SARA Law **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2810-4188, ISSN-L 2810-4188
No. 1 (2021), pp. 596-601

PROTECTION OF PERSONAL DATA FOR INDIVIDUALS ON THE TERRITORY OF THE UNION OF EUROPE

P. TĂRCHILĂ

Petru TĂRCHILĂ
Faculty of Humanities and Social Sciences
„Aurel Vlaicu" University of Arad
E-mail: petru.tarchila@yahoo.com

Abstract

Since 25 May 2018, with the entry into force of the General data Protection Regulation, all companies and organizations operating in the EU have the same set of data protection rules, wherever they are based. Due to stricter data protection rules:

- *citizens have more control over their personal data;*
- *companies enjoy a level playing field.*

The new General data Protection Regulation of the European Union ("GDPR") is an evolving extension of the data Protection Directive 95/46/EC *issued by the European Commission in 1995. The main purpose of this is to unify and strengthen data protection for EU citizens. It also sets new rules for the export of data outside the EU. It is important we know that the GDPR takes into account only personal data: names, email addresses, telephone numbers, marital status, banking and medical information, location data, IP addresses, photos, as well as personal photos and posts on social networks.*

Its main aims are:

- *reduction of the amount of personal data collected,*
- *deletion of unnecessary data,*
- *restriction of access to personal data,*
- *secure personal data.*

Keywords: *personal data (D.C.P.), privacy protection of individuals in the U.S., existence of a uniform practice, established at European Commission level*

INTRODUCTION. GENERAL ASPECTS

The basis of the GDPR, as it is known today, is Directive 95/46/EC on the protection of individuals with regard to the activity of collecting and processing personal data (PCD) and to ensure their free movement within and between Member States.

The Directive must be implemented separately in each EU country, once it has been adopted by the European Commission and the European Parliament. To this end, each Member State creates its own legislative framework, in line with the purpose of the Directive. However, there may be non-uniform practices across the EU. Regulation (EU) 679/2016 entered into force on 25 May 2016, specifying that it is to be applied as from 25 May 2018. The Regulation lays down a single set of rules, which will apply directly in all EU Member States, to better the protection of the privacy of individuals across the European Union.

The Regulation will be adopted by each EU Member State and will be applied as such without any changes. Thus, there will be a uniform practice, established at European Commission level, on matters of international law.[1]

The main issues to which the GDPR refers are: Data protection, rules and legislation, awareness, information, communication, individual rights, consent integrity.[2]

The GDPR is intended to protect and legislate the privacy of all EU citizens, to determine how organizations protect personal data.

I. LEGAL ASPECTS

1.1 Personal data

European Regulation 679 / 2016 and, by default, Law no. 190 / 2018 refer strictly to personal data. They are not the same as a company's secret data, business secrecy, state secrecy or any other information considered confidential. It refers to the relationship between a person whose data is being processed and the organization which processes the data.

The person whose data are processed shall be referred to as ***the data subject.***

The organization which processes the data shall be called ***the controller of the personal data***. It shall also be the holder of the personal data which it has obtained about the data subject and which it processes using manual, automated or computer methods.

Personal data shall mean any information relating to an identified or identifiable natural person, individually identified and referred to as a data subject. Carrier data appears in any format, on any physical or electronic media, regardless of the nature or content.[3]

The main categories of personal data are:

- "regular" data such as name, first name, date of birth, address, email, hobby, etc.
- Genetic data
- Biometrics, such as photography, etc.
- Health data
- Special data such as origin, raid, sex, criminal record, etc.

[1] LAW No 190 of 18 July 2018.
[2] https://www.axistechnolabs.com/company/gdpr-compliance
[3] https://www.legeagdpr.ro/

Personal data (PCD) shall be clearly expressed, may be anonymized or pseudonymised, may or may not be encrypted.

1.2 Principles of processing PCD

The following principles, detailed and explained in the GDPR Regulation, must be respected during the processing of the PCD:

- Legal pre-work, with due regard for fairness and transparency
- The collection and processing of the PCD will be for specified, explicit and legal purposes only
- Suitability, relevance and limitation to what is necessary
- The accuracy and proper update of the data
- The retention will only be for the time required, after which the PCD will be removed from the storage base
- Processing in an appropriate manner without prejudice to the data subject.

1.3 The rights of the data subject

The rights of the data subject are stated and explained in the GDPR Regulation and subsequently in the Law no. 190/2018. They are well defined to ensure effective protection of the privacy and privacy of the individual. The data subject shall thus be guaranteed:

- The right to correct and complete information, on request or in accordance with the Directive
- The right of access to the processing of the PCD made available to the operator, on the basis of written requests and at reasonable intervals of time
- The right to rectification, modification, correction, as many times as necessary, at reasonable intervals
- The right to deletion of data or the right to be forgotten/removed from the database only where this is not contrary to the legislation in force
- The right to restriction of processing
- The right of data portability
- The right not to be subject to individual automated decisions
- The right to be notified in case of breaches of the security of the PCD
- The right of access to justice.

II. INFORMATIONAL ASPECTS

From an informational point of view, the PCD may exist in several forms. Thus, they can be found as follows:

- On paper (printed documents, folders, etc.)
- Electronic (HDD, CD, Video, Memory Stick, Card...)
- Know-how (human resources)

Security measures shall be classified to ensure compliance with the provisions of the GDPR. Thus, there are:

- Technical security measures
- Physical, such as: access control to the physical perimeter of the PCD, classification and marking of documents, correct positioning of data processing equipment and devices, etc.

- It&C level, such as: encryption, anonymisation, pseudonymisation, information system access control, network traffic analysis, anti-virus and anti-spam installation, definition and use of appropriate passwords, backup
- Non-technical security measures
- At the level of human resources such as: internal organization, training, awareness-raising, etc.

The attributes of the security of information and, by default, of personal data are: confidentiality, integrity, availability and continuous resistance. One or more of these attributes may be affected if risks to the security of the PCD are identified, such as: destruction, loss, modification, unauthorized disclosure, unauthorized access to data, etc.

In order to ensure the security of processing of PCDs, technical and organizational measures should be implemented according to the level of risks identified for PCDs and the specific scope. Consideration must be given to the possibility of accidental or deliberate (illegal) affections of the rights and liberties of natural persons.

Security measures regarding the processing of personal data may also be associated with, but are not limited to, compliance with the provisions of ISO 27001:2018 – Security of information management.

The main categories of measures for the protection of PCDs are the following[4]:

- Organization of the security of the PCD. For example: establishing the context of processing, establishing roles and responsibilities;
- PCD management: Identification of PCD and information flows, identification of owners for PCD and processing processes;
- Mobile devices and remote work;
- Human resources security:before employment, during employment and upon termination of employment (IT access rights must be disabled and must be signed by network administrator);
- PCD rating – labeling, appropriate handling;
- Handling of storage media: security measures for storage, destruction and transfer;
- Access control: limit access and define processing limits, define and comply with the policy on access to PCDs, password and secure login, how to access IT systems, the computer network and the program source code, etc.;
- Cryptographic security measures;
- Physical and environmental security: physical access perimeter, delivery and loading areas, cable security, user-supervised equipment, clean office policy and protected screen policy;
- Security of operations: protection against potentially harmful codes (viruses, malware, spam, etc.), change management, capacity management, back-up policy, management of technical vulnerabilities, technical audit of information systems, etc.;

[4] https://www.juridice.ro/

- Security of communications: PCD transfer agreements, e-mail, confidentiality or non-disclosure agreements;
- System acquisition, development and maintenance: protection of transactions and specifications, protection of data used for program testing, etc.;
- Relationship with suppliers: PCD security policy for the relationship with suppliers, protection of own PCD that is accessible to suppliers, protection of suppliers' PCD, security clauses in contracts with suppliers, security of communication in the supply chain;
- Security incident management: definition of responsibilities and procedures, reporting of PCD security weaknesses and incidents, learning from security incidents, etc.;
- Business continuity: PCD security continuity planning, emergency procedures, plan testing and simulations, redundancy (multiple Internet providers, backup of PCD stored in a secure, independent location, availability of PCD processing facilities, etc.;
- PCD security analysis: compliance with security standards and policies, technical compliance analysis, independent PCD security audits.

III. KEY POINTS IN THE LOGIC OF THE THEME

a. The Regulation adopted by the Council of the European Union on a proposal from the European Commission and entered into force on 25 May 2018. The Regulation shall apply in a uniform way to all companies and organizations operating within the European Union. The main purpose of this is to unify and strengthen data protection for EU citizens.

b. The GDPR takes into account only personal data: names, email addresses, phone numbers, marital status, banking and medical information, location data, IP addresses, photos, as well as personal photos and posts on social networks.

CONCLUSIONS

The National Supervisory Authority for the Processing of Personal Data, as an autonomous central public authority with general competence in the field of the protection of personal data, guarantees respect for the fundamental rights to privacy and the protection of personal data, stated in particular by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, Article 16 of the Treaty on the Functioning of the European Union and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. 2016 marks a key moment in the development of European regulations on the protection of personal data by the adoption by the European Parliament and the Council of the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General data Protection Regulation). The Regulation entered into force in all Member States of the European Union as from 25 May 2018, together with the adoption of the Directive on the protection of data processed for the purposes of prevention,

detection, investigating and prosecuting offenses and other judicial activities. This reform of the legislative framework in this field involves, in the short term, for Romania, a complex evaluation of the specific tools for the protection of personal data, in order to adapt the national regulatory framework and institutional preparation for the application of the new European regulations, including effective cooperation with the European data Protection Board and other relevant authorities in the European Union.

Thus, strengthening the administrative capacity of the National Supervisory Authority for the Processing of Personal Data is a priority and requires the allocation of material, financial and human resources appropriate to the exercise of our new specific tasks in order to effectively apply the European Union standards contained in the new regulations adopted.

BIBLIOGRAPHY

Alexe I., Ploeşteanu N., *Protecţia datelor cu caracter personal*, Editura Universitară, Bucureşti, 2017.

Ploeşteanu N., *Protecţia datelor cu caracter personal, Modele şi formulare*, Editura Universitară, Bucureşti, 2019.

Muşat & Asociaţii, *Ghid practic de implementare GDPR*, https://concordcom.ro/wp-content/uploads/2017/10/1-Bogdan-Mihai-Regulament-679_2016_Ghid-final.pdf (accesat mai 2021).

*** LEGE nr. 190 din 18 iulie 2018.

https://www.legeagdpr.ro/(accesat iulie 2021).

https://decalex.ro/(accesat august 2021).

https://www.axistechnolabs.com/company/gdpr-compliance(accesat august 2021).

http://xstreamreports.com/gdpr/(accesat august 2021).

https://www.dataprotectionromania.ro/(accesat iulie 2021).