LAW AND INTERNET
FOUNDATION

RESEARCH CENTER FOR LAW AND
INFORMATION TECHNOLOGIES

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Introduction & Basic Concepts of GDPR

Martin Zahariev, PhD

Law and Internet Foundation, Legal expert

Dimitrov, Petrov & Co. Law Firm, Associate

Sofia, 22 February 2018

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Why data protection?

- *Data is the new currency* [Dr. Vivian Balakrishnan, Minister for Foreign Affairs of Singapore]
- There is **NO** business that can function without processing of personal data
- There is **NO** online service we could use without providing our personal data for processing
- The data is probably the **MOST** important economic resource of 21st century

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Why data protection?

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Evolution of data protection in EU

- Directive 95/46/EC
- Charter of Fundamental Rights (Art. 8) – 2000
- Treaty on the Functioning of EU – 2007 (Lisbon reform): Art. 16 proclaims that everyone has the right to the protection of personal data concerning them
- May 2016 – reform package:
  - **Regulation (EU) 2016/679 (GDPR)**
  - Directive (EU) 2016/680 re processing of personal data in the law enforcement sector
  - Directive (EU) 2016/681 re processing of passenger name records in the context of fight against terrorism and severe crimes

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Basic concepts of data protection

- **Personal data** – ***any*** *information relating to an identified or identifiable natural person ('data subject'). 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 person*

- What is data? – a set of objective signs of a phenomenon, process, or variable

E.g. 180, 4222443, 8804162256, blue, dark, tall, Ivanov, Bulgarian, Romanian, Ivan, Iva, 41 24 12.2 N 2 10 26.5 E

- What is information? - data in context

E.g.: Ivan Ivanov is a Bulgarian citizen, with PIN 8804162256, 180 cm tall, with blue eyes and dark hair. He is married to a woman with the name Iva, Romanian citizen. Their home phone is 4222443 and is located at 41°24'12.2"N 2°10'26.5"E

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Basic concepts of data protection

- **Processing of personal data –** **any** activity that could possibly be made with personal data (including storage, transfer, erasure or modification)
- **Data controller –** any person (natural/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
- **Data processor –** any person (natural/legal person, public authority, agency or other body) which processes personal data **on behalf** of the controller
- **Data subject –** the **natural** person to whom the personal data refers
- **Supervisory authority** – in Bulgaria it is the Commission for Personal Data Protection (https://www.cpdp.bg/)

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

GDPR

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

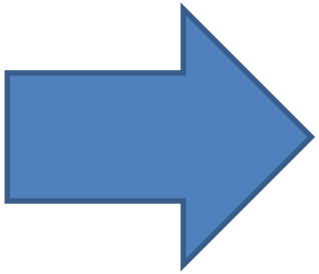
GDPR – general remarks

- **Direct effect**, no need of adoption of any additional national legislation, still national legislations need to be made compliant with its provisions
- In force – 20 days as of its promulgation (04.05.2016) in Official Journal of EU; **applies as of 25.05.2018**
- **Applies to controllers/processors situated outside EU (if the offer goods/services or monitor EU citizen's behaviour)**
- **Administrative fines up to 20 000 000 EUR / 4 % of the total worldwide annual turnover of the preceding financial year (for undertakings), whichever is higher.**
- **One-stop-shop mechanism**

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

GDPR – general remarks

- **From 28 to 1 unified regime**



Principles of data protection

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Principles of data protection

- **Lawfulness, fairness and transparency**
- **Purpose limitation**
- **Data minimization**
- **Accuracy**
- **Storage limitation**
- **Integrity and confidentiality (measures for protection)**
- **ACCOUNTABILITY**

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Lawfulness of processing

Lawful is that processing of personal data for which there is a **legal ground**.

=> What is a legal ground for processing of personal data?

A **condition** provided for by law, which if fulfilled, is sufficient for processing of personal data.

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Lawfulness of processing

Art. 6 of GDPR:

- **Consent**
- **Contract**
- **Legal obligation**
- **Vital interests**
- **Task carried out in the public interest / exercise of official authority**
- **Legitimate interest**

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Sensitive data & grounds for processing

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Sensitive data & grounds for processing

- Special categories of data ("sensitive" data) are data which intrusively interfere in data subject's private sphere
- The principle is *"it is **prohibited**, unless…."*
- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation; personal data relating to criminal convictions and offences
- GDPR does not introduce many significant amendments re grounds for processing, but rather details/elaborates on the existing grounds

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Enhanced rights of data subjects

- Right to information (extended) – Transparency principle
- Right of access (extended)
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restriction of processing
- Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Right to data portability
- Right to objection
- Right not to be subject to automated individual decision making, including profiling

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Obligations for data controllers & data processors

- **Privacy by default & privacy by design**
- **Record keeping**
- **Impact assessment**
- **Data protection officer**
- **Cooperation with the supervisory authority**
- **Security of personal data (additional requirements)**

Record keeping

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Record keeping

- **Subject to the obligation:** controllers **AND** processors
- **Nature:** duly documenting the personal data processing activities in written (including electronic) form
- **Purpose:** reducing the administrative burden for the business
- **Consequences:** as of 25.05.2018 data controller's obligation for registration within CPDP no longer applies
- Threshold of **250 employees**, but in practice such records should be kept in almost every enterprise

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Security & data breaches

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Security& data breaches

- **Appropriate technical and organizational measures**

- The level of security should be adequate to the level of risk

- **Data breach notification**
  - ✓ To the supervisory authority (without undue delay, not later than 72 hours after becoming aware of the breach);
  - ✓ From the processor to the controller (without undue delay after becoming aware of the breach).
  - ✓ To the data subjects if the breach is likely to result in a high risk to the rights and freedoms of natural persons

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Data protection officer (DPO)

<u>Mandatory</u>, if the data controller/processor:

- the processing is carried out by a public authority/body (exception for courts acting in their judicial capacity), or

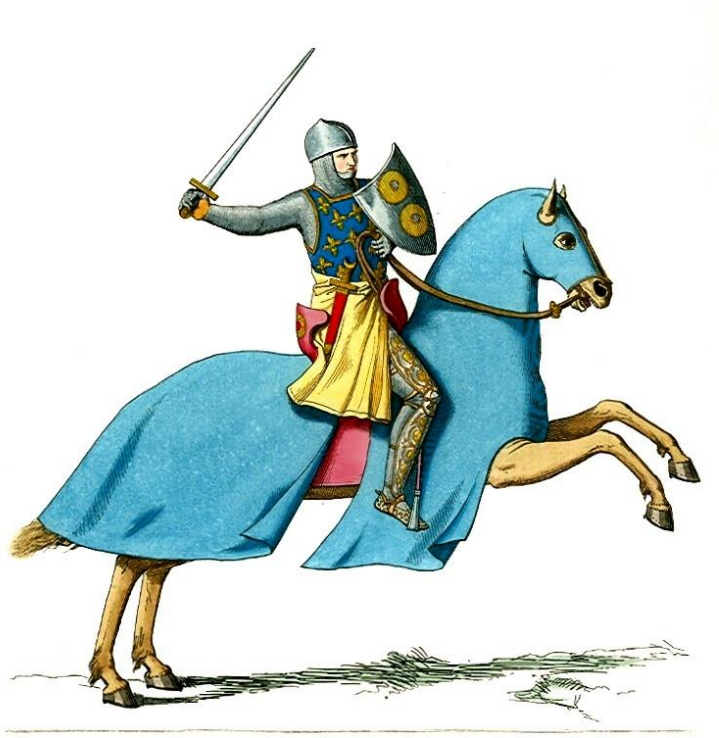
- The core activities:
  - ✓ require regular and systematic monitoring of data subjects on a large scale; or
  - ✓ consist of processing on a large scale of special categories of data pursuant and personal data relating to criminal convictions and offences

- **Member States/ EU could provide for <u>other</u> cases where DPO should be mandatory appointed.**

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Data protection officer (DPO)

- Involved **in all issues** related to the protection of personal data
- Employment contract (conflict of interest**!**)
- Service contract
- Contact point
- **Independence**



LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Final remarks

- ✓ Awareness
- ✓ Internal audit & problem identification
- ✓ Gap filling & risk management
- ✓ Transparency & accountability (including on documental level)
- ✓ Dynamic adjustment

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Thank you for your attention!

Contacts:
E-mail: martin.zahariev@dpc.bg
Phone: +3592/ 421-42-01; +359 888 95 00 77
Website: www.dpc.bg