JUDICIAL TRAINING ON DATA PROTECTION AND PRIVACY RIGHTS
On-line Classroom, 23 April 2021
GDPR provisions on BREACHES OF PERSONAL DATA

Jonika Marflak Trontelj, LLM
Higher Court Judge
Administrative Court of the Republic of Slovenia

[AD/2021/03]

ejtn refj

With financial support from the Justice Programme of the European Union

Data protection as a fundamental right

- The protection of natural persons in relation to the processing of personal data is a fundamental right.

- Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of personal data concerning him or her.

Data protection as a fundamental right

Charter of Fundamental Rights of the EU

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

Data protection as a fundamental right

- The right to the protection of personal data is not an absolute right;

- it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

Definitions: GDPR Article 4

(1) Personal Data: means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural.

Definitions: GDPR Article 4

(7) Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; (…).

(8) Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Definitions: GDPR Article 4

(11) Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

(12) Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personal data breach

- Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly and with that the possibility of violating personal data of individuals.
- Natural persons should have control of their own personal data.

Prevention from Personal Data Breach

GDPR Article 32 (Security of processing)

1. (…), the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, 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;

Prevention from Personal Data Breach

GDPR Article 32 (Security of processing)

(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 regulary testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

GDPR Article 33
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
(…)

Consequences of the Personal Data Breach

GDPR Article 33 (Notification of a personal data breach to the supervisory authority)

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

Consequences of the Personal Data Breach

- The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication (GDPR Preamble 86).

Consequences of the Personal Data Breach

It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation (GDPR Preamble 87).

GDPR Article 34
Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Complaints of the Data Subjects

GDPR Article 57

(Tasks of the Supervisory Authority)

(f) Handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, (…)

Complaints of the Data Subjects

The right to complaint is regulated by the GDPR in Article 77:

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

Powers of the Supervisory Authority

GDPR Article 58

1. Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) To carry out investigations in the form of data protection audits;

Powers of the Supervisory Authority

GDPR Article 58

(c) to carry out a review on certifications;

(d) **to notify the controller or the processor of an alleged infringement of this Regulation**;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

Powers of the Supervisory Authority

GDPR Article 58

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation.

Powers of the Supervisory Authority

GDPR Article 58

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) **To order the controller to communicate the personal data breach to the data subject.**

;

Powers of the Supervisory Authority

GDPR Article 58

(f) **to impose a temporary or definitive limitation, including a ban on processing**;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

Powers of the Supervisory Authority

GDPR Article 58

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

Powers of the Supervisory Authority

GDPR Article 58

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

Judicial Remedy

GDPR Article 78

(Right to an effective judicial remedy against a supervisory authority)

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

Judicial Remedy

GDPR Article 79

(Right to an effective judicial remedy against a controller or processor)

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

Representation of data subjects

GDPR Article 80

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

Suspension of proceedings

GDPR Article 81

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

Right to compensation and liability

GDPR Article 82

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

Administrative fines

GDPR Article 83

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. (…).When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

Administrative fines

GDPR Article 83

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

Administrative fines

GDPR Article 83

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

Administrative fines

GDPR Article 83

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

Penalties

GDPR Article 84

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.