ARTICLES [Data Ethics and Data Protection]

Guido Spina

July 2023

RIGHT TO PRIVACY

Art. 12 - *Universal Declaration of Human Rights*

No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attack upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Art. 8 - *European Convention on Human Rights*

8.1

Everyone has the right to respect for his private and family life, his home and his correspondence.

8.2

There shall be no interference by a public authority with the exercise for this right except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economical well-being of the country, for the prevention of disorders or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

RIGHT TO PROTECTION OF PERSONAL DATA

Art. 8 - *Charter of Fundamental Rights of the European Union*

8.1

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

8.2

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 the law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

8.3

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

Art. 17 (Right to Erasure) - *General Data Protection Regulation*

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him of her without undue delay and the controller shall have the obligation to erase personal data without undue delay, unless there is a compelling reason not do do so.

GDPR - General Data Protection Regulation

Art. 1

1.1

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.

1.2

This regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

1.3

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.

Art. 3

3.1

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.

3.2

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:

- The offering of goods or services, irrespective of whether a payment of the data subject us required, to such data subjects in the Union.
- the monitoring of their behavior as far as their behavior takes place within the Union.

Art. 7 (Condition for consent)

- The controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data
- Written declaration: 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.
- 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
- 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
- Right to withdraw the given consent at any time, but the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal

Art. 8 (Child's consent)

Consent is valid from 16 years old, but Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. Reasonable efforts to verify it must be taken by data controllers.

Art. 6 (Legitimate interest)

Legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Legitimate interest is not applicable to processing carried out by public authorities in the performance of their task. Balancing test must assess:

- The legitimate interest of the controller (lawful, sufficiently clearly articulated, real and present)

- Impact on the data subject (nature of the data, methods of data processing, reasonable expectations of the data subject, the status of the data subject/controller).
- Additional safeguards to prevent any undue impact on the data subjects.

Art. 37 (Data Protection Officer)

Designation of the data protection officer (internal or external) is mandatory for:

- Public authorities or bodies (a single data protection officer may be designated for several authorities/bodies)
- Data Controllers/Data processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale
- Data Controllers/Data processors whose core activities consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

They must have the following professional qualities:

- Expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
- Understanding of the processing operations carried out
- Understanding of information technologies and data security
- Knowledge of the business sector and the organization
- Ability to promote a data protection culture within the organization

They must be independent:

- Whoever appointed them must provide resources necessary to carry out the DPO's task and access to personal data and processing operations, and to maintain his or her expert knowledge.
- No instructions by the controllers or the processors regarding the exercise of the DPO's task must be handed out.
- There must not be any dismissal or penalty by the controller for the performance of the DPO's task.
- There must not be any conflict of interest with possible other tasks and duties
- DPOs are not personally responsible for non-compliance with data protection requirements

Art.32 (Security Measures)

Taking into accoun the state of the art, the cost 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 organizational measures to ensure a level of security appropriate to the risk, such as:

- Pseudonymization
- Encryption of personal data
- Measures to ensure confidentiality and integrity
- Measures to ensure availability, business continuity and resilience
- Testing tools

The controller/processor must ensure that any natural person acting under their authority does not process personal data except on instructions from the controller, unless required by law.

Art. 33 (Data Breach Register)

33.1

In the case of a personal data breach, the controller shall without unique delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisor authority, 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.

33.2

The processor shall notify the controller without unique delay after becoming aware of a personal data breach.

33.3

The notification shall at least:

- 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.
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained.

- describe the likely consequences of the personal data breach.
- 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.

33.4

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.

33.5

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.

Art. 25 (Data protection by design and by default)

25.1

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 risk 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 organizational measures, such as pseudonymization, 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.

25.2

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.

25.3

An approved certification mechanism pursuant to article 42 (*"Compliance Certification", ndr*) may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this article.

Art. 35 (Data Protection Impact Assessment

35.1

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 a similar risk.

35.2

The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

35.3

A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of :

- A systematic and extensive evaluation of a personal aspect 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.
- Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences.
- A systematic monitoring of a publicly accessible area on a large scale.

35.9

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.