The legal framework and guidance on data protection under the European Data Protection Directive No. 95/46/EC

Aslı ALKIŞ[1]

Abstract

The European Parliament and Council adopted the " Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data" on 24 October 1995 to harmonize the national data protection laws of Member States.

This article focuses on four fundamental aspects of data protection:

(1) Conditions for legitimate data processing (including sensitive data)
(2) Rights of data subjects
(3) Obligations of data controllers
(4) Legal framework (Including remedies)

In the final part of the article, I shall try to reveal the shortcomings of these fundamental aspects.

1. Criteria for Making Data Processing Legitimate

The conditions for the processing of personal data in the Member States is listed in Article 7 of the Directive:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

[1] International and European Trade and Investment Law(LL.M) student of University of Szeged

(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 or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed , except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 d).

However, the conditions in the above list are alternatives. For a particular processing operation, the controller has to comply with one only. In the vast majority of cases, controllers will be able to rely on (b)-(f) and will not require consent.[2]

According to Bainbridge, all alternatives are expressed as 'necessary' in order to obtain the consent of the data subjects. It would be more appropriate to interpret the 'necessary' in the sense of 'reasonably necessary' rather than to strictly interpret it. A stronger comment may lead to enormous administrative and financial burdens on most data controllers. The Ministry of Health estimates that this cost will exceed £ 1 billion, as there is an explicit consent to process personal data on all data issues themselves.[3]

Sensitive Data

In many judicial systems, “data revealing racial or ethnic origin”, “political opinions”, “religious or philosophical beliefs”, “trade union membership or where the processing concerns health or sex life” described as “sensitive data” because they require a higher level of protection. Article 8/1 of the Directive prohibits the processing of “sensitive data”.

The exemptions of the prohibition are given by the second paragraph of the same article, being:

(a) the data subject has given his explicit consent to the processing of those

[2] David I. Bainbridge, Processing Personal Data and the Data Protection Directive, 6 Info. & Comm. Tech. L. 17 (1997) p. 25
[3] *Id.*

data , except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation , association or any other non-profit-seeking body with a political, philosophical , religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

Article 8 (3) allows for medical purposes, preventive medicine, medical diagnosis, provision of care or treatment, or treatment of the health care administration.

By Article 8 (4), the Member States may set additional exemptions based on substantial public interest, subject to appropriate measures.

Article 8 (5) only permits the processing of personal data concerning 'crimes, criminal provisions or security measures' by or under the control of the authorities.

Article 8 (6) permits the Member States to require that official data on administrative sanctions or legal judgments be processed under the control of the official authority.

Article 8 (7) requires that the Member States determine the conditions under which national identification numbers or other identifiers of the general application can be processed.

This provision is crucial in preventing individuals from being exposed to discrimination or being subject to suffering.

2. Rights of Data Subjects

Data subjects have the following rights under the Directive:

- Access to your personal data, free of charge, and without constraint, within three months;
- Rectification of inaccurate or incomplete personal data;
- Blocking data processing in certain circumstances;
- Erasure of unlawfully processed data;
- The right to object to a processing operation on compelling grounds;[4]
- He/she should also have the right to object, on request and free of charge, to the processing of personal data that the controller anticipates being processed for the purposes of direct marketing. He/she should finally be informed before personal data are disclosed to third parties for the purposes of direct marketing, and be expressly offered the right to object to such disclosures.
- Every person shall have the right to a judicial remedy for any breach of the rights guaranteed by the national law applicable to the processing in question. In addition, any person who has suffered damage as a result of the unlawful processing of their personal data is entitled to receive compensation for the damage suffered.[5]

Exemptions and restrictions on data subject's rights:

- The scope of the principles relating to the quality of the data,

[4] https://www.eea.europa.eu/legal/privacy/data-protection-at-a-glance/view p.5
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14012

- Information to be given to the data subject,
- The right of access and the publicising of processing may be restricted in order to safeguard aspects such as national security,
- Defence,
- Public security,
- The prosecution of criminal offences,
- An important economic or financial interest of a Member State or of the European Union or the protection of the data subject.[6]

3. Obligations of Data Controllers

According to Brendan Van Alsenoy, Directive 95/46 has a "strict" liability regime for controllers in personal data processing.[7]

Data controllers have the following obligations under the Directive:

The data controller's primary duty is to identify personal data processing operations he or she carries out and to notify them to the Data Protection Officer. Notification should take place before the operation is undertaken. Operations already in place should be notified as soon as possible.

As mentioned previously, the data controller also has a responsibility to furnish certain information to data subjects. The data controller must also facilitate data subjects' access to their data and their exercising other rights such as rectification and erasure.

The data controller must also ensure that appropriate security measures are in place, and issue appropriate instructions to ensure confidentiality if data are processed by others (for example, by a sub-contractor).[8]

An entity can be a data controller, or a data processor, or both.

The duties of the processor towards the controller must be specified in a contract or another legal act. For example, the contract must indicate what happens to the personal data once the contract is terminated. A typical activity of processors is

---

[6] *Id.*
[7] Brendan Van Alsenoy, Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, 7 J. Intell. Prop. Info. Tech. & Elec. Com. L. (2016) p. 272
[8] https://www.eea.europa.eu/legal/privacy/data-protection-at-a-glance/view p.6

offering IT solutions, including cloud storage. The data processor may only sub-contract a part of its task to another processor or appoint a joint processor when it has received prior written authorisation from the data controller.[9]

Transfers of personal data from a Member State to a **third country** with an adequate level of protection are authorised. However, although transfers may not take place when an adequate level of protection is not guaranteed, there are a number of exceptions to this rule listed in the Directive, e.g. the data subject himself agrees to the transfer, in the event of the conclusion of a contract, it is necessary for public interest grounds, but also if Binding Corporate Rules or Standard Contractual Clauses have been authorised by the Member State.[10]

4. Legal Framework

4.1 National Supervisory Authorities in the Member States

A data protection authority is an independent body responsible for:

i) Supervising the processing of personal data within the jurisdiction,

ii) Recommending the legal and administrative measures concerning the processing of personal data to the competent authorities,

iii) Considering complaints about the protection of citizens' data protection rights.

In accordance with Article 28 of Directive 95/46 / EC[11], each Member State shall have at least one data protection authority in its territory with the power to initiate legal proceedings when the data protection laws have been violated, investigative powers, and efficient intervening powers.

The decisions of the supervisory authority which cause complaints can be appealed to the courts.

Each supervisory authority should regularly prepare a report on its activities. The report should be made public.

---

[9] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14012

[11] For more information: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML Article 28.

The supervisory authorities must cooperate with each other in order to fulfill their duties, in particular by interchanging all useful information.

Members of the supervisory authority and their staff, even after the end of their business, must be subject to a duty of professional secrecy concerning confidential information that they have access.

National data protection authorities have been established in almost all European countries and in many countries all around the world.

According to Article 18, *the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.*[12]

However, there is an exemption from the notification providing that a personal **data protection official** must be appointed. In respect to this exemption, the conditions which are needed to be met by the data protection official are laid down under Article 18/2:

"where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations."

4.2 Data protection authority for the European Union institutions, bodies and agencies

The EU institutions and bodies sometimes **process citizens' personal information** - in electronic, written or visual format - in the course of their duties.

[12] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML Article 18.

Processing includes collecting, recording, storing, retrieving, sending, blocking or erasing data. It is the task of the **European Data Protection Supervisor (EDPS)** to uphold the **strict privacy rules** governing these activities.[13]

The tasks of the European Data Protection Supervisor:

- Controls the processing of personal data to ensure compliance with the privacy rules of the European Union administration,
- Advises European Union institutions and organizations on all aspects of personal data processing and related policies and legislation,
- Handles the complaints and investigates,
- Works with the national authorities of Member States to ensure consistency in data protection,
- Follows new technologies that can be effective on data protection.

The Supervisor and The Assistant Supervisor are appointed once in five years, and the former Supervisor could be re-elected. For day-to-day operations, the European Data Protection Supervisor has two main entities:

- Auditing and Implementation - evaluates data protection compliance of European Union institutions and organizations.
- Policy and consultation – European Union policy-makers have recommendations on data protection issues in various policy areas and new legislative proposals.

The European Union institutions and bodies cannot process your personal data for the following information:

- racial or ethnic origin
- political views
- religious or philosophical views
- union membership

[13] https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_en

- health or sexual orientation (unless it is necessary for health care. Even then, this should be done by a health professional or a sworn person for professional secrecy.)

All EU institutions, including the EDPS, are obliged to comply with the data protection law[14] specifically applicable to them.[15]

The law stipulates at least one **Data Protection Officer (DPO)** appointment for each European Union institution.

The tasks of the Data Protection Officer are:

- to ensure that the data protection law is implemented in the institute independently.
- to register for all the operations involving the processing (for example, collection, use and / or storage) of personal data carried out by the institution.

The register must be public and has to contain information explaining the purpose and conditions of the personal data processing.

The role of the Data Protection Officer in the European Data Protection Supervisor is accompanied by many difficulties, some of which are listed below:

- to be independent in an independent institution,
- meet the high expectations of colleagues who are particularly conscious and sensitive to data protection issues,
- offer solutions that can serve as benchmarks for other institutions.

The role of the Data Protection Officer which is mentioned above take place in the EDPS's rules[16]. In addition, they should take into account both the EDPS

[14] https://edps.europa.eu/sites/edp/files/publication/reg_45-2001_en.pdf
[15] https://edps.europa.eu/about/data-protection-within-edps/data-protection-officer-edps_en
[16] https://edps.europa.eu/sites/edp/files/publication/10-10-12_edps_implementing_rules_en_1.pdf

Position paper[17] and the Data Protection Officer Network Paper on Professional Standards for Data Protection Officers[18].

The existing data protection rules applicable to European Union institutions are being revised to be in line with the General Data Protection Directive. The new rules aim to make European Union institutions more accountable in the way of personal data processing.

Remedies

If data subjects' privacy is violated by a European Union institution or organization, they must first tell the European Union staff who are responsible for their data. If they are not satisfied with the outcome, they need to contact the data protection officer of the European Union institution or body that has committed the violation.

If this also fails, a complaint can be made to the European Data Protection Supervisor using the application form[19]. The European Data Protection Supervisor will tell them if they have accepted their complaint and if so, how the situation has been corrected.

If the data subjects do not agree with the European Data Protection Supervisor's decision, it is possible to take the data subject to the European Union Court of Justice.

4.3 Article 29 Working Party

The "Article 29 Working Party"[20] is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States.

[17] https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en_0.pdf
[18] https://edps.europa.eu/sites/edp/files/publication/10-10-14_dpo_standards_en.pdf
[19] https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en
[20] For more information:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML Article 29.

The Working Party is composed of:

- representatives of the national supervisory authorities in the Member States;
- a representative of the European Data Protection Supervisor (EDPS);
- a representative of the European Commission (the latter also provides the secretariat for the Working Party).[21]

5. Result and Assessment

As a result of many years of work, the European Union Data Protection Directive has attempted to establish a comprehensive data protection regulation. It has been desirable to draft a framework law to legitimize the processing of data and to ensure that it is also adopted by each Member States to their domestic laws in a way that provides the safe and free movement of data among the Member States. But with the rapid development of technology, the framework law has been lacking in some aspects and the need for renewal has arisen.

First of all, the Directive is based on explicit consent to ensure that the processing of personal data is legitimate. However, the Directive does not include a separate provision concerning the conditions of the consent. In my opinion, it is necessary to strengthen the data subjects' consent which is known as the reason for compliance with the law. Moreover, more suitable mechanisms are needed to protect sensitive data.

As for the rights that data protection law is defined, some differences in the practices of member countries should be resolved. (For example, in terms of time limits)

In respect of obligations, only Data Control's strict liability is no longer sufficient. All actors (for example, data processor) of any processing activity related to personal data must be responsible for any breach of data or illegality resulting from such processing.

If there is no assurance that sufficient protection has been provided in the third country to which the personal data has been transferred, transfers of personal data from European Union to them is prohibited, even the consent is given to share the personal data to the data controller. However, the only person who is responsible for this judgment is the

[21] https://edps.europa.eu/node/3095#articlewp

data controller. In the increasingly globalized world, it is necessary to consider this matter with more effective mechanisms.

In addition, there are different legal approaches and practices regarding the notifications and legal remedies of data breaches to users or data protection authorities with respect to existing domestic law regulations. The uncertainty in this regard and the divergence between member countries must be resolved.

Finally, it should be noted that the directives set out the main objectives that are expected to be adopted by the Member States to their national laws, but don't establish rules about how to implement the objectives in their domestic laws. In this context, it is difficult to achieve a high level of harmonisation among the European Union countries.

Above all, high-level harmonisation has to be achieved in order to achieve a global competitive advantage through a simplified, seamless and efficient EU digital economy targeted at the European Union Digital Single Market Strategy.