JUDICIAL TRAINING ON DATA PROTECTION AND PRIVACY RIGHTS

On-line Classroom, 23 April 2021

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.

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 transmissed, stored or otherwise processed.

EXAMPLES OF PERSONAL DATA BREACHES

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

CONCEQUENCES 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 uneavailable for the period of 24 hours due to a cyber-attack.

8. EXAMPLE

An individual informes 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: Urzad 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)

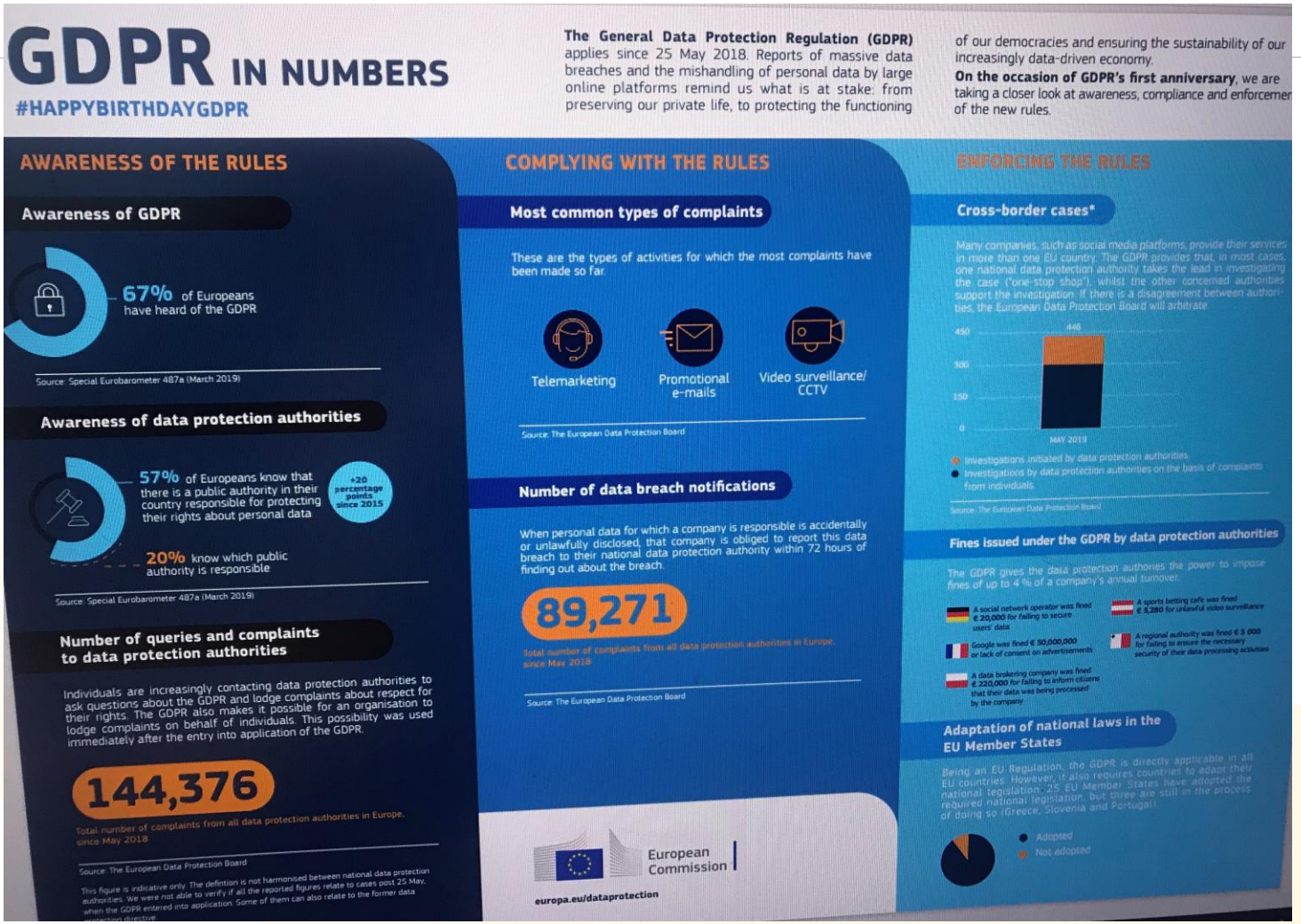
Council of Europe: Joint statement on the right to data protection in the context of the COVID-19 pandemic (30 March 2020)

European Data Protection Supervisor:

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

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

GDPR IN NUMBERS



5 biggest GDPR fines

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

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 then 1 % of all cases at the Administrative Courts.

Thank you!

With financial support from the Justice Programme of the European Union