École Pour l'Informatique et les Techniques Avancées – EPITA

Masters program – Nov 2021

Course: Data Privacy by Design

Course instructor: M Salman Nadeem

mohammad-salman.nadeem@epita.fr

Data Privacy by Design (PbD)

Course schedule (tentative)

Date & Time	No.	Topics	Duration (in hours)
22/10/2021 *	1	Data & its types, Information & knowledge, Introduction to Data Privacy by Design (PbD)	3 hours
29/10/2021 *	2	DPbd Case studies, Data privacy risks & solutions	3 hours
05/11/2021 *	3	Privacy Enhancing Technologies (PET's)	3 hours
12/11/2021 *	**4**	**General Data Protection Regulation (GDPR), PbD and GDPR**	**3 hours**
19/11/2021 *	5	Open session, Putting it all together, Quiz, Final project presentation	3 hours
* Check 'Zeus' for exact timing of each class		***Total Lecture (hours)***	***15***

Evaluation: 10% Class attendance + 10% Class participation + 30% Class/home exercises + 50% Final Evaluation

Lecture 4 Outline

- **GDPR: Introduction & key definitions**
  - **GDPR**
  - **Complemented by**
  - **Roles**
  - **Data protection impact assessment (DPIA)**
  - **DPO, DPA and EDPB**

- GDPR: Scope and Other aspects
  - Lawful basis for processing
  - Privacy by design (PbD)
  - Privacy by default
  - Individual (subject) rights
  - Accountability and governance
  - Cross-border data transfers
  - Security & Data breaches
  - Sanctions & fines
  - GDPR Mantra (+ other aspects)
- Closing
  - Putting it all together

General Data Protection Regulation (GDPR)

- A legal framework applicable directly in EU countries
  - Came into effect on **25th May 2018**
  - Repealed the previous European Directive (95/46/EC) from 1995 on Data Privacy
- Complemented by:
  - Do-not-call-me list
  - National Register Number
  - E-commerce laws
  - Cookie policy
  - ePrivacy
  - …

Why GDPR?

- Motivations behind the regulation:
  - Lecture 1 slides:
    - Your data belongs to you!
    - It's a legitimate expectation that companies handle data with care
    - Companies must adapt to work with only the personal data they need for relevant purpose(s)
- Better control & enforcement

"Only a minority (15%) feel they have complete control over the information they provide online"

Special Eurobarometer 431

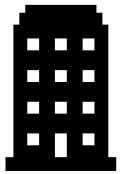
Source: https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

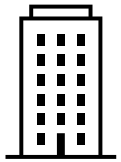
Key definitions!

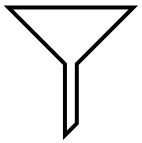
- **Personal data OR Personally Identifiable Information (PII):** Any information relating to an identifiable natural person (that can be directly or indirectly identified in particular by reference to an identifier)
- **Special categories of personal data** ("sensitive" data):
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade-union membership
  - Data concerning health, sexual orientation, …
  - Genetic or biometric data

Roles

- **Data Subject**: an individual who is the subject of personal data = any individual consumer
- **Data Controller**: an entity that determines the purposes and means of processing personal data
- **Data Processor**: an entity responsible for processing personal data on behalf of a controller
- What is **Data Processing**?
  - Collecting, recording, holding, transferring or deleting personal data are examples
  - Carrying out any operation or set of operations on personal data

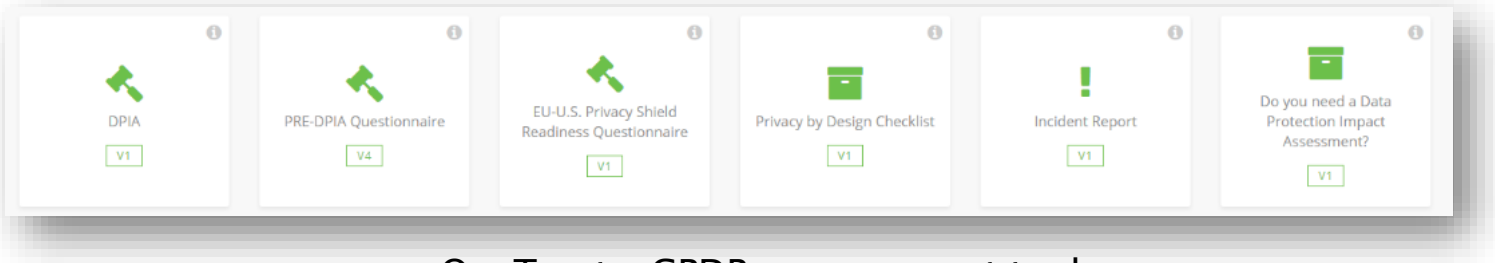






DPIA – Data protection impact assessment

- What?
  - Report assessing the risks and evaluating the technical and organizational measures
- When?
  - GDPR mandates a DPIA be conducted where data processing "is likely to result in a high risk to the rights and freedoms of natural persons"
  - Example tool (to conduct DPIA):



OneTrust – GPDR management tool

DPO, DPA and EDPB

- Data protection officer (DPO)
  - Official role as part of the accountability framework of the GDPR
  - Mandatory under certain circumstances e.g., Hospital: processing large sets of sensitive data
- Reports to national Data Protection Authority (DPA)
  - DPAs are co-operated by European Data Protection Board (EDPB): an independent European body whose purpose is to ensure consistent application of GDPR in EU

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

edpb
European Data Protection Board

Lecture 4 Outline

- GDPR: Introduction & key definitions
  - GDPR
  - Complemented by
  - Roles
  - Data protection impact assessment (DPIA)
  - DPO, DPA and EDPB

- **GDPR: Scope and Other aspects**
  - **Lawful basis for processing**
  - **Privacy by design (PbD)**
  - **Privacy by default**
  - **Individual (subject) rights**
  - **Accountability and governance**
  - **Cross-border data transfers**
  - **Security & Data breaches**
  - **Sanctions & fines**
  - **GDPR Mantra (+ other aspects)**
- Closing
  - Putting it all together

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

Scope

- Apply to company or organization controlling or processing personal Data of EU residents
  - Where no EU presence exists, the GDPR will still apply whenever:
    1. An EU resident's personal data is processed in connection with goods/services offered to him/her
    2. The behavior of individuals within the EU is *"monitored"*

1 – Lawful basis for processing

- There are six available lawful bases for processing
  - No single basis is 'better' or more important than the others (and it all depend on your purpose and relationship with the data subject)

1. Consent
2. Contract
3. Legal obligation
4. Vital interests
5. Public task
6. Legitimate interests
7. Special category data
8. Criminal offence data

You must determine your lawful basis before you begin processing, and you should document it

Your privacy notice should include your lawful basis for processing as well as the purpose(s) of the processing

2 – Data Privacy by design

"The privacy of the data subject is taken into account from the start of the conception of products and services"

- Identify & Implement technical and organizational measures that protect personal data and apply the GDPR principles from start
  - Data PbD: Objective & Strategies
  - Concrete activities
  - Full-lifecycle protection

3 – Data Privacy by default

"The standard options are privacy-friendly"

- Is a part of Data Privacy by Design
- Set to the most privacy-friendly state by default:
  - Permission is requested before processing personal data
  - A minimal amount of personal data is requested and processed
  - …

4 – Individual (subject) rights

- The procedures in place should ensure that they cover all the individual rights
  - The right to be informed
  - The right of access
  - The right to rectification
  - The right to erasure
  - The right to restrict processing
  - The right to data portability
  - The right to object
  - Rights in relation to automated decision making and profiling
- How to exercise these rights:
  - E.g., send an email to entities holding your data
    - Email templates: Open **Microsoft Teams -> Data Privacy by Design (Teams) -> Files**

If your **rights are violated OR data is misused** then:

- File a complaint (to DPA)
- File a case in court
- Get NGO representation

5 – Accountability and governance

- Accountability and governance has been elevated to a significantly greater scale compared to old directives. E.g.,
  - Contracts (Data processing agreement, …)
  - Documentation (Processing registry, …)
  - Data protection by design and default (PbD)
  - Data protection impact assessments (DPIA)
  - Data protection officers (DPO)
  - Codes of conduct and certification
  - Guide to the data protection fee (if applicable, …)

6 – Cross-border data transfers

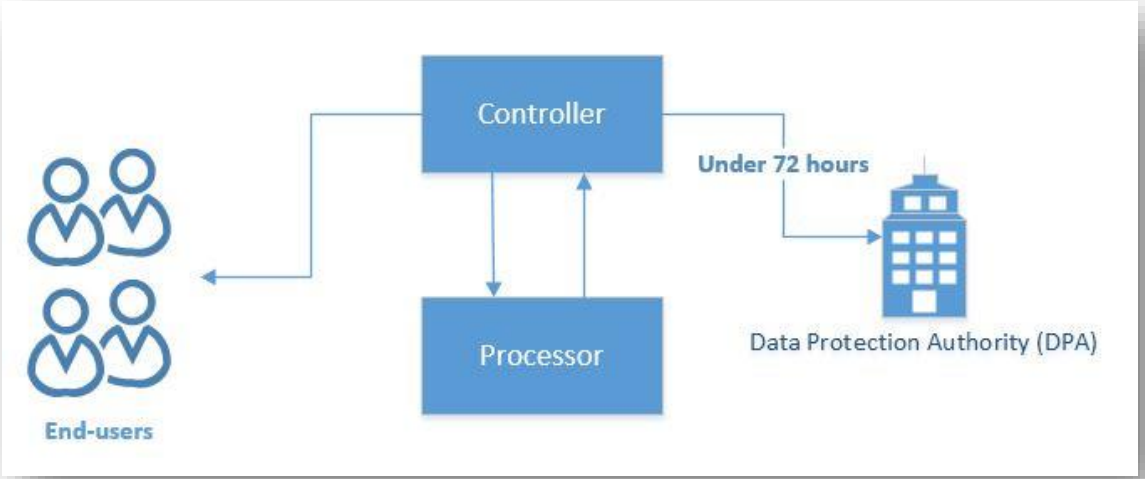
- The GDPR imposes restrictions on the transfer of personal data outside the EU, to third countries or international organizations
  - Any data processor/controller outside EU, will have to comply by GDPR
- These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined

7 – Security

- The GDPR requires personal data to be processed in a manner that ensures its security
  - This includes protection against unauthorized or unlawful processing and against accidental loss, destruction or damage
  - It requires that appropriate technical or organizational measures are used
    - See Lecture 3 (Data-PbD_Lecture-3.pdf): slide no. 10

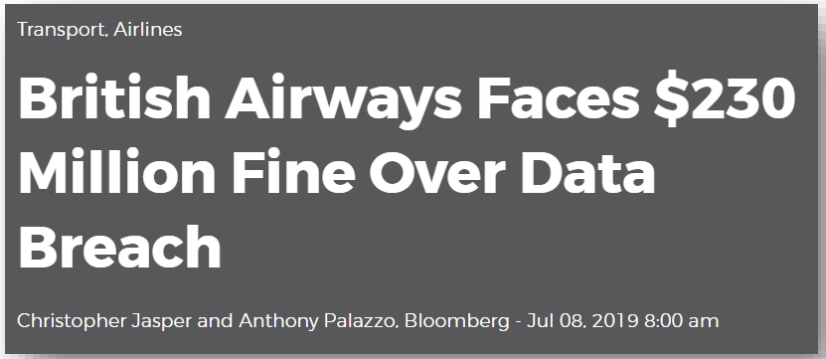
8 – Data breaches

- The GDPR introduces a duty on all organizations to report certain types of personal data breach to the relevant supervisory authority (SA) under 72 hours
  - If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the affected individuals should be informed without undue delay
- Requires robust breach detection, investigation and internal reporting procedures
  - A record of any personal data breaches, regardless of whether you are required to notify or not should be kept

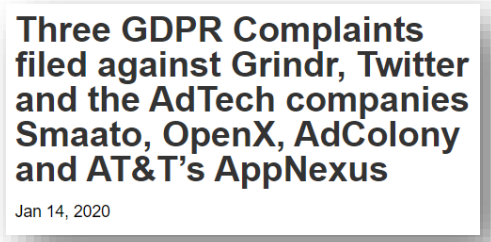


9 – Sanctions & Fines

- Hard sanctions and fines can be imposed e.g., Periodic data protection audits
  - A fine up to €10 million or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater
    - E.g., where there has been an infringement of a given article(s) /clauses of the GDPR



  - 2nd Level: In case of not reporting a data breach with-in the given time-frame
    - E.g., a fine up to €20 million or up to 4% of the annual worldwide turnover, whichever is greater
  - A warning in writing in cases of first and non-intentional non-compliance can given by the DPA too
  - …



10 – Other aspects

- Children between the ages of 13 and 15 (inclusive), can provide their own consent only via their legal guardians (whoever holds parental responsibility for the child)
- Unclear areas:

GDPR continues to evolve…

GDPR Mantra!

Data subjects rights have been widened!	• Adopt both your technical and administrative work-flows to orient them with data privacy at the core!
Document everything!	• Data handling procedures, incident response procedures, privacy by design procedures, data subject requests handling procedures…
Stay prepared!	• Design both your technical and administrative procedures to use them efficiently and effectively

Lecture 4 Outline

- GDPR: Introduction & key definitions
  - GDPR
  - Complemented by
  - Roles
  - Data protection impact assessment (DPIA)
  - DPO, DPA and EDPB

- GDPR: Scope and Other aspects
  - Lawful basis for processing
  - Privacy by design (PbD)
  - Privacy by default
  - Individual (subject) rights
  - Accountability and governance
  - Cross-border data transfers
  - Security & Data breaches
  - Sanctions & fines
  - GDPR Mantra (+ other aspects)
- **Closing**
  - **Putting it all together**

Putting it all together!

Privacy by design (Objective, Strategies, Activities)

+

Always remember the Crypto package!

+

Use of appropriate Anonymization/pseudonymisation techniques and PETs

+

Ensure threat detection and security controls

+

GDPR (Key definitions, Lawful basis for processing, Data Privacy by design & by default, Individual (subject) rights, Accountability and governance, Cross-border data transfers, Security, Data breaches, Sanctions & Fines, Other aspects)

Lecture 4 ends here

- Course material:

Open **Microsoft Teams -> Data Privacy by Design (Teams) -> Files**

- Send your questions by email:
  mohammad-salman.nadeem@epita.fr
  OR via direct message using MS Teams

- Thank You!