



JUDICIAL TRAINING ON DATA PROTECTION AND PRIVACY RIGHTS

On-line Classroom, 23 April 2021
BREACHES OF PERSONAL DATA

Jonika Marflak Trontelj, LL.M.
Higher Court Judge
Administrative Court of the Republic of Slovenia

[AD/2021/03]

Data protection as a fundamental right

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

PERSONAL DATA

Any information relating to an identified or identifiable natural person.

PERSONAL DATA BREACH

An event, leading to the accidental/unlawful :

- destruction,
- loss,
- alteration,
- unauthorised disclosure of,
- access to

personal data transmitted, stored or otherwise processed.

EXAMPLES OF PERSONAL DATA BREACHES

- Lost data transfer devices (USB memory sticks),
- hacking,
- cyber attacks,
- stolen computers,
- malware infection...

CONSEQUENCES OF PERSONAL DATA BREACH

- Loss of control over personal data,
- damage of reputation,
- loss of confidentiality of personal data,
- the reversal of pseudonymisation,
- fraud,
- identity theft...

CONTROLLER

Determines the purposes and means of the processing of personal data.

PROCESSOR

Processes personal data on behalf of the controller.

PREVENTION FROM PERSONAL DATA BREACH

Security measures corresponding to the risk, related to the processing of personal data.

THE LEVEL OF RISK

- No risk,
- risk,
- high risk.

MEASURES REQUIRED

- Documentation of the personal data breach,
- notification to the supervisory authority (risk to the rights and freedoms of the data subject),
- notification to the data subject (high risk).

THE RISK ASSESSMENT

- Type of data breach,
- nature of personal data,
- sensitivity of personal data,
- amount of personal data,
- ease of identification,
- attributes of data subject,
- attributes of the controller,
- severity of the consequences of the data breach

1. EXAMPLE

A controller stored a backup of personal data, which were encrypted on a USB key. The USB key is stolen.

2. EXAMPLE

Hackers had stolen nearly 3 million encrypted customer credit card records, plus login data for an undetermined number of user accounts.

3. EXAMPLE

The controller accidentally sent a bulk mail to invite a small number of people to a community event , using the „to“ and not the „bcc“ field, thereby enabling each recipient to see the mail address of other recipients.

4. EXAMPLE

The controller sent a similar mail (as in previous example) to a group of people who are receiving mental health counselling from the controller and the context identified health information about those people, using the „to“ and not the „bcc“ field, thereby enabling each recipient to see the mail address of other recipients.

5. EXAMPLE

A brief power outage lasting several minutes at a mobile phone company's call centre, meaning customers are unable to call the company (controller) and access their records.

6. EXAMPLE

A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated.

7. EXAMPLE

Medical records in a hospital are unavailable for the period of 24 hours due to a cyber-attack.

8. EXAMPLE

An individual informs a bank, that he/she received a monthly statement of someone else.

9. EXAMPLE

A website hosting company, which is acting as a data processor, identifies an error in the code which controls user authorisation. This error means that any user can access the account details of any other user.

10. EXAMPLE

A controller operates an online marketplace and has customers in multiple EU countries. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.



You can find more examples in the
Guidelines on Personal data breach notification
under Regulation 2016/679

CONSEQUENCES OF NON-COMPLIANCE

- Sanctions imposed by supervisory authority,
- Right to a judicial remedy against a controller or processor/ right to compensation and liability,
- Right to a judicial remedy against decision of a supervisory authority.

SUPERVISORY AUTHORITIES in EU

- Austria: Österreichische Datenschutzbehörde,
- Belgium: Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA),
- Bulgaria: Commission for Personal Data Protection,
- Croatia: Croatian Personal Data Protection Agency,
- Cyprus: Commissioner for Personal Data Protection,
- Czech Republic: Office for Personal Data Protection,
- Denmark: Datatilsynet,

SUPERVISORY AUTHORITIES in EU

- Estonia: Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon),
- Finland: Office of the Data Protection Ombudsman,
- France: Commission Nationale de l'Informatique et des Libertés - CNIL,
- Germany: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
- Greece: Hellenic Data Protection Authority,
- Hungary: Hungarian National Authority for Data Protection and Freedom of Information,
- Ireland: Data Protection Commission,

SUPERVISORY AUTHORITIES in EU

- **Italy**: Garante per la protezione dei dati personali,
- **Latvia**: Data State Inspectorate,
- **Lithuania**: State Data Protection Inspectorate,
- **Luxembourg**: Commission Nationale pour la Protection des Données,
- **Malta**: Office of the Information and Data Protection Commissioner,
- **Netherlands**: Autoriteit Persoonsgegevens,

SUPERVISORY AUTHORITIES in EU

- **Poland**: Urząd Ochrony Danych Osobowych (Personal Data Protection Office),
- **Portugal**: Comissão Nacional de Protecção de Dados – CNPD,
- **Romania**: The National Supervisory Authority for Personal Data Processing,
- **Slovakia**: Office for Personal Data Protection of the Slovak Republic,
- **Slovenia**: Information Commissioner of the Republic of Slovenia,
- **Spain**: Agencia Española de Protección de Datos (AEPD),
- **Sweden**: Datainspektionen.
- **EU**: **European Data Protection Supervisor (EDPS - data protection authority for EU institutions, bodies and agencies)**

European Data Protection Board (EDPB – EU body in charge of application of the GDPR; assembled of the head of each DPA and EDPS)

PROTECTION OF PERSONAL DATA DURING COVID-19 PANDEMIC

European Data Protection Board: Statement on the processing of personal data in the context of the covid-19 outbreak (19 March 2020)

Council of Europe: Joint statement on the right to data protection in the context of the COVID-19 pandemic (30 March 2020)

European Data Protection Supervisor:

EU Digital Solidarity: a call for a pan-European approach against the pandemic (06 April 2020)

European Commission: Recommendation 2020/518 (08 April 2020)

GDPR IN NUMBERS

GDPR IN NUMBERS

#HAPPYBIRTHDAYGDPR

The **General Data Protection Regulation (GDPR)** applies since 25 May 2018. Reports of massive data breaches and the mishandling of personal data by large online platforms remind us what is at stake: from preserving our private life, to protecting the functioning

of our democracies and ensuring the sustainability of our increasingly data-driven economy.

On the occasion of GDPR's first anniversary, we are taking a closer look at awareness, compliance and enforcement of the new rules.

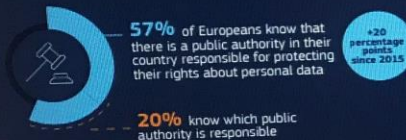
AWARENESS OF THE RULES

Awareness of GDPR



Source: Special Eurobarometer 487a (March 2019)

Awareness of data protection authorities



Source: Special Eurobarometer 487a (March 2019)

Number of queries and complaints to data protection authorities

Individuals are increasingly contacting data protection authorities to ask questions about the GDPR and lodge complaints about respect for their rights. The GDPR also makes it possible for an organisation to lodge complaints on behalf of individuals. This possibility was used immediately after the entry into application of the GDPR.

144,376

Total number of complaints from all data protection authorities in Europe, since May 2018

Source: The European Data Protection Board

This figure is indicative only. The definition is not harmonised between national data protection authorities. We were not able to verify if all the reported figures relate to cases post 25 May, when the GDPR entered into application. Some of them can also relate to the former data protection legislation.

COMPLYING WITH THE RULES

Most common types of complaints

These are the types of activities for which the most complaints have been made so far.



Telemarketing



Promotional e-mails



Video surveillance/ CCTV

Source: The European Data Protection Board

Number of data breach notifications

When personal data for which a company is responsible is accidentally or unlawfully disclosed, that company is obliged to report this data breach to their national data protection authority within 72 hours of finding out about the breach.

89,271

Total number of complaints from all data protection authorities in Europe, since May 2018

Source: The European Data Protection Board

ENFORCING THE RULES

Cross-border cases*

Many companies, such as social media platforms, provide their services in more than one EU country. The GDPR provides that, in most cases, one national data protection authority takes the lead in investigating the case ("one-stop shop"), whilst the other concerned authorities support the investigation. If there is a disagreement between authorities, the European Data Protection Board will arbitrate.



● investigations initiated by data protection authorities
● investigations by data protection authorities on the basis of complaints from individuals

Source: The European Data Protection Board

Fines issued under the GDPR by data protection authorities

The GDPR gives the data protection authorities the power to impose fines of up to 4 % of a company's annual turnover.



Adaptation of national laws in the EU Member States

Being an EU Regulation, the GDPR is directly applicable in all EU countries. However, it also requires countries to adapt their national legislation. 25 EU Member States have adopted the required national legislation, but three are still in the process of doing so (Greece, Slovenia and Portugal).



European Commission
europa.eu/dataprotection

5 biggest GDPR fines

<https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/>

5 biggest GDPR fines so far

TOP 5 BIGGEST GDPR FINES 

1	Google Inc.		€50 000 000
2	H&M Hennes & Mauritz		€35 258 708
3	TIM - Telecom Provider		€27 800 000
4	British Airways		€22 046 000
5	Marriott International		€20 450 000

DATA PROTECTION IN SLOVENIA

- Still didn't implement the GDPR.
- The new Data Protection Act is still in the process of adoption.
- Data protection cases present less than 1 % of all cases at the Administrative Courts.

Thank you!



With financial support from the Justice
Programme of the European Union