Guidelines for the application of the General Data Protection Regulation by the data controllers

CONTEXT

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

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

Regulation (EU) 2016/679 imposes a unique set of rules on data protection, 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 accountability of the data controller with reference to the way it processes the data.

Regulation (EU) 2016/679 establishes a series of specific safeguards in order to protect as effectively as possible the privacy of minors, particularly in the on-line environment.

Regulation (EU) 2016/679 strengthens the rights guaranteed to the 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 millions of euro or between 2 % and 4% of the total worldwide annual turnover for the data controllers in the private sector

TERRITORIAL SCOPE

GDPR applies to:

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.

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.

MAIN OBLIGATIONS OF THE DATA CONTROLLERS FOR THE APPLICATION OF GDPR

DESIGNATION OF THE DATA PROTECTION OFFICER

For the guidance on how personal data is handled by data controller or a processor, in some situations, a person is required to carry out an internal information, counseling and control mission: **the data protection officer**.

The designation of a data protection officer is mandatory as of 25th of May 2018, based on the provisions of Articles 37-39 of the General Data Protection Regulation, where the data controller or processor:

- public authority or body, except for courts;
- carries out a core activity which require regular or 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: personal data revealing racial or ethnic origin, religious beliefs, trade union membership, genetic data, biometric data, data concerning health) or data relating to criminal convictions or offences.

Even if the entity is not expressly required to designate a data protection officer, ANSPDCP recommends this appointment, taking into account the beneficial effect of the officer's activity to ensure compliance with the General Data Protection Regulation by that data controller or processor.

A **data protection officer** is a major asset for the data controller in order to understand and comply with GDPR's obligations, for the dialogue with data protection authorities and to reduce the risk of litigation.

Tasks of the data protection officer

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

MAPPING PERSONAL DATA PROCESSING

Each data controller from the public sector, each data processor and each data controller from the private sector with more than 250 employees has the obligation to maintain a record of processing activities under its responsibility, based on provisions of Article 30 of General Data Protection Regulation.

Even data controllers from the private system with less than 250 employees are required to map the processing in cases where the processing they perform is likely to result in a risk to the rights and freedoms of data subjects, where the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

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

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

- the different personal data processing;
- the categories of personal data processed;
- the purposes of the processing;
- the persons who process these data;
- the data flows, by indicating the origin and the destination of the data, in particular, in order to identify the eventual data transfers outside the EU.

The record kept by the data controller shall contain:

(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 organizations;

(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) of the General Data Protection Regulation, the documentation of suitable 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) of the General Data Protection Regulation.

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

WHO?

The names and the coordinates of the data controller (and its legal representative) and, where applicable, of the data protection officer shall be recorded;

The list of processors shall be drawn up as appropriate.

WHAT?

Identify the categories of processed data;

Identify the data that may raise risks due to their particular sensitivity (health data or offences)

WHY?

Indicate the purpose(s) for which you are collecting or processing such data (example: business relationship management, HR management, geolocation, video surveillance etc.).

WHERE?

Determine the location of the evidence system and, as the case may be, the data recipients.

Indicate the states where the data may be transferred to.

HOW LONG?

Indicate, for each category of data, the retention period.

HOW?

Indicate the security measures implemented in order to minimize the risks of unauthorized access to data and therefore the impact on the privacy of the data subjects.

PRIORITIZING ACTIONS

The data controllers and the processor **identity the actions** to be taken to comply with the requirements imposed by the GDPR.

These actions are **prioritized** according to the risks posed by the processing performed for the rights and freedoms of the data subjects.

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

Regardless of the processing carried out, the main aspects shall be considered:

- collecting and processing **only the data strictly necessary** for achieving the purposes;
- identification of the **legal basis** on which the processing referred to in Article 6 of the General Data Protection Regulation (e.g. consent of data subjects, contract, legal obligation);
- revision/completion of **information provided to data subjects** in order to meet the requirements of the General Data Protection Regulation (Articles 12, 13 and 14);
- ensuring that **processors** are aware of their new duties and responsibilities;
- verifying the existence of contractual clauses and updating the obligations of **processors** on the security, confidentiality and protection of the personal data processed;
- establishing the means for exercising **the rights of the data subjects** (e.g. right of access, right to rectification, right to portability, consent's withdraw);
- verifying the implemented **security measures**.

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

- The processing also covers data categories such as:
  - data revealing racial or ethnic origin, political opinions, philosophical or religious beliefs, trade union membership;
  - data concerning health or sexual orientation, genetic data or biometric data;
  - data relating to offences or criminal convictions;
  - data relating to minors.
- The processing has as purpose or effect:
  - a systematic monitoring of a publicly accessible area on a large scale;

- 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.

- The processing involves data transfers outside the European Union to countries that do not provide an adequate level of protection recognised by the European Commission or to third countries.

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

RISK MANAGEMENT

If personal data processing that could result in **high risks** to the rights and freedoms of individuals has been identified, the data controller shall perform a **data protection impact assessment**, under the conditions of Article 35 of the General Data Protection Regulation.

The data protection impact assessment shall be carried out **prior to the collection** of personal data and to the processing.

The risks assessment on data protection from the point of view of the data subject, by taking into account the nature of the data, scope, context and purposes of the processing and use of new technologies shall be emphasised.

The data protection impact assessment **supposes**:

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

The data protection impact assessment allows:

- performing a personal data processing or a product that respects 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 is particularly important in:

(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.

Where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller shall consult the supervisory authority.

ORGANISING THE INTERNAL PROCEDURES

In order to ensure a high level of protection of personal data on a permanent basis, the data controller and the processor must develop internal procedures to ensure that data protection is respected at all times, taking into account all the events that may occur during data processing, such as:

- data breach;
- requests for exercising the rights of the data subjects;
- modifying the personal data collected;
- changing the provider.

The organisation of internal procedures involves, in particular:

- **taking into consideration the protection of personal data from the moment of design** (***privacy by design***) of an application or a processing: minimization of collected data depending on the purpose, cookies, retention period, information provided to data subjects, obtaining the consent of the data subjects, security and confidentiality of personal data, ensuring the role and the responsibilities of the involved parties;

- **implementation of appropriate technical and organisational measures ensuring that, by default, only the personal data necessary for each specific purpose of the processing is processed** (***privacy by default***), taking into account the volume of the data, the degree of their processing, the retention period and their accessibility, so that personal data is not accessed, without human intervention, by an unlimited number of persons;

- **raising awareness and organizing the information dissemination,** in by developing a training and communication plan for the employees who process personal data;

- **solving complaints and requests submitted by data subjects for exercising their rights**, establishing the parties involved and the means for their exercise; the exercise of the rights should be performed also by electronic means where the data have been collected in such a way;

- **anticipating a possible personal data breach** specifying, for 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 processing** by implementing appropriate technical and organizational 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.