ROMÂNIA
AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Bld.Gen. Gheorghe Magheru Nr. 28-30, Sector 1, Cod poştal 010336, Bucureşti ; Tel: +40.31.805.9211; Fax:+40.31.805.9602 www.dataprotection.ro; e-mail: anspdcp@dataprotection.ro

Indicative guidelines for the application of the General Data Protection Regulation intended for the controllers

CONTEXT

The European Parliament and the Council adopted on the 27th of April 2016, the **Regulation (EU) 2016/679 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 – GDPR)**.

Regulation (EU) 2016/679 was published in the Official Journal of the Union L119 from the 4th of May 2016 and **its provisions shall be directly applicable in all the Member States of the European Union starting with the 25th of May 2018.**

Regulation (EU) 2016/679 imposes a single set of rules in the field of protection of personal data, by replacing Directive 95/46/EC and, implicitly, the provisions of Law no. 677/2001.

NOVELTIES

Regulation (EU) 2016/679 emphasizes the transparency towards the data subject and the responsibility of the data controller towards the way it processes personal data.

Regulation (EU) 2016/679 establishes a series of specific safeguards to protect the privacy of children, as effectively as possible, especially in the online environment.

Regulation (EU) 2016/679 strengthens the rights guaranteed to data subjects and introduces new rights: the right to be forgotten, the right to data portability and the right to restriction of processing.

Regulation (EU) 2016/679 introduces severe sanctions, up to 10 – 20 million euros or between 2% and 4% of the turnover at international level, for the controllers in the private sector.

MATERIAL SCOPE

GDPR applies to:

Processing of personal data in the activities carried out at the premises of a controller or processor on the territory of the Union, whether or not the processing takes place on the territory of the Union.

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:

- 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
- the monitoring of their behaviour as far as their behaviour takes place within the Union.

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.

THE MAIN OBLIGATIONS FOR THE CONTROLLERS IN THE APPLCATION OF THE GDPR

DESIGNATION OF A DATA PROTECTION OFFICER

In order to guide how personal data is managed within a controller or processor, in certain situations, a person is required to carry out an internal information, advisory and control mission: **the data protection officer.**

The designation of a data protection officer is mandatory starting with the 25th of May 2018, by taking into consideration the provisions of Articles 37 to 39 of the General Data Protection Regulation, in case where the controller or processor:

- is public authority or body, except for courts acting in their judicial capacity;
- carries out a core activity which leads to the performance o a regular and systematic monitoring of data subjects on a large scale;
- carries out a core activity which consist of processing on a large scale of special categories of data (such as: data revealing the racial or ethnic origin, religious beliefs, trade union membership, genetic data, biometric data, data concerning health) or personal data relating to criminal convictions and offences.

Even if the entity does not have the express obligation to appoint a data protection officer, ANSPDCP recommends its appointment, considering the beneficial effect of the responsible activity in order to ensure compliance with the General Data Protection Regulation by the respective controller or processor.

A **data protection officer** represents a major advantage for the controller in order to understand and comply with the obligations provided by the GDPR, for the dialogue with the data protection authorities and to reduce the risk of litigation.

The tasks of the data protection officer

- **to inform and advise** the controller or the processor, as well as the employees who carry out processing of their obligations in the data protection field;
- **to monitor compliance with GDPR** and with the national legislation in the field of data protection;
- **to provide advice to the controller or processor** as regards the data protection impact assessment and monitor its performance;
- **to cooperate with the data protection authority** and to act as the contact point for it.

DATA PROCESSING MAPPING

All the controllers from the public sector, the processors, as well as the controllers from the private sector with more than 250 employees, have the obligation to map the processing of personal data performed, according to the provisions of Article 30 of the General Data Protection Regulation.

Even the controllers from the private sector with less than 250 employees have the obligation to map the processing in cases where the processing they perform is likely to generate a risk for the rights and freedoms of the data subjects, if the processing is not occasional or the processing includes special categories of data or personal data relating to criminal convictions and offenses.

In this regard: In order to effectively evaluate the impact of the GDPR on the activity of the entity, it is necessary to identify the processing of personal data performed and **to maintain a record** of the processing activities.

In order to have a complete and accurate record of the processing of personal data carried out and to meet the new requirements, **it must be identified**, in advance, with precision:

- the different personal data processing;
- the categories of personal data processed;
- the aimed purposes by the data processing operations;
- the persons who process personal data;
- the data flows, by indicating the origin and the destinations of the data, especially in order to identify the possible transfers of data outside the European Union.

The record maintained by the controller shall contain:

a) the name and the 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 to 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 paragraph (1) of the General Data Protection Regulation, the documentation of suitable safeguards;
f) where possible, the envisaged time limits for the 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 paragraph (1) of the General Data Protection Regulation.

DATA PROCESSING MAPPING

As such, for each personal data processing, it is necessary to consider the following:

WHO?

The name and contact details of the controller (and of its legal representative) and, as the case may be, of the data protection officer shall be recorded; The list of authorised persons shall be drawn up, as appropriate.

WHAT?

The categories of personal data processed shall be identified; The data likely to present risks due to their highly sensitive nature (data concerning health or offences) shall also be identified.

WHY?

It shall specify the purpose or the goals for which the personal data are collected or processed (e.g. business relationship management, human resources management, geolocation, video surveillance etc.).

WHERE?

The location of the records system and, where appropriate, the recipients of the data shall be established. The states to which the data are, eventually, transferred shall be established.

HOW LONG?

For each category of data, the retention period shall be specified.

HOW?

The security measures implemented to minimise the risks of unauthorised access to data and, consequently, the impact on the privacy of the data subjects shall be specified.

PRIORITISING THE ACTIONS TO BE TAKEN

The controller and the processor shall **identify the actions** to be taken to comply with the requirements imposed by the GDPR.

These actions are **prioritised** according to the risks for the rights and freedoms of the data subjects presented by the processing carried out.

After identifying the processing of personal data performed within the entity, for each of them, the actions to be taken in order to comply with the obligations imposed by the General Data Protection Regulation are established.

Regardless of the processing carried out, the following aspects shall be considered in particular:

- the collection and processing **only of the data strictly necessary** to achieve the purposes;
- the identification of the **legal ground** based on which the processing is performed with reference to Article 6 of the General Data Protection Regulation (e.g. the consent of the data subjects, contract, legal obligation);
- reviewing/completing the **information provided to the data subjects**, in order to comply with the requirements imposed by the General Data Protection Regulation (Articles 12, 13 and 14);
- ensuring that the **processors** know their new obligations and responsibilities;
- verifying the existence of the contractual clauses and updating the obligations of the **processors** regarding the security, the confidentiality and the protection of the personal data processed;
- establishing the modalities of exercising **the rights of the data subjects** (e.g. the right of access, the right to rectification, the right to data portability, the withdrawal of consent);
- verifying the **security measures** implemented.

Special measures may be applied, such as: the data protection impact assessment, the extension of the right to information of the data subjects, obtaining the consent of the data subjects (if applicable), obtaining the authorisation for the data transfers in third countries (if applicable), if the processing of personal data carried out within the controller or processor fulfils the following **characteristics**:

The processing also covers data categories such as:

- data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership;
- data concerning health or data concerning sexual orientation, genetic or biometric data;
- data relating to criminal convictions or offences;
- data relating to children.

The processing carried out has as purpose and effect:

- systematic monitoring of a publicly accessible area on a large scale;
- systematic and extensive evaluation of personal aspects, including profiling, on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.

The processing involves data transfers outside the European Union, to states that do not provide an adequate level of protection recognised by the European Commission.

An in-depth analysis of the data protection legislation and of the requirements imposed by the General Data Protection Regulation is carried out in order to establish the measures to be applied at the level of each controller, depending on the sector of activity and the specific processing performed.

RISK MANAGEMENT

Where data processing that may present **high risks** for the rights and freedoms of the natural persons have been identified, the controller shall carry out a **data protection impact assessment**, in accordance with Article 35 of the General Data Protection Regulation.

The data protection impact assessment is performed **prior to the collection** and processing of personal data.

The **estimations of the risks on the data protection from the point of view of the data subjects, by taking into account the nature of the data, the material scope, the context and the purposes of the processing and the use of new technologies** shall be highlighted.

The data protection impact assessment **assumes**:

- a description of the data processing performed and its purposes;
- an assessment of the necessity and proportionality of the data processing performed;
- an estimation of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks and to ensure compliance with the provisions of the GDPR.

The data protection impact assessment allows:

- carrying out a personal data processing or a product that respects the privacy;
- estimating the impact on the privacy of the data subjects;
- demonstrating that the fundamental principles of the General Data Protection Regulation are respected.

The data protection impact assessment 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 persons;
b) processing on a large scale of special categories of data referred to in Article 9 paragraph (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.

When the impact assessment indicates high risks, in the absence of any measures taken by the controller to mitigate them, the National Supervisory Authority shall be consulted.

ORGANISATION OF THE INTERNAL PROCEDURES

In order to permanently ensure a high level of protection of personal data, the controller shall develop internal procedures in order to guarantee the compliance with data protection at all times, taking into account all the events that may occur during data processing, such as:

- personal data breaches;
- requests regarding the exercise of the rights of the data subjects;
- amendments of the personal data collected;
- change of the provider.

The organisation of internal procedures involves, in particular:

- **taking into account the protection of personal data from the moment of design (privacy by design)** of an application or processing: minimising the collection of data according to purpose, the cookies, the storage period, the information provided to data subjects, obtaining the consent of the data subjects, the security and confidentiality of

personal data, guaranteeing the role and responsibility of the parties involved in performing the data processing;

- **the application of adequate technical and organisational measures to ensure that, by default, only personal data that are necessary for each specific purpose of processing (privacy by default)** are taken into account, by having regard to: the volume of data collected, the degree of their processing, the storage period and their accessibility, so that personal data shall not be accessed, without the human intervention, by an unlimited number of people;
- **raising awareness and organising the dissemination of information**, in particular by establishing a training and communication plan with the persons who process personal data;
- **solving the complaints and requests addressed by the data subjects in the exercise of their rights**, by establishing the parties involved and the modalities of exercising them; the exercise of the rights should be possible also electronically, if the data were collected by such means;
- **anticipating a possible personal data breach**, specifying, in certain cases, the obligation to notify the data protection authority within 72 hours and the data subjects as soon as possible;
- **ensuring the confidentiality and security of the processing** by adopting the appropriate technical and organisational measures, 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.