EU GDPR:
4 RISK MITIGATION STEPS

Julius Zaleskis, PhD
Dataprotection.lt, Vilnius University (Lithuania)
www.dataprotection.lt

25 January 2018

Lecturer

- 2008-2017: data protection law practice at international law firm
- From 2010: teaching at Vilnius University (Lithuania)
- From 2011: national expert for various European Commission's and Council of Europe's studies
- From 2017: head of Dataprotection.lt
- All GDPR compliance services:
  - GDPR compliance audit and consultations
  - GDPR documents and procedures
  - Services of a data protection officer
  - Training for companies and data protection officers
  - Representation before data protection authorities and courts

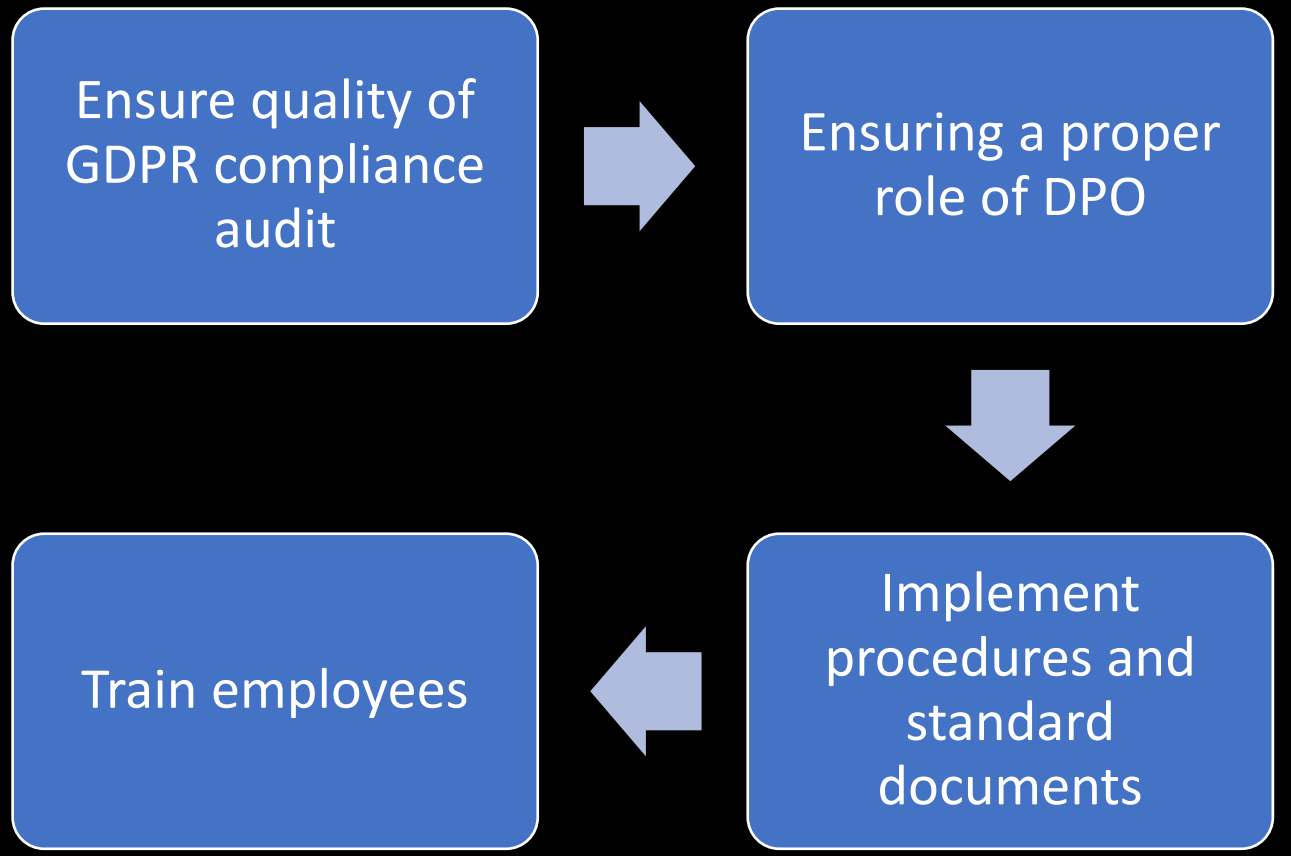
Definitions

- Art. 29 WP
- Data
- Data controller
- Data processor
- Data subject
- DPA
- DPO
- ECtHR
- GDPR

Why compliance matters?

- New directly applicable EU law
- Data economy
- Fourth industrial revolution
- Reputation
- International data flows
- Fines of up to 20 million euros or 4% of the total worldwide annual turnover

GDPR risk mitigation: 4 steps



1. ENSURE QUALITY OF GDPR COMPLIANCE AUDIT

Purposes of the audit

- Inventory of data processed
- Review of internal rules, procedures and other documents
- Assessment of IT used from the data protection perspective
- Assessment of the compliance with the GDPR requirements
- Identification of risks
- Preparing of a compliance action plan

Level of details of inventory

- Purposes of data processing as a starting point
- Categories of data
- Identification of special categories data
- Categories of data subjects
- Scale of data
- Actions of data processing
- Data recipients
- Data processors
- Access rights within organisation
- Data retention periods
- In depth inventory of automated decision making and profiling

Identification of data

- Any information
- Relating to
- Natural person
- Who can be identified

EU case law example: definition of data

- State institutions track IP addresses of its website visitors
- Part of IP addresses are dynamic, e.g., changing per each connection
- Internet service providers are legally prohibited from disclosing identity of users
- Do dynamic IP addresses constitute personal data?
- CJEU's 19 October 2016 judgment *Patrick Breyer* C-582/14:

  „The use by the EU legislature of the word 'indirectly' suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified. <...> legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings"

Principle-based requirements

- Lawful and specific data processing purposes
- Grounds for lawful data processing
- Data minimisation (data proportionality)
- Specific and proportionate data retention periods
- Exceptions allowing processing of sensitive data
- Specific grounds to transfer data to countries outside the EEA
- Crucial role of accountability

Alternative grounds for lawful data processing

- Consent
- Performance of a contract
- Legal obligation
- Vital interests of the data subject
- A task carried out in the public interest or in the exercise of official authority vested in the controller
- Legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of the data subject

EU case law example: legitimate interests (1)

- A taxi passenger committed administrative offence by opening the door and damaging the passing trolleybus
- To bring civil proceedings against the passenger, trolleybus company requested national police to provide the first name and surname, identity document number, and address of the taxi passenger, the statements given in the case
- The police provided the first name and surname, but not the remaining information which can be disclosed only to the parties of proceedings
- Can a legitimate interest (1) justify and (2) obligate the requested disclosure?
- CJEU's 4 May 2017 judgment in Rīgas C-13/16:

  „the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest <...> communication of merely the first name and surname of the person who caused the damage does not make it possible to identify that person with sufficient precision <...>. Article 7(f) of that directive does not preclude such disclosure on the basis of national law".

ECtHR case law: legitimate interests (2)

- In Romania employer adopted internal rules prohibiting personal use of provided work computer and internet access, employees signed these rules
- Employer determined that an employee in his work time used *Yahoo Messenger* to chat with fiancée and brother and dismissed him
- Romanian courts found that a lawful balance between was struck between employer's business interest and employee's privacy interest
- Was there a privacy violation?
- ECtHr Grand Chamber's 5 September 2017 judgments in *Bărbulescu v. Romania:*

  No, because domestic courts did not assess, whether an employee was informed of computer monitoring, were there specific reasons justifying monitoring, was it is possible to achieve purposes by less intrusive means

Grounds for transferring data to third countries

- European Commission’s adequacy findings
- Binding corporate rules
- Standard data protection clauses adopted by the Commission
- Standard data protection clauses adopted by a DPA and approved by the commission
- An approved code of conduct
- An approved certification mechanism

Whitelisted countries and sectors

- Andorra
- Argentina
- Canadian commercial organisations
- Faeroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
- US companies having Privacy Shield certification

EU case law example: international data transfers

- Woman working in church set up a webpage including information on her colleagues: names, hobbies, jobs, telephone numbers
- The information became accessible anywhere in the world
- Does such data processing constitute transfer of data to third countries?
- CJEU's 6 November 2003 judgment Bodil Lindqvist Case C-101/01:

  „Given, first, the state of development of the internet at the time Directive 95/46 was drawn up and, second, the absence, in Chapter IV, of criteria applicable to use of the internet, one cannot presume that the Community legislature intended the expression transfer[of data] to a third country to cover the loading, <…>, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them."

2. ENSURE A PROPER DPO‘S ROLE WITHIN AN ORGANISATION

Guiding principles

- Expert competence
- Independence
- No conflict of interest
- Accessibility
- Necessary resources
- Confidentiality
- Accountability

How to ensure cooperation with the DPO?

- Process-level awareness of data protection requirements
- Data protection audits
- Procedure for communication
- Standard questionnaires and checklists
- Constant follow-ups
- Training

DPO’s role: practical example

- The DPO may consider that a new CRM system is likely to result in a high risk for data protection because of extensive data being collected
- The DPO advises a project leader to carry out a data protection impact assessment
- The project leader does not agree with the DPO’s assessment, states that the DPO acts contrary to business needs
- The project leader refers the DPO to HR department for incompetence and proceeds with the project
- What steps the DPO should take?
- What action can be taken against the DPO?
- What steps the DPO could take to avoid the situation?

3. TAKE CARE OF A PROPER SET OF PROCEDURES OF DOCUMENTS

Procedures to be prepared (1)

- No exhaustive list
- Accountability
- Data protection policy / rules
- User-friendly manuals
- CCTV
- Management of data breaches

Procedures to be prepared (2)

- Management of data subjects’ complaints and requests
- Involvement of the DPO
- Data protection impact assessments and prior consultations
- Using letigimate interest provision
- Obtaining consent
- Data protection by design and by default
- IT security

Other documents to be prepared

- No exhaustive list
- Identification of lead and concerned DPAs
- Consent forms
- Information forms
- Web privacy policies
- Provisions for customer contracts
- Provisions for employment contracts
- Data processing agreement
- Cookie and other disclaimers
- Data processing records

FINETUNE A PROCEDURE ON MANAGEMENT OF DATA BREACHES

Concept of data security breach

- Accidental or unlawful destruction
- Accidental or unlawful loss
- Accidental or unlawful alteration
- Unauthorised disclosure
- Unauthorised access
- Unauthorised transmission
- Unauthorised storage
- Other unauthorised processing

Possible risks

- Physical damage
- Material damage
- Non-material damage
- Loss of control over data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of data protected by professional secrecy
- Any other significant economic or social disadvantage

Assessment of risks

- Data controller can demonstrate that data breach is unlikely to result in a risk to the data subject
  - No notification needed
- Data controller cannot demonstrate the above, however, the breach is not likely to result in a high risk
  - Notifcation to the DPA needed
- The breach is likely to result in a high risk
  - Notifcation needed to both, the DPA and the data subjects
- Upon notification the DPA determines that the breach is likely to result in a high risk
  - Obligation to notify the data subjects

Data security breach notification: practice

- Computer was stolen from an insurance broker
- Computer was encrypted and password protected, no back-up copy
- Computer contained over 100 insurance applications with comprehensive data of potential clients
- What ultimate or hypothetical risks are clients exposed to?
- Does the security breach trigger notification to DPA and data subjects?
- Which means could a data controller implement to mitigate risks?

FINETUNE A PROCEDURE ON MANAGEMENT OF DATA SUBJECTS' REQUESTS

Rights of data subjects

- Right of access
- Right to rectification
- Right to be forgotten
- Right to restriction of processing
- Right to data portability
- Right to object to data processing
- Right not to be subject to automated individual decision-making, including profiling

Elements of data portability

- Right of the data subject to receive data and to store those data for further personal use
- A right to transmit personal data from one data controller to another data controller without hindrance

Limits of the right

- Processing means (electronic)
- Ground for processing (consent or agreement)
- Content of data (data relating to individual implement a right)
- Data source (the data subject)
- Protection of other persons
- Repetitive or manifestly unfounded requests

Practical example: portability

- On 26 May 2018 a company receives a request from dismissed employee to transfer e-mail inbox to a new employer
- How to address the request?
- How the internal procedure should regulate this type of cases?

FINETUNE A PROCEDURE ON DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATIONS WITH DPA

The concept

- Replacing procedure on general notification of data processing to the DPA
- Applied to data processing operations: IT systems, applications, devices
- Legal rather than IT assessment
- Advance nature
- Assessment on whether assessment is necessary
- Importance of documentation
- Risk-based approach
- Conclusion determined necessity for consultations with the DPA

Operations requiring for assessment

- Likelihood of a high risk to the data subjects
- Systematic and extensive automated evaluation of personal aspects, including profiling, producing legal or similar significant effects to the natural person
- Processing on a large scale of sensitive data
- Systematic monitoring of a publicly accessible area on a large scale
- List of processing operations requiring for data protection impact assessment
- List of processing operations not requiring for data protection impact assessment

TAKE CARE OF DOCUMENTATION SHOWING WHICH DPAs ARE LEAD AND CONCERNED

Lead DPA

- One stop shop for supervision of cross-border data processing
- Place of main establishment
- Central administration within the EU
- Place of the EU establishment where data processing decision are adopted and implemented
- Several lead DPAs

Concerned DPA

- Two necessary conditions to join in:
  - Breaches of exceptionally national nature
  - The lead DPA does not decide on investigation within 3 weeks upon receipt of information
- Procedure of cooperation
- Procedures of mutual assistance and joint investigations

EU practical example: lead DPA

- A bank has its corporate headquarters in Sweden, and all its banking processing activities are organised from there.
- Bank's insurance department is located in Oslo. Establishment in Oslo has the power to decide on all insurance data processing activity and to implement these decisions for the whole EU.
- Clients are located in all Scandinavian and Baltic countries.
- Which supervisory authority would be the lead authority in respect of the cross border processing of personal data?

TAKE CARE OF A STANDARD DATA PROCESSING CONSENT FORM

Requirements for consents

- Freely given
- Specific
- Unambiguous
- Informed
- Form
- Provable
- Revocable

EU case law example: consent

- Subscribers had consented to have their personal data published in one directory
- The subscriber has been correctly informed of the possibility that his personal data may be passed to a third-party undertaking for the same purpose
- Is renewed consent needed from the subscriber for the passing of those same data to another undertaking?
- CJEU's 5 May 2011 judgment *Deutsche Telekom AG* C-543/09:

  „No, if it is guaranteed that the data in question will not be used for purposes other than those for which the data were collected with a view to their first publication".

FINETUNE A STANDARD DATA PROTECTION NOTICE

General information requirements

- Identity and contact details of the data controller
- Data processing purposes
- Grounds of lawful data processing
- Data retention periods
- Rights of the data subjects
- Right to file a complaint with the data subject

Additional information, if needed

- Identity and contact details of the data controller’s representative
- Whether the data subject is obliged to provide the personal data
- The right to withdraw consent at any time
- Specific interests of the data controller or a third party
- The existence of automated decision-making, including profilig, the logic involved, envisaged consequences of such processing
- The recipients or categories of recipients of the personal data
- Transfer of data to a third country or international organisation and the ground therefor
- Contact details of the DPO

4. TRAIN EMPLOYEES

Who should be trained?

- Management
- IT
- HR
- Marketing
- Customer service
- Legal
- Accountancy
- Other

www.dataprotection.lt

info@dataprotection.lt