevleri şunlardır:

a) Veri Sorumluları Sicilini tutmak.

b) Kurumun ve Kurulun büro ve sekretarya işlemlerini yürütmek.

c) Kurumun taraf olduğu davalar ile icra takiplerinde avukatlar vasıtasıyla Kurumu temsil etmek, davaları takip etmek veya ettirmek, hukuk hizmetlerini yürütmek.

ç) Kurul üyeleri ile Kurumda görev yapanların özlük işlemlerini yürütmek.

d) Kanunlarla mali hizmet ve strateji geliştirme birimlerine verilen görevleri yapmak.

e) Kurumun iş ve işlemlerinin yürütülmesi amacıyla bilişim sisteminin kurulmasını ve kullanılmasını sağlamak.

f) Kurulun yıllık faaliyetleri hakkında veya ihtiyaç duyulan konularda rapor taslaklarını hazırlamak ve Kurula sunmak.

g) Kurumun stratejik plan taslağını hazırlamak.

ğ) Kurumun personel politikasını belirlemek, personelin kariyer ve eğitim planlarını hazırlamak ve uygulamak.

h) Personelin atama, nakil, disiplin, performans, terfi, emeklilik ve benzeri işlemlerini yürütmek.

ı) Personelin uyacağı etik kuralları belirlemek ve gerekli eğitimi vermek.

i) 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanunu çerçevesinde Kurumun ihtiyacı olan her türlü satın alma, kiralama, bakım, onarım, yapım, arşiv, sağlık, sosyal ve benzeri hizmetleri yürütmek.

j) Kuruma ait taşınır ve taşınmazların kayıtlarını tutmak.

k) Kurul veya Başkan tarafından verilen diğer görevleri yapmak.

(5) Hizmet birimleri ile bu birimlerin çalışma usul ve esasları, bu Kanunda belirtilen faaliyet alanı, görev ve yetkilere uygun olarak Kurumun teklifi üzerine Bakanlar Kurulu kararıyla yürürlüğe konulan yönetmelikle belirlenir.

MADDE 26- Kişisel Verileri Koruma Uzmanı ve uzman yardımcıları

(1) Kurumda, Kişisel Verileri Koruma Uzmanı ve Kişisel Verileri Koruma Uzman Yardımcısı istihdam edilebilir. Bunlardan 657 sayılı Kanunun ek 41 inci maddesi çerçevesinde Kişisel Verileri Koruma Uzmanı kadrosuna atananlara bir defaya mahsus olmak üzere bir derece yükseltilmesi uygulanır.

MADDE 27- Personele ve özlük haklarına ilişkin hükümler

(1) Kurum personeli, bu Kanunla düzenlenen hususlar dışında 657 sayılı Kanuna tabidir.

(2) Kurul Başkan ve üyeleri ile Kurum personeline 27/6/1989 tarihli ve 375 sayılı Kanun Hükmünde Kararnamenin ek 11 inci maddesi uyarınca belirlenmiş emsali personele mali ve sosyal haklar kapsamında yapılan ödemeler aynı usul ve esaslar çerçevesinde ödenir. Emsali personele yapılan ödemelerden vergi ve diğer yasal kesintilere tabi olmayanlar bu Kanuna göre de vergi ve diğer kesintilere tabi olmaz.

(3) Kurul Başkan ve üyeleri ile Kurum personeli 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 4 üncü maddesinin birinci fıkrasının (c) bendi hükümlerine tabidir. Kurul Başkan ve üyeleri ile Kurum personeli emeklilik hakları bakımından da emsali olarak belirlenen personel ile denk kabul edilir. 5510 sayılı Kanunun 4 üncü maddesinin birinci fıkrasının (c) bendi kapsamında sigortalı iken Kurul Başkanı ve üyeliklerine atananlardan bu görevleri sona erenler veya bu görevlerinden ayrılma isteğinde bulunanların bu görevlerde geçen hizmet süreleri kazanılmış hak aylık, derece ve kademelerinin tespitinde dikkate alınır. Bunlardan bu görevleri sırasında 5510 sayılı Kanunun geçici 4 üncü maddesi kapsamına girenlerin bu görevlerde geçen süreleri makam tazminatı ile temsil tazminatı ödenmesi gereken süre olarak değerlendirilir. Kamu kurum ve kuruluşlarında 5510 sayılı Kanunun 4 üncü maddesinin birinci fıkrasının (a) bendi kapsamında sigortalı iken Kurul Başkanı ve üyeliklerine atananların, önceki kurum ve kuruluşları ile ilişiklerinin kesilmesi kendilerine kıdem tazminatı veya iş sonu tazminatı ödenmesini gerektirmez. Bu durumda olanların kıdem tazminatı veya iş sonu tazminatı ödenmesi gereken hizmet süreleri, Kurul Başkanı ile Kurul üyeliği olarak geçen hizmet süreleri ile birleştirilir ve emeklilik ikramiyesi ödenecek süre olarak değerlendirilir.

(4) Merkezi yönetim kapsamındaki kamu idarelerinde, sosyal güvenlik kurumlarında, mahallî idarelerde, mahallî idarelere bağlı idarelerde, mahallî idare birliklerinde, döner sermayeli kuruluşlarda, kanunlarla kurulan fonlarda, kamu tüzel kişiliğini haiz kuruluşlarda, sermayesinin yüzde ellisinden fazlası kamuya ait kuruluşlarda, iktisadi devlet teşekkülleri ve kamu iktisadi kuruluşları ile bunlara bağlı ortaklıklar ve müesseselerde görevli memurlar ile diğer kamu görevlileri kurumlarının muvafakati ile aylık, ödenek, her türlü zam ve tazminatlar ile diğer mali ve sosyal hak ve yardımları kurumlarınca ödenmek kaydıyla geçici olarak Kurumda görevlendirilebilir. Kurumun bu konudaki talepleri, ilgili kurum ve kuruluşlarca öncelikle sonuçlandırılır. Bu şekilde görevlendirilen personel, kurumlarından aylıklı izinli sayılır. Bu personelin izinli oldukları sürece memuriyetleri ile ilgileri ve özlük hakları devam ettiği gibi, bu süreler yükselme ve emekliliklerinde de hesaba katılır ve yükselmeleri başkaca bir işleme gerek duyulmadan süresinde yapılır. Bu madde kapsamında görevlendirilenlerin, Kurumda geçirdikleri süreler, kendi kurumlarında geçirilmiş sayılır. Bu şekilde görevlendirilenlerin sayısı Kişisel Verileri Koruma Uzmanı ve

Kişisel Verileri Koruma Uzman Yardımcısı toplam kadro sayısının yüzde onunu aşamaz ve görevlendirme süresi iki yılı geçemez. Ancak ihtiyaç hâlinde bu süre bir yıllık dönemler hâlinde uzatılabilir.

(5) Kurumda istihdam edilecek personele ilişkin kadro unvan ve sayıları ekli (I) sayılı cetvelde gösterilmiştir. Toplam kadro sayısını geçmemek üzere 13/12/1983 tarihli ve 190 sayılı Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kararnamenin eki cetvellerde yer alan kadro unvanlarıyla sınırlı olmak kaydıyla unvan ve derece değişikliği yapma, yeni unvan ekleme ve boş kadroların iptali Kurul kararıyla yapılır.

YEDİNCİ BÖLÜM
Çeşitli Hükümler

MADDE 28- İstisnalar

(1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.

b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

(2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.

b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.

c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

MADDE 29- Kurumun bütçesi ve gelirleri

(1) Kurumun bütçesi, 5018 sayılı Kanunda belirlenen usul ve esaslara göre hazırlanır ve kabul edilir.

(2) Kurumun gelirleri şunlardır:

a) Genel bütçeden yapılacak hazine yardımları.

b) Kuruma ait taşınır ve taşınmazlardan elde edilen gelirler.

c) Alınan bağış ve yardımlar.

ç) Gelirlerinin değerlendirilmesinden elde edilen gelirler.

d) Diğer gelirler.

MADDE 30- Değiştirilen ve eklenen hükümler

(1) 5018 sayılı Kanunun eki (III) sayılı Cetvele aşağıdaki sıra eklenmiştir.

"10) Kişisel Verileri Koruma Kurumu"

(2) 5237 sayılı Kanunun 135 inci maddesinin ikinci fıkrasında yer alan "Kişilerin" ibaresi "Kişisel verinin, kişilerin" şeklinde; "bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır" ibaresi "olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır" şeklinde değiştirilmiştir.

(3) 5237 sayılı Kanunun 226 ncı maddesinin üçüncü fıkrasında yer alan "çocukları" ibaresi "çocukları, temsili çocuk görüntülerini veya çocuk gibi görünen kişileri" şeklinde değiştirilmiştir.

(4) 5237 sayılı Kanunun 243 üncü maddesinin birinci fıkrasında yer alan "ve" ibaresi "veya" şeklinde değiştirilmiş ve maddeye aşağıdaki fıkra eklenmiştir.

"(4) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."

(5) 5237 sayılı Kanuna 245 inci maddeden sonra gelmek üzere aşağıdaki 245/A maddesi eklenmiştir.

"Yasak cihaz veya programlar

MADDE 245/A- (1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır."

(6) 7/5/1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanununun 3 üncü maddesinin birinci fıkrasının (f) bendi aşağıdaki şekilde değiştirilmiştir.

“f) Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Sağlık Bakanlığı ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla, Sağlık Bakanlığınca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabilir.”

(7) 11/10/2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 47 nci maddesi aşağıdaki şekilde değiştirilmiştir.

“MADDE 47- (1) Sağlık hizmeti almak üzere, kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verileri işlenebilir.

(2) Sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlık, birinci fıkra kapsamında elde edilen verileri alarak işleyebilir. Bu veriler, Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamaz.

(3) Bakanlık, ikinci fıkra gereğince toplanan ve işlenen kişisel verilere, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistem kurar.

(4) Üçüncü fıkraya göre kurulan sistemlerin güvenliği ve güvenilirliği ile ilgili standartlar Kişisel Verileri Koruma Kurulunun belirlediği ilkelere uygun olarak Bakanlıkça belirlenir. Bakanlık, bu Kanun uyarınca elde edilen kişisel sağlık verilerinin güvenliğinin sağlanması için gerekli tedbirleri alır. Bu amaçla, sistemde kayıtlı bilgilerin hangi görevli tarafından ne amaçla kullanıldığının denetlenmesine imkân tanıyan bir güvenlik sistemi kurar.

(5) Sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişiler, istihdam ettiği personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlüdür.

(6) Kişisel sağlık verilerinin işlenmesi, güvenliği ve bu maddenin uygulanması ile ilgili diğer hususlar Bakanlıkça yürürlüğe konulan yönetmelikle düzenlenir.”

MADDE 31- Yönetmelik

(1) Bu Kanunun uygulanmasına ilişkin yönetmelikler Kurum tarafından yürürlüğe konulur.

GEÇİCİ MADDE 1- Geçiş hükümleri

(1) Bu Kanunun yayımı tarihinden itibaren altı ay içinde 21 inci maddede öngörülen usule göre Kurul üyeleri seçilir ve Başkanlık teşkilatı oluşturulur.

(2) Veri sorumluları, Kurul tarafından belirlenen ve ilan edilen süre içinde Veri Sorumluları Siciline kayıt yaptırmak zorundadır.

(3) Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir. Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhâl silinir, yok edilir veya anonim hâle getirilir. Ancak bu Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması hâlinde, bu Kanuna uygun kabul edilir.

(4) Bu Kanunda öngörülen yönetmelikler bu Kanunun yayımı tarihinden itibaren bir yıl içinde yürürlüğe konulur.

(5) Bu Kanunun yayımı tarihinden itibaren bir yıl içinde, kamu kurum ve kuruluşlarında bu Kanunun uygulanmasıyla ilgili koordinasyonu sağlamak üzere üst düzey bir yönetici belirlenerek Başkanlığa bildirilir.

(6) İlk seçilen Başkan, İkinci Başkan ve kura ile belirlenen iki üye altı yıl; diğer beş üye ise dört yıl görev yapar.

(7) Kuruma bütçe tahsis edilene kadar;

a) Kurumun giderleri Başbakanlık bütçesinden karşılanır.

b) Kurumun hizmetlerini yerine getirmesi amacıyla bina, araç, gereç, mefruşat ve donanım gibi gerekli tüm destek hizmetleri Başbakanlıkça sağlanır.

(8) Kurumun hizmet birimleri faaliyete geçinceye kadar sekretarya hizmetleri Başbakanlık tarafından yerine getirilir.

MADDE 32- Yürürlük

(1) Bu Kanunun;

a) 8 inci, 9 uncu, 11 inci, 13 üncü, 14 üncü, 15 inci, 16 ncı, 17 nci ve 18 inci maddeleri yayımı tarihinden altı ay sonra,

b) Diğer maddeleri ise yayımı tarihinde,

yürürlüğe girer.

MADDE 33- Yürütme

(1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

(I) SAYILI CETVEL KİŞİSEL VERİLERİ KORUMA KURUMU KADRO LİSTESİ

SINIF	UNVAN	DERECE	TOPLAM
GİH	Başkan Yardımcısı	1	1
GİH	Daire Başkanı	1	7
GİH	Hukuk Müşaviri	1	1
GİH	Hukuk Müşaviri	3	3
AH	Avukat	6	4
GİH	Kişisel Verileri Koruma Uzmanı	5	10

GİH	Kişisel Verileri Koruma Uzmanı	7	20
GİH	Kişisel Verileri Koruma Uzman Yardımcısı	9	60
GİH	Mali Hizmetler Uzmanı	6	2
GİH	Mali Hizmetler Uzman Yardımcısı	9	2
GİH	Memur	5	5
GİH	Memur	7	5
GİH	Memur	9	5
GİH	Memur	11	5
GİH	Memur	13	5
GİH	Bilgisayar İşletmeni	7	5
GİH	Veri Hazırlama ve Kontrol İşletmeni	6	5
GİH	Veri Hazırlama ve Kontrol İşletmeni	7	5
GİH	Veri Hazırlama ve Kontrol İşletmeni	8	5
GİH	Veri Hazırlama ve Kontrol İşletmeni	9	5
GİH	Veri Hazırlama ve Kontrol İşletmeni	10	5
GİH	Sekreter	5	3
GİH	Sekreter	8	7
GİH	Santral Memuru	9	1
GİH	Şoför	11	4
TH	Teknisyen	6	3
YH	Teknisyen Yardımcısı	9	2
YH	Hizmetli	11	10
	TOPLAM		**195**

4721 SAYILI TÜRK MEDENİ KANUNU'NUN KİŞİSEL VERİLERİN KORUNMASIYLA İLGİLİ HÜKÜMLERİ

> ***Künye:*** *22.11.2001 tarihli 4721 sayılı Kanun.*
> *(08.12.2001 tarihli 24607 sayılı Resmi Gazete)*
> ***Tam metin için:***
> *http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf 19.03.16*

Madde 23 (I. Vazgeçme ve aşırı sınırlamaya karşı B. Kişiliğin korunması)

Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez.

Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlâka aykırı olarak sınırlayamaz.

Yazılı rıza üzerine insan kökenli biyolojik Maddelerin alınması, aşılanması ve nakli mümkündür. Ancak, biyolojik Madde verme borcu altına girmiş olandan edimini yerine getirmesi istenemez; maddî ve manevî tazminat isteminde bulunulamaz.

Madde 24 (1. İlke II. Saldırıya karşı B. Kişiliğin Korunması)

Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.

Madde 25 (2. Davalar)

Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.

Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir.

Davacının, maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır.

Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; mirasbırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez.

Davacı, kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yeri mahkemesinde dava açabilir.

Madde 26 (1. Adın korunması III. Ad üzerindeki hak)

Adının kullanılması çekişmeli olan kişi, hakkının tespitini dava edebilir.

Adı haksız olarak kullanılan kişi buna son verilmesini; haksız kullanan kusurlu ise ayrıca maddî zararının giderilmesini ve uğradığı haksızlığın niteliği gerektiriyorsa manevî tazminat ödenmesini isteyebilir.

Madde 27 (2. Adın değiştirilmesi)

Adın değiştirilmesi, ancak haklı sebeplere dayanılarak hâkimden istenebilir.

Adın değiştirildiği nüfus siciline kayıt ve ilân olunur.

Ad değişmekle kişisel durum değişmez.

Adın değiştirilmesinden zarar gören kimse, bunu öğrendiği günden başlayarak bir yıl içinde değiştirme kararının kaldırılmasını dava edebilir.

4857 SAYILI İŞ KANUNU'NUN İLGİLİ HÜKÜMLERİ

> ***Künye**: 22.05.2003 tarihli 2709 sayılı Kanun.*
> *(10.06.2003 tarihli 25134 sayılı Resmi Gazete)*
> ***Tam metin için:***
> *http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4857.pdf 19.03.16*

Madde 75 (İşçi özlük dosyası)

İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.

İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür.

4982 SAYILI BİLGİ EDİNME HAKKI KANUNU

Künye: *09.10.2003 tarihli 4982 sayılı Kanun.*
(24/10/2003 tarihli 25269 sayılı Resmi Gazete)
Tam metin için:
http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4982.pdf 19.03.16

BİRİNCİ BÖLÜM
Amaç, Kapsam ve Tanımlar

Madde 1- Amaç

Bu Kanunun amacı; demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak kişilerin bilgi edinme hakkını kullanmalarına ilişkin esas ve usulleri düzenlemektir.

Madde 2- Kapsam

Bu Kanun; kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinde uygulanır.

1.11.1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun hükümleri saklıdır.

(Ek fıkra: 12/7/2013-6495/33 md.; İptal fıkra: Anayasa Mahkemesi'nin 4/12/2014 tarihli ve E.:2013/114, K.:2014/184 sayılı Kararı ile.)

Madde 3- Tanımlar

Bu Kanunda geçen;

a) Kurum ve kuruluş: Bu Kanunun 2 nci maddesinde geçen ve kapsama dahil olan bilgi edinme başvurusu yapılacak bütün makam ve mercileri,

b) Başvuru sahibi: Bu Kanun kapsamında bilgi edinme hakkını kullanarak kurum ve kuruluşlara başvuran gerçek ve tüzel kişileri,

c) Bilgi: Kurum ve kuruluşların sahip oldukları kayıtlarda yer alan bu Kanun kapsamındaki her türlü veriyi,

d) Belge: Kurum ve kuruluşların sahip oldukları bu Kanun kapsamındaki yazılı, basılı veya çoğaltılmış dosya, evrak, kitap, dergi, broşür, etüt, mektup, program, talimat, kroki, plân, film, fotoğraf, teyp ve video kaseti, harita, elektronik ortamda kaydedilen her türlü bilgi, haber ve veri taşıyıcılarını,

e) Bilgi veya belgeye erişim: İstenen bilgi veya belgenin niteliğine göre, kurum ve kuruluşlarca, başvuru sahibine söz konusu bilgi veya belgenin bir kopyasının verilmesini, kopya verilmesinin mümkün olmadığı hâllerde, başvuru sahibinin bilgi veya belgenin aslını inceleyerek not almasına veya içeriğini görmesine veya işitmesine izin verilmesini,

f) Kurul: Bilgi Edinme Değerlendirme Kurulunu,

İfade eder.

İKİNCİ BÖLÜM
Bilgi Edinme Hakkı ve Bilgi Verme Yükümlülüğü

Madde 4- Bilgi edinme hakkı

Herkes bilgi edinme hakkına sahiptir.

Türkiye'de ikamet eden yabancılar ile Türkiye'de faaliyette bulunan yabancı tüzel kişiler, isteyecekleri bilgi kendileriyle veya faaliyet alanlarıyla ilgili olmak kaydıyla ve karşılıklılık ilkesi çerçevesinde, bu Kanun hükümlerinden yararlanırlar.

Türkiye'nin taraf olduğu uluslararası sözleşmelerden doğan hak ve yükümlülükleri saklıdır.

Madde 5- Bilgi verme yükümlülüğü

Kurum ve kuruluşlar, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idarî ve teknik tedbirleri almakla yükümlüdürler.

Bu Kanun yürürlüğe girdiği tarihten itibaren diğer kanunların bu Kanuna aykırı hükümleri uygulanmaz.

ÜÇÜNCÜ BÖLÜM
Bilgi Edinme Başvurusu

Madde 6- Başvuru usulü

Bilgi edinme başvurusu, başvuru sahibinin adı ve soyadı, imzası, oturma yeri veya iş adresini, başvuru sahibi tüzel kişi ise tüzel kişinin unvanı ve adresi ile yetkili kişinin imzasını ve yetki belgesini içeren dilekçe ile istenen bilgi veya belgenin bulunduğu kurum veya kuruluşa yapılır. Bu başvuru, kişinin kimliğinin ve imzasının veya yazının kimden neşet ettiğinin tespitine yarayacak başka bilgilerin yasal olarak belirlenebilir olması kaydıyla elektronik ortamda veya diğer iletişim araçlarıyla da yapılabilir.

Dilekçede, istenen bilgi veya belgeler açıkça belirtilir.

Madde 7- İstenecek bilgi veya belgenin niteliği

Bilgi edinme başvurusu, başvurulan kurum ve kuruluşların ellerinde bulunan veya görevleri gereği bulunması gereken bilgi veya belgelere ilişkin olmalıdır.

Kurum ve kuruluşlar, ayrı veya özel bir çalışma, araştırma, inceleme ya da analiz neticesinde oluşturulabilecek türden bir bilgi veya belge için yapılacak başvurulara olumsuz cevap verebilirler.

İstenen bilgi veya belge, başvurulan kurum ve kuruluştan başka bir yerde bulunuyorsa, başvuru dilekçesi bu kurum ve kuruluşa gönderilir ve durum ilgiliye yazılı olarak bildirilir.

Madde 8- Yayımlanmış veya kamuya açıklanmış bilgi veya belgeler

Kurum ve kuruluşlarca yayımlanmış veya yayın, broşür, ilân ve benzeri yollarla kamuya açıklanmış bilgi veya belgeler, bilgi edinme başvurularına konu olamaz. Ancak, yayımlanmış veya kamuya açıklanmış bilgi veya belgelerin ne şekilde, ne zaman ve nerede yayımlandığı veya açıklandığı başvurana bildirilir.

Madde 9- Gizli bilgileri ayırarak bilgi veya belge verme

İstenen bilgi veya belgelerde, gizlilik dereceli veya açıklanması yasaklanan bilgiler ile açıklanabilir nitelikte olanlar birlikte bulunuyor ve bunlar birbirlerinden ayrılabiliyorsa, söz konusu bilgi veya belge, gizlilik dereceli veya açıklanması yasaklanan bilgiler çıkarıldıktan sonra başvuranın bilgisine sunulur. Ayırma gerekçesi başvurana yazılı olarak bildirilir.

Madde 10- Bilgi veya belgeye erişim

Kurum ve kuruluşlar, başvuru sahibine istenen belgenin onaylı bir kopyasını verirler.

Bilgi veya belgenin niteliği gereği kopyasının verilmesinin mümkün olmadığı veya kopya çıkarılmasının aslına zarar vereceği hâllerde, kurum ve kuruluşlar ilgilinin;

a) Yazılı veya basılı belgeler için, söz konusu belgenin aslını incelemesi ve not alabilmesini,

b) Ses kaydı şeklindeki bilgi veya belgelerde bunları dinleyebilmesini,

c) Görüntü kaydı şeklindeki bilgi veya belgelerde bunları izleyebilmesini,

Sağlarlar.

Bilgi veya belgenin yukarıda belirtilenlerden farklı bir şekilde elde edilmesi mümkün ise, belgeye zarar vermemek koşuluyla bu olanak sağlanır.

Başvurunun yapıldığı kurum ve kuruluş, erişimine olanak sağladığı bilgi veya belgeler için başvuru sahibinden erişimin gerektirdiği maliyet tutarı kadar bir ücreti bütçeye gelir kaydedilmek üzere tahsil edebilir.

Madde 11- Bilgi veya belgeye erişim süreleri

Kurum ve kuruluşlar, başvuru üzerine istenen bilgi veya belgeye erişimi onbeş iş günü içinde sağlarlar. Ancak istenen bilgi veya belgenin, başvurulan kurum ve kuruluş içindeki başka bir birimden sağlanması; başvuru ile ilgili olarak bir başka kurum ve kuruluşun görüşünün alınmasının gerekmesi veya başvuru içeriğinin birden fazla kurum ve kuruluşu ilgilendirmesi durumlarında bilgi veya belgeye erişim otuz iş günü içinde sağlanır. Bu durumda, sürenin uzatılması ve bunun gerekçesi başvuru sahibine yazılı olarak ve onbeş iş günlük sürenin bitiminden önce bildirilir.

10 uncu maddede belirtilen bilgi veya belgelere erişim için gereken maliyet tutarının idare tarafından başvuru sahibine bildirilmesiyle onbeş iş günlük süre kesilir. Başvuru sahibi onbeş iş günü içinde ücreti ödemezse talebinden vazgeçmiş sayılır.

Madde 12- Başvuruların cevaplandırılması

Kurum ve kuruluşlar, bilgi edinme başvurularıyla ilgili cevaplarını yazılı olarak veya elektronik ortamda başvuru sahibine bildirirler. Başvurunun reddedilmesi hâlinde bu kararın gerekçesi ve buna karşı başvuru yolları belirtilir.

Madde 13- İtiraz usulü

Bilgi edinme istemi (…)[22]reddedilen başvuru sahibi, yargı yoluna başvurmadan önce kararın tebliğinden itibaren onbeş gün içinde Kurula itiraz edebilir. Kurul, bu konudaki kararını otuz iş günü içinde verir. Kurum ve kuruluşlar, Kurulun istediği her türlü bilgi veya belgeyi onbeş iş günü içinde vermekle yükümlüdürler.

Kurula itiraz, başvuru sahibinin idarî yargıya başvurma süresini durdurur.

Madde 14- Bilgi Edinme Değerlendirme Kurulu

Bilgi edinme başvurusuyla ilgili yapılacak itirazlar üzerine, (…)[23] verilen kararları incelemek ve kurum ve kuruluşlar için bilgi edinme hakkının kullanılmasına ilişkin olarak kararlar vermek üzere; Bilgi Edinme Değerlendirme Kurulu oluşturulmuştur.

Kurul; birer üyesi Yargıtay ve Danıştay genel kurullarının kendi kurumları içinden önerecekleri ikişer aday, birer üyesi ceza hukuku, idare hukuku ve anayasa hukuku alanlarında profesör veya doçent unvanına sahip kişiler, bir üyesi Türkiye Barolar Birliğinin baro başkanı seçilme yeterliliğine sahip kişiler içinden göstereceği iki aday, iki üyesi en az genel müdür düzeyinde görev yapmakta olanlar ve bir üyesi de Adalet Bakanının önerisi üzerine bu Bakanlıkta idarî görevlerde çalışan hâkimler arasından Bakanlar Kurulunca seçilecek dokuz üyeden oluşur.

Kurul üyeliğine önerilen adayların muvafakatları aranır.

Kurul Başkanı, kurul üyelerince kendi aralarından seçilir.

Kurul, en az ayda bir defa veya ihtiyaç duyulduğu her zaman Başkanın çağrısı üzerine toplanır.

Kurul üyelerinin görev süreleri dört yıldır. Görev süresi sona erenler yeniden seçilebilirler. Görev süresi dolmadan görevinden ayrılan üyenin yerine aynı usule göre seçilen üye, yerine seçildiği üyenin görev süresini tamamlar. Yeni seçilen Kurul göreve başlayıncaya kadar önceki Kurul görevine devam eder.

Kurul üyelerine 10.2.1954 tarihli ve 6245 sayılı Harcırah Kanunu hükümleri saklı kalmak kaydıyla fiilen görev yaptıkları her gün için (3000) gösterge rakamının memur aylık katsayısı ile çarpımı sonucu bulunacak miktarda huzur hakkı ödenir. Bu ödemelerde damga vergisi hariç herhangi bir kesinti yapılmaz. **(Ek cümle: 17/11/2005-5432/2 md.)** Bir ayda fiilen görev yapılan gün sayısının dördü aşması halinde, aşan günler için huzur hakkı ödenmez.(1)

---

[22] Bu arada yer alan "16 ve 17 nci maddelerde öngörülen sebeplerle" ibaresi, 17/11/2005 tarihli ve 5432 sayılı Kanunun 1 inci maddesiyle madde metninden çıkarılmıştır.

[23] 17/11/2005 tarihli ve 5432 sayılı Kanunun 2 nci maddesiyle, birinci fıkrada yer alan "16 ve 17 nci maddelerde öngörülen sebeplere dayanılarak" ibaresi, madde metninden çıkarılmış; yedinci fıkrada yer alan "uhdesinde kamu görevi bulunanlara (1000), uhdesinde kamu görevi bulunmayanlara ise (2000)" ibaresi, "(3000)" olarak değiştirilmiş ve metne işlenmiştir.

Kurul, belirleyeceği konularda komisyonlar ve çalışma grupları kurabilir; ayrıca gerekli gördüğü takdirde, ilgili bakanlık ile diğer kurum ve kuruluşların ve sivil toplum örgütlerinin temsilcilerini bilgi almak üzere toplantılarına katılmaya davet edebilir.

Kurulun sekretarya hizmetleri Başbakanlık tarafından yerine getirilir.

Kurulun görev ve çalışmalarına ilişkin esas ve usuller Başbakanlıkça hazırlanarak yürürlüğe konulacak bir yönetmelikle düzenlenir.

DÖRDÜNCÜ BÖLÜM
Bilgi Edinme Hakkının Sınırları

Madde 15- Yargı denetimi dışında kalan işlemler

Yargı denetimi dışında kalan idarî işlemlerden kişinin çalışma hayatını ve mesleki onurunu etkileyecek nitelikte olanlar, bu Kanun kapsamına dahildir. Bu şekilde sağlanan bilgi edinme hakkı işlemin yargı denetimine açılması sonucunu doğurmaz.

Madde 16- Devlet sırrına ilişkin bilgi veya belgeler

Açıklanması hâlinde Devletin emniyetine, dış ilişkilerine, millî savunmasına ve millî güvenliğine açıkça zarar verecek ve niteliği itibarıyla Devlet sırrı olan gizlilik dereceli bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır.

Madde 17- Ülkenin ekonomik çıkarlarına ilişkin bilgi veya belgeler

Açıklanması ya da zamanından önce açıklanması hâlinde, ülkenin ekonomik çıkarlarına zarar verecek veya haksız rekabet ve kazanca sebep olacak bilgi veya belgeler, bu Kanun kapsamı dışındadır.

Madde 18- İstihbarata ilişkin bilgi veya belgeler

Sivil ve askerî istihbarat birimlerinin görev ve faaliyetlerine ilişkin bilgi veya belgeler, bu Kanun kapsamı dışındadır.

Ancak, bu bilgi ve belgeler kişilerin çalışma hayatını ve meslek onurunu etkileyecek nitelikte ise, istihbarata ilişkin bilgi ve belgeler bilgi edinme hakkı kapsamı içindedir.

Madde 19- İdarî soruşturmaya ilişkin bilgi veya belgeler

Kurum ve kuruluşların yetkili birimlerince yürütülen idarî soruşturmalarla ilgili olup, açıklanması veya zamanından önce açıklanması hâlinde;

a) Kişilerin özel hayatına açıkça haksız müdahale sonucunu doğuracak,

b) Kişilerin veya soruşturmayı yürüten görevlilerin hayatını ya da güvenliğini tehlikeye sokacak,

c) Soruşturmanın güvenliğini tehlikeye düşürecek,

d) Gizli kalması gereken bilgi kaynağının açığa çıkmasına neden olacak veya soruşturma ile ilgili benzeri bilgi ve bilgi kaynaklarının temin edilmesini güçleştirecek,

Bilgi veya belgeler, bu Kanun kapsamı dışındadır.

Madde 20- Adlî soruşturma ve kovuşturmaya ilişkin bilgi veya belgeler

Açıklanması veya zamanından önce açıklanması hâlinde;

a) Suç işlenmesine yol açacak,

b) Suçların önlenmesi ve soruşturulması ya da suçluların kanunî yollarla yakalanıp kovuşturulmasını tehlikeye düşürecek,

c) Yargılama görevinin gereğince yerine getirilmesini engelleyecek,

d) Hakkında dava açılmış bir kişinin adil yargılanma hakkını ihlâl edecek,

Nitelikteki bilgi veya belgeler, bu Kanun kapsamı dışındadır.

4.4.1929 tarihli ve 1412 sayılı Ceza Muhakemeleri Usulü Kanunu, 18.6.1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanunu, 6.1.1982 tarihli ve 2577 sayılı İdari Yargılama Usulü Kanunu ve diğer özel kanun hükümleri saklıdır.

Madde 21- Özel hayatın gizliliği

Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır.

Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir.

Madde 22- Haberleşmenin gizliliği

Haberleşmenin gizliliği esasını ihlâl edecek bilgi veya belgeler, bu Kanun kapsamı dışındadır.

Madde 23- Ticarî sır

Kanunlarda ticarî sır olarak nitelenen bilgi veya belgeler ile, kurum ve kuruluşlar tarafından gerçek veya tüzel kişilerden gizli kalması kaydıyla sağlanan ticarî ve malî bilgiler, bu Kanun kapsamı dışındadır.

Madde 24- Fikir ve sanat eserleri

Fikir ve sanat eserlerine ilişkin olarak yapılacak bilgi edinme başvuruları hakkında ilgili kanun hükümleri uygulanır.

Madde 25- Kurum içi düzenlemeler

Kurum ve kuruluşların, kamuoyunu ilgilendirmeyen ve sadece kendi personeli ile kurum içi uygulamalarına ilişkin düzenlemeler hakkındaki bilgi veya belgeler, bilgi edinme hakkının kapsamı dışındadır. Ancak, söz konusu düzenlemeden etkilenen kurum çalışanlarının bilgi edinme hakları saklıdır.

Madde 26- Kurum içi görüş, bilgi notu ve tavsiyeler

Kurum ve kuruluşların faaliyetlerini yürütmek üzere, elde ettikleri görüş, bilgi notu, teklif ve tavsiye niteliğindeki bilgi veya belgeler, kurum ve kuruluş tarafından aksi kararlaştırılmadıkça bilgi edinme hakkı kapsamındadır.

Bilimsel, kültürel, istatistik, teknik, tıbbî, malî, hukukî ve benzeri uzmanlık alanlarında yasal olarak görüş verme yükümlülüğü bulunan kişi, birim ya da kurumların görüşleri, kurum ve kuruluşların alacakları kararlara esas teşkil etmesi kaydıyla bilgi edinme istemlerine açıktır.

Madde 27- Tavsiye ve mütalaa talepleri

Tavsiye ve mütalaa talepleri bu Kanun kapsamı dışındadır.

Madde 28- Gizliliği kaldırılan bilgi veya belgeler

Gizliliği kaldırılmış olan bilgi veya belgeler, bu Kanunda belirtilen diğer istisnalar kapsamına girmiyor ise, bilgi edinme başvurularına açık hâle gelir.

BEŞİNCİ BÖLÜM
Çeşitli ve Son Hükümler

Madde 29- Ceza hükümleri

Bu Kanunun uygulanmasında ihmâli, kusuru veya kastı bulunan memurlar ve diğer kamu görevlileri hakkında, işledikleri fiillerin genel hükümler çerçevesinde ceza kovuşturması gerektirmesi hususu saklı kalmak kaydıyla, tâbi oldukları mevzuatta yer alan disiplin cezaları uygulanır.

Bu Kanunla erişilen bilgi ve belgeler ticarî amaçla çoğaltılamaz ve kullanılamaz.

Madde 30- Rapor düzenlenmesi

Kurum ve kuruluşlar, bir önceki yıla ait olmak üzere;

a) Kendilerine yapılan bilgi edinme başvurularının sayısını,

b) Olumlu cevaplanarak bilgi veya belgelere erişim sağlanan başvuru sayısını,

c) Reddedilen başvuru sayısı ve bunların dağılımını gösterir istatistik bilgileri,

d) Gizli ya da sır niteliğindeki bilgiler çıkarılarak ya da bu nitelikteki bilgiler ayrılarak bilgi veya belgelere erişim sağlanan başvuru sayısını,

e) Başvurunun reddedilmesi üzerine itiraz edilen başvuru sayısı ile bunların sonuçlarını,

Gösterir bir rapor hazırlayarak, bu raporları her yıl Şubat ayının sonuna kadar Bilgi Edinme Değerlendirme Kuruluna gönderirler. Bağlı, ilgili ve ilişkili kamu kurum ve kuruluşları raporlarını bağlı, ilgili ya da ilişkili oldukları bakanlık vasıtasıyla iletirler. Kurul, hazırlayacağı genel raporu, söz konusu kurum ve kuruluşların raporları ile birlikte her yıl Nisan ayının sonuna kadar Türkiye Büyük Millet Meclisine gönderir. Bu raporlar takip eden iki ay içinde Türkiye Büyük Millet Meclisi Başkanlığınca kamuoyuna açıklanır.

Madde 31- Yönetmelik

Bu Kanunun uygulanması ile ilgili esas ve usullerin belirlenmesine ilişkin yönetmelik, Kanunun yayımını takip eden altı ay içinde Başbakanlık tarafından hazırlanarak Bakanlar Kurulunca yürürlüğe konulur.

Madde 32- Yürürlük

Bu Kanun yayımı tarihinden itibaren altı ay sonra yürürlüğe girer.

Madde 33- Yürütme

Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

4982 SAYILI KANUNA EK VE DEĞİŞİKLİK GETİREN MEVZUATIN VEYA ANAYASA MAHKEMESİ TARAFINDAN İPTAL EDİLEN HÜKÜMLERİN YÜRÜRLÜĞE GİRİŞ TARİHİNİ GÖSTERİR LİSTE

Değiştiren Kanunun/KHK'nin/ İptal Eden Anayasa Mahkemesi Kararının Numarası	**4982 sayılı Kanunun değişen veya iptal edilen maddeleri**	**Yürürlüğe Giriş Tarihi**
5432	13 ve 14	22/11/2005
6495	2	2/8/2013
Anayasa Mahkemesi'nin 4/12/2014 tarihli ve E.: 2013/114, K.: 2014/22 (Yürürlüğü Durdurma) Kararı	2	6/12/2014
Anayasa Mahkemesi'nin 4/12/2014 tarihli ve E.: 2013/114, K.: 2014/184 sayılı Kararı	2	16/7/2015

5237 SAYILI TÜRK CEZA KANUNUNUN İLGİLİ HÜKÜMLERİ

Künye: 26.09.2004 tarihli 5237 sayılı Kanun.
(12/10/2004 tarihli 25611 sayılı Resmi Gazete)
Tam metin için:
http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf 19.03.16

DOKUZUNCU BÖLÜM
Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar
Madde 132- Haberleşmenin gizliliğini ihlal

[24] (1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. **(Ek cümle: 2/7/2012-6352/79 md.)** İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

(4) **(Mülga: 2/7/2012-6352/79 md.)**

Madde 133- Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması)

[25] (1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

(3) **(Değişik: 2/7/2012-6352/80 md.)** Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

---

[24] *2/7/2012 tarihli ve 6352 sayılı Kanunun 79 uncu maddesiyle, bu maddenin birinci fıkrasında yer alan "altı aydan iki yıla kadar hapis veya adlî para" ibaresi "bir yıldan üç yıla kadar hapis" ve "bir yıldan üç yıla kadar hapis cezasına hükmolunur" ibaresi ise "verilecek ceza bir kat artırılır" şeklinde; ikinci fıkrasında yer alan "bir yıldan üç yıla kadar hapis" ibaresi "iki yıldan beş yıla kadar hapis" şeklinde; üçüncü fıkrasında yer alan "altı aydan iki yıla kadar hapis veya adlî para" ibaresi "bir yıldan üç yıla kadar hapis" şeklinde değiştirilmiş, fıkraya "rızası olmaksızın" ibaresinden sonra gelmek üzere "hukuka aykırı olarak" ibaresi eklenmiştir.*

[25] *2/7/2012 tarihli ve 6352 sayılı Kanunun 80 inci maddesiyle, bu maddenin birinci fıkrasında yer alan "iki aydan altı aya kadar hapis" ibaresi "iki yıldan beş yıla kadar hapis" şeklinde; ikinci fıkrasında yer alan "altı aya kadar hapis" ibaresi "altı aydan iki yıla kadar hapis" şeklinde değiştirilmiştir.*

Madde 134- Özel hayatın gizliliğini ihlal

[26] (1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.

(2) **(Değişik: 2/7/2012-6352/81 md.)** Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

Madde 135- Kişisel verilerin kaydedilmesi

(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.[27]

(2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır[28].

Madde 136- Verileri hukuka aykırı olarak verme veya ele geçirme

(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.[29]

Madde 137- Nitelikli haller

(1) Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle,

İşlenmesi halinde, verilecek ceza yarı oranında artırılır.

---

[26] 2/7/2012 tarihli ve 6352 sayılı Kanunun 81 inci maddesiyle, bu maddenin birinci fıkrasında yer alan "altı aydan iki yıla kadar hapis veya adlî para" ibaresi "bir yıldan üç yıla kadar hapis" ve "cezanın alt sınırı bir yıldan az olamaz" ibaresi ise "verilecek ceza bir kat artırılır" şeklinde değiştirilmiştir.

[27] 21/2/2014 tarihli ve 6526 sayılı kanunun 3 üncü maddesiyle bu fıkrada yer alan "altı aydan" ibaresi "bir yıldan" şeklinde değiştirilmiştir.

[28] 24/3/2016 tarihli ve 6698 sayılı Kanunun 30 uncu maddesiyle, bu fıkrada yer alan "Kişilerin" ibaresi "Kişisel verinin, kişilerin" şeklinde; "bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır" ibaresi "olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır" şeklinde değiştirilmiştir.

[29] 21/2/2014 tarihli ve 6526 sayılı kanunun 4 üncü maddesiyle bu fıkrada yer alan "bir yıldan" ibaresi "iki yıldan" şeklinde değiştirilmiştir.

Madde 138- Verileri yok etmeme

(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.[30]

(2) **(Ek: 21/2/2014-6526/5 md.)** Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.

Madde 139- Şikayet

(1) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikayete bağlıdır.

Madde 140- Tüzel kişiler hakkında güvenlik tedbiri uygulanması

(1) Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

…

Madde 243- Bilişim sistemine girme

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir. (1)

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

(4) (Ek: 24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

---

[30] *21/2/2014 tarihli ve 6526 sayılı kanunun 5 inci maddesiyle bu fıkrada yer alan "altı aydan bir yıla kadar hapis" ibaresi "bir yıldan iki yıla kadar hapis" şeklinde değiştirilmiştir.*

5271 SAYILI CEZA MUHAKEMESİ KANUNUNUN İLGİLİ HÜKÜMLERİ

Künye: 04.12.2004 tarihli 5271 sayılı Kanun.
(17.12.2004 tarihli 25673 sayılı Resmi Gazete)
Tam metin için:
http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf 07.04.2016

ÜÇÜNCÜ KISIM
Tanıklık, Bilirkişi İncelemesi ve Keşif

(…)

ÜÇÜNCÜ BÖLÜM
Gözlem Altına Alma, Muayene, Keşif ve Otopsi

(…)

Madde 80- Genetik inceleme sonuçlarının gizliliği (Değişik: 25/5/2005 – 5353/4 md.)

(1) 75, 76 ve 78 inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez.

(2) Bu bilgiler, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir.

5429 SAYILI TÜRKİYE İSTATİSTİK KANUNUNUN İLGİLİ HÜKÜMLERİ

Künye: 10.11.2015 tarihli 5429 sayılı Kanun.
(18.11.2005 tarihli 25997 sayılı Resmi Gazete)
Tam metin için:
http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5429.doc 05.04.2016

Madde 2- Tanımlar

Bu Kanunun uygulanmasında; (…)

n) **Veri**: Anket veya idarî kayıtlar yoluyla elde edilen nicel ve/veya nitel istatistikî bilgileri,

o) **Bireysel veri**: Hakkında bilgi toplanan istatistikî birimlerin, özellikleri ile birlikte tanımlandığı veriyi,

5651 SAYILI İNTERNET ORTAMINDA YAPILAN YAYINLARIN DÜZENLENMESİ VE BU YAYINLAR YOLUYLA İŞLENEN SUÇLARLA MÜCADELE EDİLMESİ HAKKINDA KANUNUN İLGİLİ HÜKÜMLERİ

> ***Künye:*** *04.05.2007 tarihli 5651 sayılı Kanun.*
> *(23.05.2007 tarihli 26530 sayılı Resmi Gazete)*
> ***Tam metin için:***
> *http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf*

Madde 2- Tanımlar

Bu Kanunun uygulanmasında; (…)

ç) Bilgi: Verilerin anlam kazanmış biçimini,

k) Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,

5502 SAYILI SOSYAL GÜVENLİK KURUMU KANUNUNUN İLGİLİ HÜKÜMLERİ

> ***Künye**: 16.05.2006 tarihli 5502 sayılı Kanun.*
> *(20.05.2006 tarihli 26173 sayılı Resmi Gazete)*
> ***Tam metin için:***
> *http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5502.pdf*

Madde 2- Tanımlar

Bu Kanunda geçen (…)

c) Kurum: Sosyal Güvenlik Kurumunu; (…)

ifade eder.

Madde 35- Kurumun taşınmaz edinimi, taşınır ve taşınmaz mal varlıkları ile gayri maddi haklarının hukuki durumu

(5) (Ek fıkra: 10/9/2014-6552/37 md.; Değişik: 4/4/2015-6645/43 md.) Kurum, bu Kanun ve diğer kanunlarla verilen görevleri yerine getirmek amacıyla işlediği kişisel veriler ile ticari sır niteliğinde olan verileri, veri sahibinin noter onaylı muvafakati olmadan gerçek veya tüzel kişilerle paylaşamaz. Ancak, 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununun eki (I), (II), (III) ve (IV) sayılı cetvellerde yer alan kamu idarelerinin kanunlarında belirtilen görevleri yapabilmeleri için ihtiyaç duydukları sağlık verisi dışındaki kişisel veriler ile ticari sır niteliğindeki veriler paylaşılabilir. Kurum, bunların dışındaki gayri maddi hakları ile kimliği belirli veya belirlenebilir bir gerçek veya tüzel kişiyle ilişkilendirilemeyecek şekilde anonim hâle getirdiği verileri araştırma, planlama ve istatistik gibi amaçlar için kamu idareleri, bilimsel araştırma yapan kamu personeli, bilimsel dernekler, kamu kurumu niteliğindeki meslek kuruluşları veya üniversiteler ile ücretsiz olarak paylaşabilir. Anonim hâle getirilen verinin tüzel kişilere ait olması hâlinde bu fıkrada sayılanlar dışındaki gerçek veya tüzel kişilere tüzel kişinin noter onaylı muvafakati alınmak kaydıyla ücretli olarak verilebilir. Veri paylaşılan kamu idareleri ile gerçek ve tüzel kişiler, paylaşılan verinin gizliliğinden ve güvenliğinden sorumludur. Bu fıkranın aksine davrananlar hakkında, veri paylaşımı yapılanlar da dâhil olmak üzere 5237 sayılı Türk Ceza Kanunu ile diğer ilgili mevzuat hükümleri uygulanır.

6098 SAYILI TÜRK BORÇLAR KANUNU'NUN İLGİLİ HÜKÜMLERİ

Künye: 11/1/2011 tarihli 6098 sayılı Kanun.
(04.02.2011 tarihli 27836 sayılı Resmi Gazete)
Tam metin için:
http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6098.pdf 19.03.16

İKİNCİ AYIRIM
Haksız Fiillerden Doğan Borç İlişkileri

I. Genel olarak
MADDE 49

Kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür.

Zarar verici fiili yasaklayan bir hukuk kuralı bulunmasa bile, ahlaka aykırı bir fiille başkasına kasten zarar veren de, bu zararı gidermekle yükümlüdür.

II. Zararın ve kusurun ispatı
MADDE 50

Zarar gören, zararını ve zarar verenin kusurunu ispat yükü altındadır.

Uğranılan zararın miktarı tam olarak ispat edilemiyorsa hâkim, olayların olağan akışını ve zarar görenin aldığı önlemleri göz önünde tutarak, zararın miktarını hakkaniyete uygun olarak belirler.

III. Tazminat

1. Belirlenmesi
MADDE 51

Hâkim, tazminatın kapsamını ve ödenme biçimini, durumun gereğini ve özellikle kusurun ağırlığını göz önüne alarak belirler.

Tazminatın irat biçiminde ödenmesine hükmedilirse, borçlu güvence göstermekle yükümlüdür.

2. İndirilmesi
MADDE 52

Zarar gören, zararı doğuran fiile razı olmuş veya zararın doğmasında ya da artmasında etkili olmuş yahut tazminat yükümlüsünün durumunu ağırlaştırmış ise hâkim, tazminatı indirebilir veya tamamen kaldırabilir.

Zarara hafif kusuruyla sebep olan tazminat yükümlüsü, tazminatı ödediğinde yoksulluğa düşecek olur ve hakkaniyet de gerektirirse hâkim, tazminatı indirebilir.

IV. Özel durumlar

1. Ölüm ve bedensel zarar

a. Ölüm
MADDE 53

Ölüm hâlinde uğranılan zararlar özellikle şunlardır:

1. Cenaze giderleri.

2. Ölüm hemen gerçekleşmemişse tedavi giderleri ile çalışma gücünün azalmasından ya da yitirilmesinden doğan kayıplar.

3. Ölenin desteğinden yoksun kalan kişilerin bu sebeple uğradıkları kayıplar.

b. Bedensel zarar
MADDE 54

Bedensel zararlar özellikle şunlardır:

1. Tedavi giderleri.

2. Kazanç kaybı.

3. Çalışma gücünün azalmasından ya da yitirilmesinden doğan kayıplar.

4. Ekonomik geleceğin sarsılmasından doğan kayıplar.

c. Belirlenmesi
MADDE 55

Destekten yoksun kalma zararları ile bedensel zararlar, bu Kanun hükümlerine ve sorumluluk hukuku ilkelerine göre hesaplanır. Kısmen veya tamamen rücu edilemeyen sosyal güvenlik ödemeleri ile ifa amacını taşımayan ödemeler, bu tür zararların belirlenmesinde gözetilemez; zarar veya tazminattan indirilemez. Hesaplanan tazminat, miktar esas alınarak hakkaniyet düşüncesi ile artırılamaz veya azaltılamaz.

Bu Kanun hükümleri, her türlü idari eylem ve işlemler ile idarenin sorumlu olduğu diğer sebeplerin yol açtığı vücut bütünlüğünün kısmen veya tamamen yitirilmesine ya da kişinin ölümüne bağlı zararlara ilişkin istem ve davalarda da uygulanır.

d. Manevi tazminat
MADDE 56

Hâkim, bir kimsenin bedensel bütünlüğünün zedelenmesi durumunda, olayın özelliklerini göz önünde tutarak, zarar görene uygun bir miktar paranın manevi tazminat olarak ödenmesine karar verebilir.

Ağır bedensel zarar veya ölüm hâlinde, zarar görenin veya ölenin yakınlarına da manevi tazminat olarak uygun bir miktar paranın ödenmesine karar verilebilir.

2. Haksız rekabet
MADDE 57

Gerçek olmayan haberlerin yayılması veya bu tür ilanların yapılması ya da dürüstlük kurallarına aykırı diğer davranışlarda bulunulması yüzünden müşterileri azalan veya onları kaybetme tehlikesiyle karşılaşan kişi, bu davranışlara son verilmesini ve kusurun varlığı hâlinde zararının giderilmesini isteyebilir.

Ticari işlere ait haksız rekabet hakkında Türk Ticaret Kanunu hükümleri saklıdır.

3. Kişilik hakkının zedelenmesi
MADDE 58

Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir.

Hâkim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir.

4. Ayırt etme gücünün geçici kaybı
MADDE 59

Ayırt etme gücünü geçici olarak kaybeden kişi, bu sırada verdiği zararları gidermekle yükümlüdür. Ancak, ayırt etme gücünü kaybetmede kusuru olmadığını ispat ederse, sorumluluktan kurtulur.

V. Sorumluluk sebeplerinin çokluğu

1. Sebeplerin yarışması
MADDE 60

Bir kişinin sorumluluğu, birden çok sebebe dayandırılabiliyorsa hâkim, zarar gören aksini istemiş olmadıkça veya kanunda aksi öngörülmedikçe, zarar görene en iyi giderim imkânı sağlayan sorumluluk sebebine göre karar verir.

2. Müteselsil sorumluluk

a. Dış ilişkide
MADDE 61

Birden çok kişi birlikte bir zarara sebebiyet verdikleri veya aynı zarardan çeşitli sebeplerden dolayı sorumlu oldukları takdirde, haklarında müteselsil sorumluluğa ilişkin hükümler uygulanır.

b. İç ilişkide
MADDE 62

Tazminatın aynı zarardan sorumlu müteselsil borçlular arasında paylaştırılmasında, bütün durum ve koşullar, özellikle onlardan her birine yüklenebilecek kusurun ağırlığı ve yarattıkları tehlikenin yoğunluğu göz önünde tutulur.

Tazminatın kendi payına düşeninden fazlasını ödeyen kişi, bu fazla ödemesi için, diğer müteselsil sorumlulara karşı rücu hakkına sahip ve zarar görenin haklarına halef olur.

VI. Hukuka aykırılığı kaldıran hâller

1. Genel olarak
MADDE 63

Kanunun verdiği yetkiye dayanan ve bu yetkinin sınırları içinde kalan bir fiil, zarara yol açsa bile, hukuka aykırı sayılmaz.

Zarar görenin rızası, daha üstün nitelikte özel veya kamusal yarar, zarar verenin davranışının haklı savunma niteliği taşıması, yetkili kamu makamlarının müdahalesinin zamanında sağlanamayacak olması durumunda kişinin hakkını kendi gücüyle koruması veya zorunluluk hâllerinde de fiil, hukuka aykırı sayılmaz.

2. Sorumluluk
MADDE 64

Haklı savunmada bulunan, saldıranın şahsına veya mallarına verdiği zarardan sorumlu tutulamaz.

Kendisini veya başkasını açık ya da yakın bir zarar tehlikesinden korumak için diğer bir kişinin mallarına zarar verenin, bu zararı giderim yükümlülüğünü hâkim hakkaniyete göre belirler.

Hakkını kendi gücüyle koruma durumunda kalan kişi, durum ve koşullara göre o sırada kolluk gücünün yardımını zamanında sağlayamayacak ise ve hakkının kayba uğramasını ya da kullanılmasının önemli ölçüde zorlaşmasını önleyecek başka bir yol da yoksa, verdiği zarardan sorumlu tutulamaz.

(…)

IV. İşçinin kişiliğinin korunması

3. Kişisel verilerin kullanılmasında
MADDE 419

İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir.

Özel kanun hükümleri saklıdır.

ELEKTRONİK HABERLEŞME SEKTÖRÜNDE TÜKETİCİ HAKLARI YÖNETMELİĞİ

> ***Künye:*** *28.07.2010 tarihli 27655 sayılı Resmi Gazete.*
> ***Tam metin için:***
> *http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.14148&MevzuatIliski=0&sourceXmlSearch=ki%C5%9Fisel%20veri*

Madde 4- Tanımlar

Bu Yönetmelikte geçen; (…)

f) Kişisel veri: Belirli veya kimliği belirlenebilir gerçek veya tüzel şahıslara ilişkin bütün bilgileri,

(…)

ifade eder.

Madde 5- Tüketici hakları

(1) Elektronik haberleşme hizmetlerinden yararlanan tüketiciler aşağıda sıralanan haklara sahiptir;

(…)

c) Abonelerin kişisel verilerinin kamuya açık rehberlerde yer alıp almamasını talep etme hakkı,

(…)

MADDE 15- Abonelik sözleşmelerinin uygulanması

(…)

(4) Telefon hizmetlerinde, sunulan elektronik ve/veya yazılı rehber hizmetleri için abonelik sözleşmesi imzalanırken, aboneden bu rehberlerde kişisel verilerinin yer alıp almayacağı hususunda onayı alınır.

(…)

ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN İŞLENMESİ VE GİZLİLİĞİNİN KORUNMASI HAKKINDA YÖNETMELİK

Künye: *24.07.2012 tarihli 28363 sayılı Resmi Gazete.*
Tam metin için:
http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.16405&MevzuatIliski=0&sourceXmlSearch=ki%C5%9Fisel%20verilerin 19.03.16

BİRİNCİ BÖLÜM / AMAÇ, KAPSAM, DAYANAK VE TANIMLAR

MADDE 1 – Amaç ve kapsam

(1) Bu Yönetmeliğin amacı, elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması için elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenlemektir.

(2) Haberleşmenin içeriğine ilişkin verilerin saklanması bu Yönetmeliğin kapsamına dâhil değildir.

MADDE 2 – Dayanak

(1) Bu Yönetmelik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 4, 6, 12 ve 51 inci maddelerine dayanılarak hazırlanmıştır.

MADDE 3 – Tanımlar ve kısaltmalar

(1) Bu Yönetmelikte geçen;

a) Abone: Bir işletmeci ile elektronik haberleşme hizmetinin sunumuna yönelik olarak yapılan bir sözleşmeye taraf olan gerçek ya da tüzel kişiyi,

b) Acil yardım çağrıları: Ulusal ve uluslararası düzenlemelerde kabul görmüş yangın, sağlık, doğal afetler ve güvenlik gibi acil durumlarla ilgili olarak itfaiye, polis, jandarma, sağlık ve benzeri kuruluşlara yardım talebiyle yapılan çağrıları,

c) **(Değişik:RG-11/7/2013-28704)** Anonim hale getirme: Kişisel verilerin, belirli veya kimliği belirlenebilir bir gerçek ya da tüzel kişiyle ilişkilendirilemeyecek veya kaynağı belirlenemeyecek hale getirilmesini,

ç) **(Değişik:RG-11/7/2013-28704)** Gerçekleşmeyen arama: Başarılı bir şekilde bağlantı kurulmasına rağmen haberleşmenin gerçekleşmemesini,

d) Hücre kimliği: Mobil telefon çağrısının başladığı ya da sona erdiği hücrenin kimliğini,

e) IMEI: Uluslararası mobil cihaz kimliğini,

f) IMSI: Uluslararası mobil abone kimliğini,

g) **(Değişik:RG-11/7/2013-28704)** İşlem kaydı: Kişisel verilere erişen kişiler tarafından yapılan işlemin ileriki bir tarihte tanımlanabilmesini teminen asgari olarak işlem, işlemin detayı, işlemi yapan kişi, işlemin yapıldığı tarih ve zaman ile işlemi yapan kişinin bağlandığı nokta bilgilerini içeren elektronik kayıtları,

ğ) İşletmeci: Yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketi,

h) Kişisel veri: Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgileri,

ı) Kişisel veri ihlali: İstem dışı, yetki dışı ya da yasa dışı olarak; kişisel verilerin tahrip edilmesine, kaybolmasına, iletilmesine, değiştirilmesine, depolanmasına veya başka bir ortama kaydedilmesine, işlenmesine, ifşa edilmesine ve söz konusu verilere erişilmesine neden olan güvenlik ihlalini,

i) Kişisel verilerin işlenmesi: Kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi, tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen işlem ya da işlemler bütününü,

j) Konum verisi: Kamuya açık elektronik haberleşme hizmeti kullanıcısına ait bir cihazın coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde veya elektronik haberleşme hizmeti aracılığıyla işlenen belirli veriyi,

k) Kullanıcı: Aboneliği olup olmamasına bakılmaksızın elektronik haberleşme hizmetlerinden yararlanan gerçek veya tüzel kişiyi,

l) Kullanıcı kimliği: İnternet erişim hizmetlerine ya da internet haberleşme hizmetlerine abonelik ya da kayıt esnasında tahsis edilen tek ve kişiye özel tanımlamayı,

m) Kurul: Bilgi Teknolojileri ve İletişim Kurulunu,

n) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,

o) **(Değişik:RG-11/7/2013-28704)** NAT: Şebekede taşınan IP paketlerindeki IP adres bilgisi yanında port bilgileri de kullanılarak aynı IP'lerin birden çok abone tarafından kullanılmasını sağlayan teknolojiyi,

ö) Rıza: İlgili kişinin kendisine ait kişisel verisinin işlenmesine yönelik, verinin işlenme amaç ve kapsamı dâhilinde, verinin işlenmesi öncesinde özgür iradesiyle verdiği ispatlanabilir kabul beyanını,

p) Trafik verisi: Bir elektronik haberleşme şebekesinde haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi,

r) Veri: Abone ya da kullanıcıyı teşhis etmek için yararlanılan trafik verisi, konum verisi ya da ilgili diğer bilgileri,

ifade eder.

(2) **(Değişik:RG-11/7/2013-28704)** Bu Yönetmelikte geçen ancak birinci fıkrada tanımlanmayan kavramlar ve kısaltmalar için ilgili mevzuatta yer alan tanımlar geçerlidir.

İKİNCİ BÖLÜM /
UYGULAMA ESASLARI

MADDE 4 – Kişisel verilerin işlenmesine ilişkin ilkeler

(1) Kişisel verilerin;

a) Hukuka ve dürüstlük kurallarına uygun olarak işlenmesi,

b) İlgili kişinin rızasına dayalı olarak işlenmesi,

c) Elde edilme amacıyla bağlantılı, yeterli ve orantılı olması,

ç) Doğru olması ve gerektiğinde güncellenmesi,

d) İlgili kişilerin kimliklerini belirtecek biçimde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar muhafaza edilmesi

esastır.

(2) **(Ek:RG-11/7/2013-28704)** Kişisel veriler yurt dışına çıkarılamaz.

(3) **(Ek:RG-11/7/2013-28704)** Kişisel verilerin işlenmesi kapsamında abone tarafından işletmeciye verilen rıza, sadece alınan hizmete özgü olmak koşuluyla, kişisel verilerin işletmeci tarafından yetkilendirilen taraflar marifetiyle işlenebilmesini de kapsar.

(4) **(Ek:RG-11/7/2013-28704)** İşletmeci tarafından yetkilendirilen taraflarca bu Yönetmelik hükümlerinin ihlal edilmesi de dâhil olmak üzere kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda kullanılmasının temininden işletmeci sorumludur.

MADDE 5 – Güvenlik

(1) İşletmeciler, kişisel verilerin işlenmesine ilişkin olarak güvenlik politikası belirler. İşletmeciler şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alır. Söz konusu güvenlik tedbirleri, teknolojik imkânlar göz önünde bulundurularak muhtemel riske uygun bir düzeyde sağlanır.

(2) Birinci fıkrada belirtilen tedbirler, asgari istem dışı, yetki dışı ya da yasa dışı olarak; kişisel verilerin tahrip edilmesi, kaybolması, değiştirilmesi, depolanması veya başka bir ortama kaydedilmesi, işlenmesi, ifşa edilmesi ve söz konusu verilere erişilmesine karşı kişisel verilerin korunmasını içerir.

(3) **(Değişik:RG-11/7/2013-28704)** İşletmeciler, kişisel verilere sadece yetkili kişiler tarafından erişilebilmesini ve kişisel verilerin saklandığı sistemlerin ve kişisel verilere erişim sağlamak için kullanılan uygulamaların güvenliğini sağlamakla yükümlüdür.

(4) **(Değişik:RG-11/7/2013-28704)** İşletmeciler, kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtlarını saklamakla yükümlüdür.

(5) **(Değişik:RG-11/7/2013-28704)** Kurum, gerekli gördüğü hallerde işletmecilerden, kişisel verilerin saklandığı sistemlere ve alınan güvenlik tedbirlerine ilişkin tüm bilgi ve belgeleri isteme, ayrıca söz konusu güvenlik tedbirlerinde değişiklik talep etme hakkını haizdir.

MADDE 6 – Riskin ve kişisel veri ihlalinin bildirilmesi

(1) **(Değişik:RG-11/7/2013-28704)** İşletmeci, şebekenin ve kişisel verilerin güvenliğini ihlal eden belirli bir risk olması durumunda bu risk hakkında Kurumu ve Kurum tarafından gerekli görülmesi halinde abonelerini/kullanıcılarını etkin ve hızlı bir şekilde bilgilendirmekle yükümlüdür.

(2) Bu riskin işletmeci tarafından alınan tedbirlerin dışında kalması halinde, söz konusu riskin kapsamı, giderilme yöntemleri ve yaklaşık maliyeti hakkında abonelerin/kullanıcıların etkin ve hızlı bir şekilde bilgilendirilmesi sağlanır.

(3) İşletmeci, kişisel veri ihlali olması durumunda söz konusu ihlalin niteliği ve sonuçları hakkında abonelere/kullanıcılara yapılacak bilgilendirmenin detayları ve ihlalin giderilmesi için alınan tedbirlere ilişkin olarak Kurumu bilgilendirir.

(4) Kişisel veri ihlalinden abonelerin/kullanıcıların olumsuz yönde etkilenme ihtimalinin bulunması halinde işletmeci, kişisel veri ihlalinin niteliğine, daha fazla bilginin elde edilebileceği iletişim noktalarına ve ihlalin olası olumsuz etkilerini azaltmak için aboneler/kullanıcılar tarafından alınabilecek önlemlere ilişkin olarak aboneleri/kullanıcıları ücretsiz olarak bilgilendirir.

(5) İşletmeci, gerçekleşen kişisel veri ihlallerine ilişkin olarak söz konusu ihlalin sebeplerini, etkilerini ve çözüme yönelik tedbirleri içeren bilgileri gizliliğini ve bütünlüğünü sağlayarak kaydetmekle yükümlüdür.

ÜÇÜNCÜ BÖLÜM /
VERİLERİN İŞLENMESİ VE SAKLANMASI

MADDE 7 – Haberleşmenin gizliliği

(1) Elektronik haberleşme ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve gözetimi yasaktır.

(2) Elektronik haberleşme şebekeleri, haberleşmenin iletimini gerçekleştirmek dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili kullanıcıların/abonelerin verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve rızalarının alınması kaydıyla kullanılabilir.

MADDE 8 – Trafik verisinin işlenmesi

(1) İşletmeciler, sundukları hizmetin kapsamı dışındaki amaçlar için trafik verisini işleyemez.

(2) Trafik verisi, ilgili mevzuat hükümlerine uygun olarak, trafiğin yönetimi, arabağlantı, faturalama, yolsuzluk tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır.

(3) **(Değişik:RG-11/7/2013-28704)** Elektronik haberleşme hizmetlerini pazarlamak veya katma değerli elektronik haberleşme hizmetleri sunmak amacıyla ihtiyaç duyulan trafik verileri anonim hale getirilerek veya ilgili abonelerin/kullanıcıların işlenecek trafik verileri ve işleme süresi hakkında bilgilendirilmelerinden sonra rızalarının alınması kaydıyla, alınan rızaya uygun olarak sadece katma değerli elektronik haberleşme hizmetlerinin, pazarlama faaliyetlerinin ve benzer hizmetlerin gerektirdiği ölçü ve sürede işlenebilir.

(4) **(Değişik:RG-11/7/2013-28704)** Abonelere/kullanıcılara ait işlenen ve saklanan trafik verileri, bu verilerin işlenmesini ve saklanmasını gerekli kılan faaliyetin tamamlanmasından sonra silinir veya anonim hale getirilir.

(5) İşletmeciler, abonelerin/kullanıcıların, kısa mesaj, çağrı merkezi, internet ve benzeri yöntemlerle vermiş oldukları rızayı aynı yöntem ya da basit bir yöntem ile her zaman ücretsiz olarak geri almalarına imkân sağlar.

MADDE 9 – Trafik verisini işleme yetkisi

(Değişik:RG-11/7/2013-28704)

(1) Trafik verisini işleme yetkisi; trafik yönetimi, arabağlantı, faturalama, yolsuzluk tespitleri, tüketici şikâyetlerinin değerlendirilmesi, elektronik haberleşme hizmetlerinin pazarlanması veya katma değerli elektronik haberleşme hizmetlerinin sunulması hususlarında işletmeci ve işletmeci tarafından yetkilendirilen kişilerle sınırlıdır.

MADDE 10 – Trafik verisinin bildirilmesi

(1) Trafik verisi, arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü, tüketici şikâyetlerinin değerlendirilmesi ve denetim faaliyetlerinin gerçekleştirilmesi amacıyla yazılı olarak talep edilmesi halinde kanunların yetkili kıldığı mercilere verilir.

MADDE 11 – Konum verisinin işlenmesi

(Değişik:RG-11/7/2013-28704)

(1) Katma değerli elektronik haberleşme hizmetleri sunmak amacıyla ihtiyaç duyulan ve trafik verisi niteliğinde olmayan konum verileri, anonim hale getirilerek veya ilgili abonelerin/kullanıcıların işlenecek konum verileri, işleme amacı ve süresi hakkında bilgilendirilmelerinden sonra rızalarının alınması kaydıyla, alınan rızaya uygun olarak sadece katma değerli elektronik haberleşme hizmetlerinin gerektirdiği ölçü ve sürede işlenebilir. İşletmeciler trafik verisi niteliğinde olmayan konum verilerinin işlenmesinde abone/kullanıcılara geçici olarak bu verilerin işlenmesini reddetme imkânı sağlar.

(2) İşletmeciler, abonelerin/kullanıcıların trafik verisi niteliğinde olmayan konum verilerinin işlenmesi için, kısa mesaj, çağrı merkezi, internet ve benzeri yöntemlerle vermiş oldukları rızayı aynı yöntem ya da basit bir yöntem ile her zaman ücretsiz olarak geri almalarına imkân sağlar.

(3) İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, ancak afet ve acil durum halleri ile acil yardım çağrıları kapsamında abonenin/kullanıcının rızası aranmaksızın konum verisi ve ilgili kişilerin kimlik bilgileri işlenebilir.

MADDE 12 – Konum verisini işleme yetkisi

(Değişik:RG-11/7/2013-28704)

(1) Konum verisini işleme yetkisi, katma değerli elektronik haberleşme hizmetlerinin sunulması hususunda ya da afet ve acil durum halleri ile acil yardım çağrıları kapsamında işletmeci ve işletmeci tarafından yetkilendirilen kişilerle sınırlı olup, bu yetki söz konusu hizmetlerin gerektirdiği kapsamda kullanılır.

MADDE 13 – Saklanacak veri kategorileri

(1) Bu Yönetmelik kapsamında saklanması öngörülen veri kategorileri, aşağıda belirtilmiştir.

a) Haberleşmenin takibi ve kaynağının tanımlanması için:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; gerçekleşmeyen aramalar da dâhil olmak üzere haberleşmenin başlatıldığı hatta ait telefon numarası, abonenin adı ve adresi, hattın hangi tarihte hangi aboneye tahsis edildiğine ait bilgi.

2) İnternet ortamına erişim, elektronik posta ve internet telefonu ile ilgili olarak; tahsis edilmiş kullanıcı kimliği ve/veya telefon numarası, haberleşmenin gerçekleştiği andaki internet protokol adresi, abonenin/kullanıcının adı ve adresi.

b) Haberleşmenin sonlandırılacağı noktayı belirlemek için:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; haberleşmenin sonlandırıldığı/sonlandırılacağı numara veya numaralar, çağrı iletme ve çağrı transferi gibi ek hizmetlerin olması durumunda çağrının yönlendirildiği numara veya numaralar, abonelerin adı ve adresi.

2) Elektronik posta ve internet telefonu ile ilgili olarak; elektronik posta alıcılarına ait kullanıcı kimliği, internet telefonu ile aranan alıcılara ait kullanıcı kimliği veya telefon numarası, internet telefonu veya elektronik posta alıcılarının adı ve adresi.

c) Haberleşmenin tarihi, zamanı ve süresini belirlemek için:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; haberleşmenin başlangıç ile bitiş tarih ve zamanı.

2) **(Değişik:RG-11/7/2013-28704)** İnternet erişimi, elektronik posta ve internet telefonu ile ilgili olarak; internet erişimi ile ilgili oturum açma, kapatma tarihi ve zamanı, tahsis edilen dinamik veya statik internet protokol adresi, NAT kullanılan şebekelerde internet protokol adresi yanında port bilgisi, abone/kullanıcı kimliği, elektronik posta veya internet telefonu ile ilgili oturum açma ile kapatma tarihi ve zamanı.

ç) Haberleşmenin türünü tanımlamak için:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; kullanılan elektronik haberleşme hizmeti.

2) Elektronik posta ve internet telefonu ile ilgili olarak; kullanılan internet hizmeti.

d) Kullanıcıların haberleşme cihazlarını veya bunların ekipmanlarını tanımlamak için:

1) Sabit telefon hizmetiyle ilgili olarak; haberleşmenin başlatıldığı ve sonlandırıldığı telefon numaraları.

2) **(Değişik:RG-11/7/2013-28704)** Mobil telefon hizmetiyle ilgili olarak; haberleşmenin başlatıldığı ve sonlandırıldığı telefon numaraları, haberleşmenin başlatıldığı ve/veya sonlandırıldığı tarafa ait IMSI ve IMEI

numaraları; abone kaydı olmayan arama kartlı hizmetlerin olması durumunda hizmetin aktif hale getirildiği tarih ve zaman ile hizmetin aktif hale getirildiği hücre kimliği.

3) İnternet ortamına erişim, elektronik posta ve internet telefonu ile ilgili olarak; çevirmeli ağ erişimi için arayan telefon numarası, sayısal abone hattı numarası ya da haberleşmenin kaynaklandığı diğer nokta.

e) İlgili mevzuatın öngördüğü hallerde mobil haberleşme cihazının konumunu tespit etmek için; haberleşmenin başladığı hücre kimliği, haberleşme verilerinin saklandığı sürede hücre kimlikleri ile ilgili olarak hücrelerin coğrafi konumlarını tanımlayan veri, hücre adresi ve hücre kimliğinin o adrese atanma ve kaldırılma tarihleri.

(2) Bu Yönetmelik kapsamında, elektronik posta ve internet telefonu ile ilgili olarak verilerin saklanmasına ilişkin getirilen yükümlülükler, sadece işletmecilerin kendilerinin sundukları hizmetler ile sınırlıdır.

MADDE 14 – İşletmecilerin veri saklama süreleri

(Değişik:RG-11/7/2013-28704)

(1) 13 üncü madde kapsamında tanımlanan veri kategorileri, haberleşmenin yapıldığı tarihten itibaren bir yıl, gerçekleşmeyen aramalara ilişkin kayıtlar ise üç ay süre ile saklanır.

(2) Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler, ilgili süreç tamamlanıncaya kadar saklanır.

(3) Kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları dört yıl süre ile saklanır.

MADDE 15 – Saklanan verinin korunması ve güvenliği

(1) Bu Yönetmelik kapsamında saklanması öngörülen veriler için işletmeciler asgari olarak;

a) Saklanan veriler ile şebekedeki diğer verilerin aynı kalite, güvenlik ve koruma özelliklerine tabi olmasını,

b) **(Değişik:RG-11/7/2013-28704)** Verilerin yurt içinde saklanmasını,

c) Saklanan verilerin, istem dışı, yetki dışı ya da yasa dışı, erişim, tahrip, kayıp, değişiklik, depolama, işleme ve ifşasına karşı uygun teknik ve idari tedbirlerin alınmasını,

ç) Verilerin sadece özel yetkilendirilmiş kişiler tarafından erişilebilir olmasının sağlanması için uygun teknik ve idari tedbirlerin alınmasını,

d) **(Değişik:RG-11/7/2013-28704)** İşlenen ve saklanan verinin, saklama süresinin bitiminden itibaren en geç bir ay içinde imha edilmesi veya anonim hale getirilmesi ve bu işlemlerin tutanakla veya sistemsel olarak kayıt altına alınmasını

sağlamakla yükümlüdür.

(2) İşletmeciler sundukları hizmetler kapsamında elde ettikleri verilerin güvenliğini, bütünlüğünü, gizliliğini ve erişilebilirliğini her aşamada sağlamakla yükümlüdür. Bu yükümlülük işletmeci tarafından yetkilendirilmiş kişiler marifetiyle yapılan işlemleri de kapsar.

(3) İşletmeciler, kanunların yetkili kıldığı mercilerce talep edilmesi halinde, saklanan veri ve söz konusu veriye ilişkin gerekli tüm bilgileri gecikmeksizin sağlamakla yükümlüdür.

MADDE 16 – İstatistikî bilgilerin verilmesi

(1) İşletmeciler son bir yıl içerisinde;

a) Yetkili merciler tarafından ilgili mevzuatı çerçevesinde talep edilen verilerin kategorileri ve talep edilme sayılarına,

b) Verinin saklanmaya başlandığı tarih ile yetkili merciler tarafından talep edildiği tarih arasında geçen süreye,

c) Veri talebinin karşılanamadığı durumlara,

ilişkin istatistikî bilgileri saklamakla ve talep halinde Kuruma göndermekle yükümlüdür.

(2) Bu maddenin birinci fıkrasında belirtilen istatistikî bilgiler, kişisel verileri içermez.

DÖRDÜNCÜ BÖLÜM / SAĞLANAN İMKÂNLAR

MADDE 17 – Numaranın gizlenmesi

(1) İşletmeci, arayan numaranın görünmesine imkân sağladığı durumlarda;

a) **(Değişik:RG-11/7/2013-28704)** Arayan kullanıcıya basit bir yöntemle ve ücretsiz olarak numarasını gizleme imkânı sağlamakla,

b) Aranan aboneye basit bir yöntemle ve ücretsiz olarak, gelen aramalarda arayan numaranın gösterilmesini engelleme imkânı sağlamakla,

c) Arayan kişinin numarasını gizlemesi halinde, aranan abonenin/kullanıcının isteğine bağlı ve ücretsiz olarak, gelen aramaların abone/kullanıcı tarafından reddedilmesine imkân sağlamakla

yükümlüdür.

(2) **(Değişik:RG-11/7/2013-28704)** İşletmeci, bağlanılan numaranın görünmesine imkân sağladığı durumlarda, bağlanılan aboneye basit bir yöntemle ve ücretsiz olarak, bağlanılan numaranın arayan kullanıcıya gösterilmesini engelleme imkânı sağlamakla yükümlüdür.

(3) İşletmeci, bu maddenin birinci ve ikinci fıkrasında belirtilen hizmet imkânları hakkında abonelerini/kullanıcılarını kısa mesaj, internet, basın, yayın organları, posta veya benzeri araçlarla ücretsiz olarak bilgilendirmekle yükümlüdür.

(4) Arayan numaranın gizlenmesi imkânı, acil yardım çağrıları için geçerli değildir.

MADDE 18 – Otomatik çağrı yönlendirme

(1) **(Mülga:RG-11/7/2013-28704)**

(2) İşletmeciler tarafından başka bir numaraya veya otomatik mesaj sistemine yapılan yönlendirmelerin ücretli olması halinde abonenin/kullanıcının rızası alınır.

MADDE 19 – Aboneler için hazırlanan rehberler

(1) Aboneler, basılı ve/veya elektronik abone rehberlerinin, yayımlanma amaçları ve bu rehberlerde yer alacak kişisel veriler ile bu rehberlerin elektronik sürümlerinde olabilecek sorgulama seçenekleri ve kullanım imkânları hakkında rehbere kaydedilmeden önce ücretsiz olarak bilgilendirilirler.

(2) Kamuya açık rehberlerde yer alan kişisel veriler, rehberlik hizmetinin amaç ve kapsamına uygun olarak belirlenir.

(3) Abone rehberlerinde yer almayı kabul eden aboneler, rehberlerde yer alan kişisel verilerinin düzeltilmesini, teyit edilmesini ve/veya çıkarılmasını ücretsiz ve basit bir yöntemle talep edebilirler.

(4) Rehberlik hizmeti kapsamında yapılacak sorgulamalarda, Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği'nin Elektronik Haberleşme Hizmet, Şebeke ve Altyapılarının Tanım, Kapsam ve Süreleri ile ilgili 27 nci maddesi kapsamında yapılan düzenlemeler esastır.

MADDE 20 – Ayrıntılı faturalarda gizlilik

(1) İşletmeciler, ayrıntılı fatura gönderdikleri abonelerin talep etmeleri halinde, fatura ayrıntısında yer alan telefon numaralarının bazı rakamlarının gizlenmesini sağlar.

BEŞİNCİ BÖLÜM /
ÇEŞİTLİ VE SON HÜKÜMLER

MADDE 21 – İdari para cezaları ve diğer yaptırımlar

(1) İşletmecilerin bu Yönetmelik ile belirlenen yükümlülükleri yerine getirmemeleri halinde 5/9/2004 tarihli ve 25574 sayılı Resmî Gazete'de yayımlanan Telekomünikasyon Kurumu Tarafından İşletmecilere Uygulanacak İdari Para Cezaları ile Diğer Müeyyide ve Tedbirler Hakkında Yönetmelik hükümleri uygulanır.

MADDE 22 – Hüküm bulunmayan haller

(1) Bu Yönetmelikte hüküm bulunmayan hallerde, Tebliğ veya Kurul Kararı ile düzenleme yapılır.

MADDE 23 – Yürürlükten kaldırılan yönetmelik

(1) 6/2/2004 tarihli ve 25365 sayılı Resmî Gazete'de yayımlanan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik yürürlükten kaldırılmıştır.

MADDE 24 – Atıflar

(1) Mevzuatta 6/2/2004 tarihli ve 25365 sayılı Resmî Gazete'de yayımlanan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğe yapılan atıflar bu Yönetmeliğe yapılmış sayılır.

GEÇİCİ MADDE 1 – Mevcut düzenlemelerin durumu

(1) Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğe dayanılarak yapılan usul ve esaslar, alınan Kurul Kararları ile diğer idari işlemlerin bu Yönetmeliğe aykırı olmayan hükümleri konuya ilişkin yeni bir işlem yapılana kadar geçerliliğini muhafaza eder.

MADDE 25 – Yürürlük

(Değişik:RG-11/7/2013-28704)

(1) Bu Yönetmeliğin;

a) 4 üncü maddesinin ikinci fıkrası 1/1/2014,

b) diğer hükümleri 24/7/2013,

tarihinde yürürlüğe girer.

MADDE 26 – Yürütme

(1) Bu Yönetmelik hükümlerini Bilgi Teknolojileri ve İletişim Kurumu Başkanı yürütür.

	Yönetmeliğin Yayımlandığı Resmî Gazete'nin	
	Tarihi	**Sayısı**
	24/7/2012	28363
	Yönetmelikte Değişiklik Yapan Yönetmeliklerin Yayımlandığı Resmî Gazetelerin	
	Tarihi	**Sayısı**
1.	15/2/2013	28560
2.	11/7/2013	28704

§ DİĞER BAZI DÜZENLEMELER

ALMAN FEDERAL VERİ KORUMA KANUNU

Düzenlemenin orijinal ismi: *Bundesdatenschutzgesetz (BDSG)*
Düzenlemenin künyesi: *Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814)*
Düzenlemenin orijinal metni için:
http://www.bfdi.bund.de/SharedDocs/Publikationen/GesetzeVerordnungen/BDSG.pdf?__blob=publicationFile
Düzenlemenin İngilizce metni için:
http://www.gesetze-im-internet.de/englisch_bdsg/federal_data_protection_act.pdf

İSVİÇRE FEDERAL VERİ KORUMA KANUNU

Düzenlemenin orijinal ismi: *Bundesgesetz über den Datenschutz*
Düzenlemenin künyesi: *The Federal Assembly of the Swiss Confederation's decision date: 19 June 1992, In force 1 July 1993.*
Düzenlemenin orijinal metni (ALM.) için:
https://www.admin.ch/opc/de/classified-compilation/19920153/201401010000/235.1.pdf ***Düzenlemenin İngilizce metni için:***
https://www.admin.ch/opc/en/classified-compilation/19920153/201401010000/235.1.pdf

§ İÇTİHATLAR

YARGITAY HUKUK GENEL KURULU'NUN "UNUTULMA HAKKI" KARARI, 17.6.2015

T.C. YARGITAY HUKUK GENEL KURULU E. 2014/4-56 K. 2015/1679 T. 17.6.2015

• UNUTULMA HAKKI (Davacının Geçmişte Yaşadığı Kötü Bir Olayın Toplum Hafızasından Silinmesini Unutularak Geleceğini Serbestçe Şekillendirmek İstediği/ Bu Hakkın Yalnızca Dijital Ortamdaki Kişisel Veriler İçin Değil Kamunun Kolayca Ulaşabileceği Yerde Tutulan Kişisel Verilere Yönelik Olarak da Kabul Edilmesi Gerektiği - Davacının İsminin Rumuzlanmadan Kitapta Yer Almasının Unutulma Hakkını İhlal Ettiği)

• ÖZEL HAYATIN GİZLİLİĞİNİ İHLAL (Dört Yıl Önce Gerçekleşen Bir Olayın Mağduru Olan Kişinin Adının Açık Bir Şekilde Yazılarak Kitapta Yer Alması Halinde Unutulma Hakkının Bunun Sonucunda da Davacının Özel Hayatının Gizliliğinin İhlal Edildiğinin Kabulü Gerektiği - Manevi Tazminat)

• YARGI KARARLARINDA ADI GEÇEN KİŞİLERİN RUMUZLANMADAN KİTAPTA YER ALMASI (Manevi Tazminat Davası - Dört Yıl Önce Gerçekleşen Bir Olayın Mağduru Olan Kişinin Adının Rumuzlanmadan Açık Bir Şekilde Yazılarak Kitapta Yer Almasının Davacının Özel Hayatının Gizliliğinin İhlal Ettiğinin Kabulü Gerektiği)

• MANEVİ TAZMİNAT DAVASI (Kişilik Hakkına Saldırı Nedenine Dayalı - Davacının İsminin Rumuzlanmadan Kitapta Yer Almasının Unutulma Hakkını ve Bunun Neticesinde Özel Hayatın Gizliliğini İhlal Ettiği Dikkate Alındığında Davacı Lehine Manevi Tazminat Koşullarının Gerçekleştiğinin Kabulü Gerektiği)

• KİŞİLİK HAKLARINA SALDIRI (Davacının Unutulma Hakkı İle Özel Hayatına İlişkin Kişisel Verilerinin Üçüncü Kişiler Tarafından Bilinmemesini Aradan Geçen Süre Nedeniyle Toplum Hafızasından Silinmesini İstediği - Davacının İsminin Rumuzlanmadan Kitapta Yer Almasının Unutulma Hakkını İhlal Ettiği/Manevi Tazminat Davası)

2709/m.20

4721/m.24

ÖZET : Dava, kişilik hakkına saldırı nedenine dayalı tazminat istemine ilişkindir. Davacı, kamu görevinin veya hizmet ilişkisinin sağladığı nüfuzu kötüye kullanarak, müteselsilen cinsel saldırı suçunun mağdurudur. 2006 yılında gerçekleşen eylem tarihinde davacı bekâr olup maruz kaldığı eylem geleceği açısından etkilidir. Yapılan

yargılama sonunda kamu görevlisi olan sanık ceza almıştır. Temyiz istemi üzerine yapılan inceleme sonunda ise hüküm 2009 yılında onanmıştır. Mağdur davacı gerek hazırlık gerekse de yargılama sırasında cinsel saldırının nasıl gerçekleştiğini açık bir şekilde anlatmış, bu anlatımlar doğal olarak karar metnine geçirilmiştir. Karar mağdur ve sanığın ismi rumuzlanmadan 2010 yılı nisan ayında yayınlanan kitapta yer almıştır. Hemen ifade edilmelidir ki; davacının rızası dışında bir kitapta geçen ismi kişisel veri niteliğindedir. Ayrıca şunun da ifade edilmesi gereklidir ki; unutulma hakkı tanımlarına bakıldığında her ne kadar dijital veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki **kişisel veri**ler için değil, kamunun kolayca ulaşabileceği yerde tutulan **kişisel veri**lere yönelik olarak da kabul edilmesi gerektiği açıktır. Davacı, geçmişte yaşadığı kötü bir olayın toplum hafızasından silinmesini istemektedir. Unutulma hakkı ile geçmişindeki yaşanan talihsiz bir olayın unutularak geleceğini serbestçe şekillendirmek, diğer bir deyişle hayatında, yeni bir sayfa açma olanağı istemektedir. Kaldı ki, davacı da yargılama sırasında verdiği dilekçelerinde bu istem üzerinde ısrarla durmuştur. Davacı unutulma hakkı ile özel hayatına ilişkin **kişisel veri**lerinin üçüncü kişiler tarafından bilinmemesini, aradan geçen süre nedeniyle toplum hafızasından silinmesini istemektedir. Bu bağlamda değerlendirildiğinde; 4 yıl önce gerçekleşen bir olayın mağduru olan kişinin adının açık bir şekilde yazılarak kitapta yer alması halinde unutulma hakkının bunun sonucunda da davacının özel hayatının gizliliğinin ihlal edildiği kabul edilmelidir. O halde davacının isminin rumuzlanmadan kitapta yer almasının unutulma hakkını ve bunun neticesinde özel hayatın gizliliğini ihlal ettiği dikkate alındığında davacı lehine manevi tazminat koşullarının gerçekleştiğinin kabulü zorunludur.

DAVA : Taraflar arasındaki "manevi tazminat" davasından dolayı yapılan yargılama sonunda; İzmir 3. Asliye Hukuk Mahkemesince davanın kısmen kabulüne dair verilen 11.04.2011 gün ve 2010/399 E. 2011/172 K. sayılı kararın incelenmesi taraflar vekili tarafından istenilmesi üzerine, Yargıtay 4. Hukuk Dairesinin 08.11.2012 gün ve 2011/7193 E. 2012/16450 K. sayılı ilamı ile;

(... Dava, haksız fiil nedeni ile manevi tazminat istemine ilişkindir. Yerel mahkemece istemin bir bölümü kabul edilmiş; karar, taraflarca temyiz olunmuştur

Davacı vekili, müvekkilinin cinsel taciz suçundan şikayetçi olduğu ceza davasının yapılan yargılaması sonucunda, mahkeme ilamının temyizi sonrasında Yargıtay'ca verilen kararın davalılara ait Yorumlu-Uygulamalı Türk Ceza Kanunu adlı altı ciltlik eserde müvekkilinin ve diğer kişilerin isimlerinin açıkça yazılmak suretiyle yayınlandığını, bu durumun kişilik haklarına saldırı oluşturduğunu, belirterek davalıların manevi tazminatla sorumlu tutulmalarını talep etmiştir.

Davalılar vekili, söz konusu kitapların bilimsel eser niteliğinde olduğu, Avrupa İnsan Hakları Mahkemesi kararlarında davaların davacıların ismiyle adlandırıldığı, kitabın geniş kitlelere hitap etmediği, ceza hakimleri, savcılar ve ceza avukatlarınca okunduğu, kitapta isim belirtmenin hukuka aykırı olmadığını belirterek davanın reddini talep etmiştir.

Mahkemece, adı geçen eserde davacı ve diğer kişilerin isimlerinin kodlanmadan açıkça yazıldığı, söz konusu olayların anlatımında açıkça isim belirtmenin kitap içeriğine bir fayda sağlamadığı gibi, davacının isminin geçtiği olayın hassasiyeti ve Türk toplum yapısı da göz önünde tutulduğunda, yurt çapında dağıtımı ve satışı yapılan bir kitapta, bu tür bir olayla davacının adının açıkça belirtilmesinin davacının kişilik haklarını zedelediği, çevresine karşı davacıyı zor duruma düşürdüğü gerekçesi ile davanın kısmen kabulüne karar verilmiştir.

Bilimsel bilgi, taşıdığı özellikler dolayısıyla fikir üretiminin en yüce değer ve biçimi olma niteliğine haizdir ve herşeyden önce, insanlığın gerçekliğe ulaşması bakımından önemli bir araç sayılır. Bu durum, bilimsel bilgi ve

onu üreten araştırmacının geniş bir özgürlük alanında bulunmasını gerektirir. Bilimi serbestçe öğrenme, araştırma, yayma ve öğretme haklarını içeren bilim özgürlüğü Anayasada kişisel haklar arasında (madde 27) düzenlenmiştir. Anılan madde de herkesin bilim ve sanatı serbestçe öğrenme ve öğretme, açıklama ve yayma ve bu konularda araştırma yapma hakkına sahip olduğu belirtilmektedir. Keza, AB Temel Haklar Bildirgesinin 13. maddesinde "sanat ve bilimsel araştırma kısıtlamaya tabi olmamalıdır. Akademik özgürlüğe saygı gösterilmelidir" ibaresine yer verilmiştir. Bu bağlamda bilimsel özgürlük, bilimsel bir etkinlikte bulunan veya böyle bir faaliyette bulunmak isteyen tüm bireylere tanınmış ve bu bireylerin kişiliğine sıkı sıkıya bağlı kalmış, öznel temel haktır.

Taşıdığı önem dolayısıyla insan hakları belgelerine giren bilim özgürlüğü, araştırma özgürlüğünü, araştırma için zorunlu araçlara ve ortama sahip olma hakkını ve bilimsel üretme özgürlüğü veya bilgilendirme ve yayın hakkını içerir. Bu çerçevede bilim adamı bilimsel metotlarını kullanarak araştırma yapma hakkına ve bu araştırmanın sonuçlarını yayma hakkına sahip olacak, kural olarak bu konularda dış bir engelle karşılaşmayacaktır. Hatta bu konularda karşılaşacağı maddi ve manevi engeller devlet tarafından ortadan kaldırılacaktır.

Düşünce özgürlüğünün bir alt kategorisi olan fakat, üretilmesindeki özel çabanın ya da emeğin doğal sonucu olarak, sıradan düşünceye göre daha sistematik ve derin sayılması gereken bilimsel eserler, kural olarak ancak kendi ilkeleri çerçevesinde sınır tanırlar ve istisnaen ancak insan yaşamına yönelen bir tehlike olasılığında kısıtlanabilirler. Bunun ötesine geçilerek yapılan sınırlamalar, toplumun bilimsel düşüncelerle buluşmasını önleyebilecek ve dolayısıyla gerçekliğe ulaşılmasını engelleyebilecektir. Bu bakımdan bilimsel özgürlük hukuki rejim ve yaptırım açısından diğer entelektüel özgürlüklere göre daha mutlak bir özgürlük rejiminden yararlanmasını gerektirir. Fakat tüm özgürlüklerde olduğu gibi bilimsel özgürlük de sınırsız değildir. Bilim özgürlüğü ile kişilerin, kişilik değerlerinin karşı karşıya geldiği durumlarda somut olaydaki olgular itibariyle koruma altına alınmış bulunan bu iki değerden birinin diğerine üstün tutulması gerekecektir.

Davaya konu olayda; bilimsel araştırma özgürlüğü kapsamında, aleniyet kazanmış ve kamu malı haline gelmiş Yargıtay ilamı, tarafların isimleri kodlanmadan davalıların yazmış oldukları Yorumlu-Uygulamalı Türk Ceza Kanunu adlı altı ciltlik bilimsel çalışma ürünü olan kitapta yayınlanmıştır. Adı geçen eserin bilimsel nitelikli bir çalışma olduğu, kamuya açık hale gelen Yargıtay kararının bilimsel çalışma ürünü olan kitapta olduğu gibi yer almasından dolayı yukarıda anlatılan ilkeler ğereği davalıların sorumlu tutulamayacağı, çatışan yararlar dengesinin davacı aleyhine bozulmadığı, bu olayın davacının kişilik haklarına saldırı teşkil etmeyeceği gözetilerek davanın tümden reddine karar verilmesi gerekirken, yazılı biçimde karar verilmiş olması usul ve yasaya uygun düşmediğinden kararın bozulması gerekmiştir...),

Gerekçesiyle bozularak dosya yerine geri çevrilmekle, yeniden yapılan yargılama sonunda; mahkemece önceki kararda direnilmiştir.

Hukuk Genel Kurulunca incelenerek direnme kararının süresinde temyiz edildiği anlaşıldıktan ve dosyadaki kağıtlar okunduktan sonra gereği görüşüldü:

KARAR : Dava, kişilik hakkına saldırı nedenine dayalı tazminat istemine ilişkindir.

Davacı M. T. vekili 16/08/2010 harç tarihli dava dilekçesinde özetle; "müvekkilinin 14/11/2003 tarihinden beri İzmir Adliyesinde savcılık zabıt katibi olarak görev yaptığını, 18/07/2005 ile 11/04/2006 tarihleri arasında o dönem İzmir C. Başsavcı vekili olarak görev yapan Z. ile çalışmak için görevlendirildiğini ancak başladıktan sonra 8 ay boyunca Başsavcı vekilinin sözlü ve fiziksel taciziyle karşı karşıya kaldığını, fiziksel tacizin başlaması ve bu durumun çekilmez hale gelmesi nedeniyle davacının şikayette bulunduğunu, ailesinin ve çevresinin

duymaması için çaba sarf ettiğini, Z. hakkında soruşturma açıldığını ve cezalandırıldığını, sanığın Başsavcı vekili olması nedeni ile olayların o dönem için basında yer aldığını, davacının bu olayları unutmaya başladığı bir dönemde Yargıtay 4. Ceza Dairesi Başkanı ve tetkik hakimleri olan davalıların Nisan 2010 tarihinde yorumlu-uygulamalı Türk Ceza Kanunu adlı altı ciltlik eser yayınladıklarını, örnek Yargıtay kararlarının başladığı 3262 nolu sayfa ve devamındaki sayfalarda davacının başına gelen olayların, tüm aktörlerin isimlerinin açıkça yazılmak suretiyle ve olayın tamamının açık bir şekilde anlatıldığını, davacı tarafından bu durumun öğrenilmesiyle davacının tekrar psikolojik bunalıma girdiğini, bütün kötü olayları tekrar yaşamak zorunda kaldığını, adliyede çalışması nedeniyle bu olayın davacının çevresinde, savcı ve avukatlar tarafından duyulduğunu, müvekkilinin zor da olsa saklayabildiği bir olayın kamuoyuna duyurulduğunu, iffetinin tartışılır hale geldiğini, bir genç kızın hayalleri ve geleceğinin kararmış olduğunu, eserin bir defa yararlanılacak bir eser olmadığını, uzun yıllar boyunca yaygın kitlelerce okunacak nitelikte bulunduğunu belirterek tüm bu nedenlerle davacının isminin geçtiği söz konusu ciltlerin toplatılmasını, 50.000,00-TL manevi tazminatın davalılardan tahsiline karar verilmesini istemiştir.

Davalılar O. Y., H. T. G., M. A. ve A... Ltd. Şti. vekili 11.10.2010 havale tarihli cevap dilekçesinde özetle; " Söz konusu kitapların bilimsel eser niteliğinde olduğunu, bilimsel eser niteliğinde olan kitaplarda fail ve mağdur adının olmasının hukuka aykırı olmadığını, ceza hukukundaki kitaplarının kaynağının yargısal kararlar olduğunu, geniş kitlelere hitap etmediğini, ceza hakimleri, savcılar ve ceza avukatlarınca okunduğunu, kitapta isim belirtmenin hukuka aykırı olmadığını, eserde adı geçen kişilerle ilgili vakıalar daha önce yargı konusu olduğu için ilgili mahkemelerin bulunduğu yerlerdeki kişiler tarafından duyulup öğrenildiğini, bu nedenle sözü edilen vakıaların ilk defa dava konusu eserde gündeme getirilmediğini, AİHM kararlarının ve Anayasa Mahkemesi kararlarının da isimler çıkarılmadan yayınlandığını, 2011 yılının başından itibaren UYAP sisteminde bulunan kararlardaki **kişisel veri**ler rumuzlanmadan hakim ve savcının kullanımına açıldığını, dava konusu kararın son bölümünde rumuzlama yapılmış ise de ilk bölümünde yapılmamasının dizgi hatası olduğunu, olayın üzerine adliyeye gelen müfettişin yaptığı soruşturma sırasında tüm adliyenin olayı öğrendiğini ve olayın basına da yansıdığını, yine davacının ileri sürdüğü hususların daha sonra düzeltildiğini ve düzeltilmiş bir nüshasının davacı vekilini sunulduğunu bu nedenle kitabın toplatılmasına gerek olmadığını istenen tazminatın fahiş olduğunu savunarak" davanın reddine karar verilmesini talep etmiştir.

Mahkemece, davanın kısmen kabulüne dair verilen kararın taraflarca temyiz edilmesi üzerine yukarıda başlık bölümde yazılan Yargıtay ilamı ile bozulmuş, karar düzeltme istemi oyçokluğu ile reddedilmiş, mahkemece önceki gerekçeler tekrar edilerek direnilmiş; hükmü davalılar vekili temyize getirmiştir.

Hukuk Genel Kurulu önüne gelen uyuşmazlık; davalılar O. Y., H. ve M. A. tarafından yayına hazırlanan ve davalılardan A... Ltd. Şti. tarafından basılan eserde yer alan kararda, davalının isminin rumuzlanmadan ve rızası alınmadan açık bir şekilde yazılmasının kişilik hakkında saldırı oluşturup oluşturmayacağı noktasında toplanmaktadır.

İşin esasına girilmeden önce davacıya ait 13.01.2014 tarihli dilekçenin temyiz harcının tahsil edilip edilmediğinin belirlenmesi için dosyanın mahkemesine geri çevrilmesinin gerekip gerekmediği ön sorun olarak tartışılmış, şu sonuca varılmıştır:

Davacı vekiline gerekçeli karar 09.12.2013 tarihinde tebliğ edilmiştir. 15 günlük yasal temyiz süresi geçtikten sonra davacı vekili tarafından mahkemeye verilmiş bir dilekçe olmamasına rağmen 25.12.2013 (Çarşamba) tarihinde yazı işleri müdürü tarafından davacıdan temyiz harcı tahsil edilmesi için müzekkere yazılmıştır. Ancak

temyiz harcının tahsiline dair tahsilât makbuzu dosya içinde bulunmamaktadır. Bir diğer deyişle süresi içinde harcı yatırılmış davacıya ait bir temyiz dilekçesi dosya içinde bulunmamaktadır. Davalılara ait temyiz dilekçesi ise 30.12.2013 tarihinde davacı vekiline tebliğ edilmiştir. 10 günlük yasal karşı temyiz süresi 09.01.2014 (Perşembe) sona erdikten sonra davacı vekili (dilekçe tarihi: 13.01.2014 pazartesi havale tarihi 13.01.2014) temyize cevap dilekçesi vermiş direnme kararının onanmasını; az olan miktar yönünden dosyanın incelenmek üzere Yargıtay 4. Hukuk Dairesine gönderilmesi istenilmiştir. Bu nedenle davacının hem asıl hem de karşı temyiz süresini geçirdikten sonra verdiği dilekçe nedeni ile dosyanın geri çevrilmesine gerek olmadığı oybirliği ile kabul edilmiştir.

İşin esasına gelince; uyuşmazlığın çözümünde etkili yasal mevzuata bakılacak olursa;

Avrupa İnsan Hakları Sözleşmesinin ilgili maddeleri;

Özel ve aile hayatına saygı hakkı

1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla .öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, .düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

şeklindedir.

Türkiye Cumhuriyeti Anayasası'nın ilgili maddeleri;

"IX. Bilim ve sanat hürriyeti

Madde 27 – Herkes, bilim ve sanatı serbestçe öğrenme ve öğretme, açıklama, yayma ve bu alanlarda her türlü araştırma hakkına sahiptir.

..."

"A. Özel hayatın gizliliği

Madde 20 – Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Üçüncü cümle mülga: 3/10/2001-4709/5 md.)

…

(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili **kişisel veri**ler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. **Kişisel veri**ler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. **Kişisel veri**lerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

şeklindedir.

Türk Medeni Kanunu'nun ilgili maddeleri;

“II. Saldırıya karşı

1. İlke

Madde 24- Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.”

şeklindedir.

Önümüze gelen sorunun temelinde unutulma hakkı ve bunun sonucu olan **kişisel veri**lerin ve kişilik hakkının korunması ile bilim ve sanat hürriyetinin birbiri karşısında sınırlarının belirlenmesi yatmaktadır. Sorunun çözümünde dikkat edilmesi gereken husus, bilim ve sanat özgürlüğü ile bireyin temel hakları arasında adil bir dengenin kurulmasıdır.

Kişisel veri belli veya belirlenebilir olan gerçek veya tüzel bir kişiye ilişkin her türlü bilgiyi ifade eder. Avrupa Birliği'nin 95/46/EC sayılı Bireylerin **Kişisel Veri**lerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Direktif'in 2/a ve Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi'nin 2 (a) maddelerinde benzer tanımlama yer almaktadır.

Kişisel verilerin korunması insan haklarıyla yakından ilişkilidir. Çünkü **kişisel veri**lerin açıklanması öncelikle özel hayatın gizliliğini ihlal edilebileceği gibi bir takım diğer bağlantılı hakları da zarar görebilir.

AİHS'de kişisel verilerle ilgili bir hüküm yoktur. Ancak mahkeme konuyla ilgili kararlarında **kişisel veri** içeriğini doldurmuştur. Hemen ifade edilmesi gerekir ki **kişisel veri**nin sayısal olarak sınırlandırılması mümkün değildir. Ancak içtihatlar ve akademik yayınlar dikkate alındığında bireyin kimliğini ortaya çıkartan, bir kişiyi belirli kılan ve karakterize eden kişinin kimlik, ekonomik ve dijital bilgileri, tabiiyeti, kanaatleri, ırk, siyasî düşünce, felsefî inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık bilgileri, fotoğrafları, parmak izi, sağlık verileri, telefon mesajları, telefon rehberi, sosyal paylaşım sitelerinde yazdığı veya paylaştığı yazı, fotoğraf, ses veya görüntü kayıtları**kişisel veri**leri olarak kabul edilebilir.

Kişisel verilerin korunması, çağımızda, insan hakları kavramı ve korunması bilincinin gittikçe gelişmesine paralel olarak önemini artırmaktadır. **Kişisel veri**lerin korunması hakkının temel amacı, bireyin özel yaşamının gizliliğinin güvence altına alınması yoluyla kişiyi korumaktır. Bilgi toplumunda giderek oldukça önemli bir konu haline gelen **kişisel veri**lerin korunması hakkı, bireyin, demokratik bir hukuk devletinde özgür iradesiyle kendi yaşamını bizzat düzenleyebilmesinin bir gereği olarak karşımıza çıkmaktadır. Diğer taraftan bireyin kişiliğini serbestçe geliştirmesi, kişiliğinin korunması ve özgür bireylerden oluşan bir toplum düzeninin oluşturulması, ancak bireyin **kişisel veri**lerine ilişkin hakkının korunmasıyla mümkündür. Bu hak yukarıda ifade edildiği üzere TC Anayasası'nın 20/2 maddesinde açık bir şekilde düzenlenmiştir.

Unutulma hakkına gelince; unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında **kişisel veri**lerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin **kişisel veri**leri üzerinde serbestçe tasarruf edebilmesini,

geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, **kişisel veri**lerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır.

Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanılan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği **kişisel veri**lerin silinmesini ve yayılmasının önlemesini isteme hakkı olarak ifade edilebilir.

Bu hak bir yandan kişiye "geçmişini kontrol etme", "belirli hususların geçmişinden silinmesini ve hatırlanmamayı isteme hakkı" sağladığı gibi, diğer yandan muhataplarına kişi hakkındaki bir kısım bilgilerin üçüncü kişilerin kullanmamasını veya üçüncü kişilerin hatırlamamasına yönelik önlenmeleri alma yükümlülüğü yükler. Bu hakkın; bireylerin fotoğraf, internet günlüğü gibi kendileri hakkındaki içerikleri silmek için üçüncü şahısları zorlamayı içermesinin yanında geçmişteki cezalarına ilişkin bilgilerin veya haklarında olumsuz yorumlara neden olabilecek bilgi ve fotoğraflarının kaldırılmasını isteme hakkını tanıdığı kabul edilmektedir. Diğer taraftan bu hak, bireyin geçmişindeki belirli yönlerinin mümkün olmayacak biçimde hatırlanmaması için önlemler alınmasını gerektirmektedir.

Avrupa İnsan Hakları Sözleşmesi (AİHS)'nin 8. maddesinde yer alan özel yaşama saygı hakkı altında korunan "mahremiyet hakkı"nın, bireyin kendisi hakkındaki bilgileri kontrol edebilmesi şeklindeki hukuki çıkarlarını da içerdiği ifade edilmektedir. Zira bireyin kendisine ait herhangi bir bilginin, kendi rızası olmaksızın açıklanmaması, yayılmaması ve bu bilgilere başkalarının ulaşamaması kısacası **kişisel veri**lerinin mahrem kalması konusunda hukuki menfaati bulunmaktadır. (Gülay Arslan Öncü, Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması, Beta Yayınları, İstanbul 2011, s.182)

Kişiye unutulma hakkının sağlanması ile birlikte özel hayatının gizliliği korunmuş olacaktır.

Somut olaya bu kapsamda bakıldığında; davacı, kamu görevinin veya hizmet ilişkisinin sağladığı nüfuzu kötüye kullanarak, müteselsilen cinsel saldırı suçunun mağdurudur. 2006 yılında gerçekleşen eylem tarihinde davacı bekâr olup maruz kaldığı eylem geleceği açısından etkilidir. Yapılan yargılama sonunda kamu görevlisi olan sanık ceza almıştır. Temyiz istemi üzerine yapılan inceleme sonunda ise hüküm 2009 yılında onanmıştır. Mağdur davacı gerek hazırlık gerekse de yargılama sırasında cinsel saldırının nasıl gerçekleştiğini açık bir şekilde anlatmış, bu anlatımlar doğal olarak karar metnine geçirilmiştir. Karar mağdur ve sanığın ismi rumuzlanmadan 2010 yılı nisan ayında yayınlanan kitapta yer almıştır.

Hemen ifade edilmelidir ki; davacının rızası dışında bir kitapta geçen ismi **kişisel veri** niteliğindedir.

Ayrıca şunun da ifade edilmesi gereklidir ki; unutulma hakkı tanımlarına bakıldığında her ne kadar dijital veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki **kişisel veri**ler için değil, kamunun kolayca ulaşabileceği yerde tutulan **kişisel veri**lere yönelik olarak da kabul edilmesi gerektiği açıktır.

Davacı, geçmişte yaşadığı kötü bir olayın toplum hafızasından silinmesini istemektedir. Unutulma hakkı ile geçmişindeki yaşanan talihsiz bir olayın unutularak geleceğini serbestçe şekillendirmek, diğer bir deyişle

hayatında, yeni bir sayfa açma olanağı istemektedir. Kaldı ki, davacı da yargılama sırasında verdiği dilekçelerinde bu istem üzerinde ısrarla durmuştur. Davacı unutulma hakkı ile özel hayatına ilişkin **kişisel veri**lerinin üçüncü kişiler tarafından bilinmemesini, aradan geçen süre nedeniyle toplum hafızasından silinmesini istemektedir.

Bu bağlamda değerlendirildiğinde; 4 yıl önce gerçekleşen bir olayın mağduru olan kişinin adının açık bir şekilde yazılarak kitapta yer alması halinde unutulma hakkının bunun sonucunda da davacının özel hayatının gizliliğinin ihlal edildiği kabul edilmelidir. Avrupa Birliği Adalet Divanı'nın "Google Kararı"nda açıkladığı gibi ilgili verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi şeklinde, üstün bir kamu yararını ortaya koyan özel sebepler bulunmadığına göre bilimsel esere alınan kararda**kişisel veri**ler açık bir şekilde yer almamalıdır.

Görüşmeler sırasında azınlıkta kalan üyeler mahkeme kararlarında yer alan isimlerin rumuzlanmasına gerek olmadığını, yargılamanın istisnalar haricinde açık bir şekilde yapıldığını hükmün alenen tefhim edildiğini, bu nedenle özel hayatın gizliliğinin ihlal edilmediğini savunmuşlar ise bu görüş "sorunun mahkeme kararlarında isimlerin rumuzlanmadan yer alması değil, kararların kitaba alınması sırasında rumuzlanması gerekip gerekmediği sorunu olduğu" gerekçesi ile kurul çoğunluğu tarafından kabul edilmemiştir.

O halde davacının isminin rumuzlanmadan kitapta yer almasının unutulma hakkını ve bunun neticesinde özel hayatın gizliliğini ihlal ettiği dikkate alındığında davacı lehine manevi tazminat koşullarının gerçekleştiğinin kabulü zorunludur.

Ne var ki, Özel Dairece tazminat miktarı yönünden inceleme yapılmadığından bu yöne ilişkin temyiz itirazlarının incelenmesi için dosyanın Özel Daireye gönderilmesi gerekir.

SONUÇ : Yukarıda yazılı gerekçelerle yerel mahkemenin direnme kararı yerinde bulunduğundan tazminat miktarı yönünden mahkemenin kurduğu hükme yönelik temyiz itirazlarının incelenmesi için dosyanın 4. Hukuk Dairesine gönderilmesine, 17.06.2015 gününde oyçokluğu ile karar verildi.