

# Information and technology law course

---

LECTURE 13-14 – 4-7 NOVEMBER 2024

FEDERICA CASAROSA – 2024/2025

# GDPR – Risk assessment and data breach

---

# Risk in GDPR

---

## Art. 24 GDPR Technical and organisational measures

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

Those measures shall be reviewed and updated where necessary.”

## Art. 25 data protection by design and by Default

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

# Risk in GDPR

---

## Art. 32 GDPR Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

# Risk in GDPR

---

## Art 35 DPIA

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

# What is a risk?

---

A “risk” is a scenario describing an event and its consequences, estimated in terms of severity and likelihood.

# Risk catalogue

---

## Recital 75

The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular:

- where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;
- where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed;
- or where processing involves a large amount of personal data and affects a large number of data subjects.

# DPIA

---

Overall effects of the data processing:

- Damage to reputation
- Discrimination
- Identity theft
- Financial loss
- Physical or psychological damage
- Loss of control of data
- Other economic or social disadvantages
- Inability to exercise rights, services or opportunities



# Risk assessment

---

“Risk assessment” can be defined as the coordinated activities to direct and control an organization with regard to risk.

Elements to be considered in the risk assessment:

- origin, nature, severity, **likelihood**, **impact** on the rights and freedoms of people;

# Risk assessment

---

## Recital 76

The likelihood and severity of the risks to rights and freedoms of individuals should be determined by reference to:

- The nature
- Scope
- Context
- Purposes of processing

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

		LIKELIHOOD			
		10 Low	20 Medium	30 High	40 Very High
IMPACT	10 Low	4	1	1	3
	20 Medium	4	5	7	7
	30 High	7	7	10	6
	40 Very High	7	12	14	9

# DPIA

---

In line with the risk-based approach carrying out a DPIA is not mandatory for every processing operation.

- DPIA is only required where a type of processing is “likely to result in a high risk to the rights and freedoms of natural persons” (Article 35(1)).
- The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers’ general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects.

In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is “likely to result in a high risk to the rights and freedoms of natural persons”.

# What is a DPIA?

---

The GDPR does not formally define the concept of a DPIA as such, but its minimal content is specified by Article 35(7):

- “(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned”;

# Which processing operations are subject to a DPIA?

---

Apart from exceptions, where they are “likely to result in a high risk”.

In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law.

Even though a DPIA could be required in other circumstances, Article 35(3) provides some examples when a processing operation is “likely to result in high risks”:

- “(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person<sup>12</sup>;
- (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- (c) a systematic monitoring of a publicly accessible area on a large scale”.

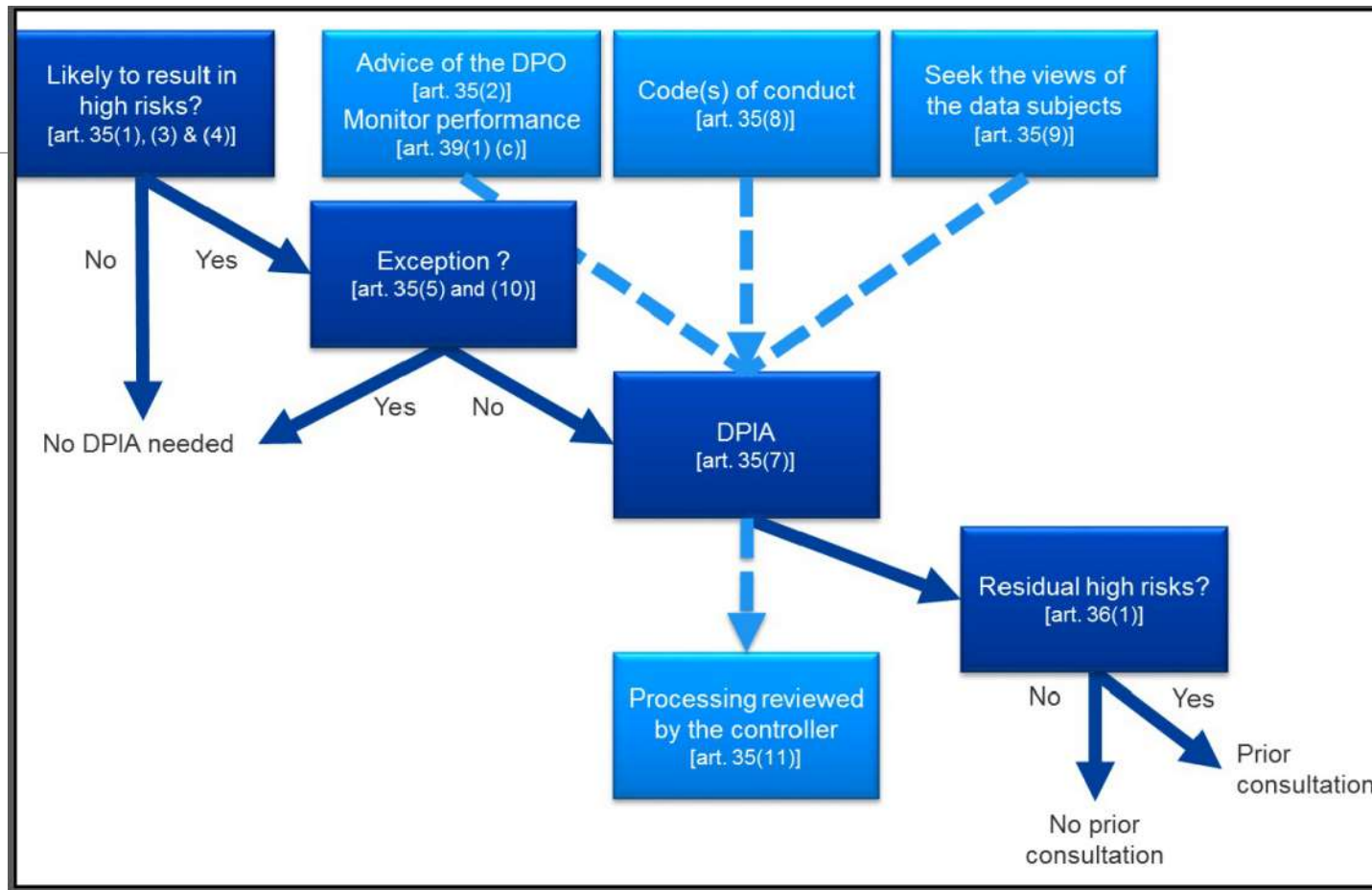
# When isn't a DPIA required?

---

WP29 considers that a DPIA is not required in the following cases:

- where the processing is not "likely to result in a high risk to the rights and freedoms of natural persons"
- when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out. In such cases, results of DPIA for similar processing can be used;
- when the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed;
- where a processing operation, pursuant to point (c) or (e) of article 6(1), has a legal basis in EU or Member State law, where the law regulates the specific processing operation and where a DPIA has already been carried out as part of the establishment of that legal basis;
- where the processing is included on the optional list (established by the supervisory authority) of processing operations for which no DPIA is required;





# How to carry out a DPIA? At what moment should a DPIA be carried out?

---

The DPIA should be carried out “prior to the processing”. This is consistent with data protection by design and by default principles

The DPIA should be seen as a tool for helping decision-making concerning the processing.

The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance.

Carrying out a DPIA is a continual process, not a one-time exercise.

# Who is obliged to carry out the DPIA?

---

The controller is responsible for ensuring that the DPIA is carried out.

Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.

The controller must also seek the advice of the Data Protection Officer (DPO).

If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information.

The controller must “seek the views of data subjects or their representatives” “where appropriate”.

# Sanctions

---

Non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority.

- Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)-(4)),
- Carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9)),
- Failing to consult the competent supervisory authority where required (Article 36(3)(e)),

.. can result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

# Security and data breach

---

# Risk in GDPR

---

## Art. 32 GDPR Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

# Personal data breach

---

art. 4(12) : A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

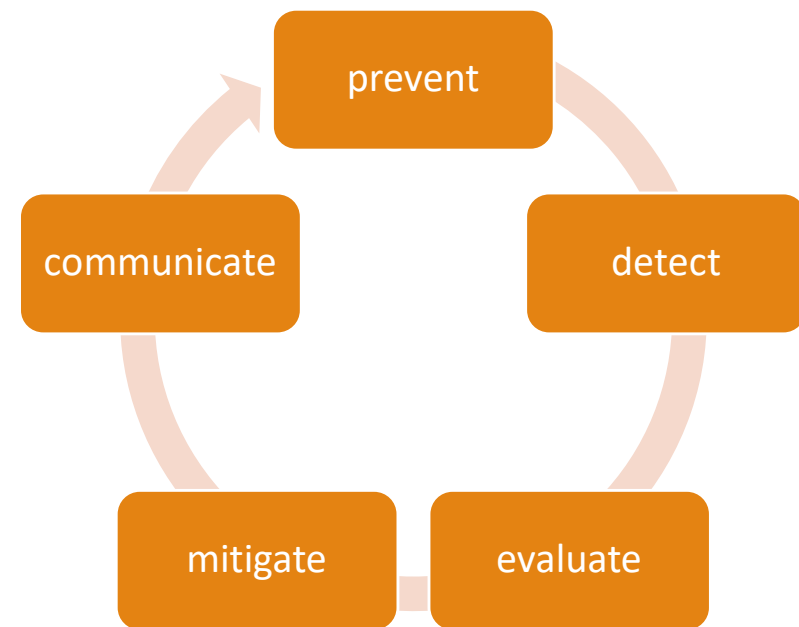
- Not all violations are data breaches
  - A security breach where there is no evidence that it has led to “accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”
  - Unlawful processing of personal data that is not due to a security incident.

# Data breach management framework

---

## Recital 87

It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject.





# Data breach management framework

---

## Prevent

- 1. Educate
- 2. Minimize (data collection, access to data, data stores, ...)
- 3. Dispose securely
- 4. Secure mobile devices (encryption, updates & patches, ..)
- 5. Secure networks (VPN)
- 6. Keep software & hardware up-to-date and maintained
- 7. Manage contractors
- 8. Develop & clearly communicate policies
- 9. Prepare for the worst (incidence response, disaster recovery)
- 10. Audit

# Data breach management framework

---

## Detect

- 1. Identify the security incident: What, when, who, where
  - The breach-detection gap
  - 90% of compromises happen within seconds/minutes; while the time to detect within seconds/hours accounts for just ca. 25% of the breaches (ETL 2016).
  - Tools:
    - Logging & monitoring
    - Intrusion detection & alerts.
- 2. Understand the root cause:
  - Was the breach due to a firewall with an open port, malware on the system, email phishing attack, outdated antivirus software, or an employee that accidentally disclosed personal data?
  - Tools:
    - Forensic analysis
    - Audit
- 3. Escalate & report (internally).

# Data breach management framework

---

## Evaluate

1. Is this a personal data breach?
2. Important: How to ascertain that technical and organisational measures are in place?
3. Do I have to notify a competent authority?
4. Do I have to communicate to data subjects?
  - IMPORTANT FACTORS TO BE TAKEN INTO ACCOUNT:
  - Types of personal data breached
  - Number of affected persons
  - What is the time between breach and detection

# Data breach management framework

---

## Mitigate

### Take immediate actions

- - e.g. isolate affected system, change passwords, take hacked webpages down (when possible!)
- - Ensure systems are out of danger (fix problem)
- - Document everything on the way
- - Take corrective actions (to avoid a new breach)
- - Notify (internally and externally)

# Data breach management framework

---

## Communicate (1)

### From processor to controller (internal)

- Art. 33 (2) GDPR : the processor must notify the controller immediately after becoming aware of the data breach
- Art. 28(3)(f) GDPR : Processors also must assist controllers in ensuring compliance with the latter's obligation to notify a breach to the DPA

# Data breach management framework

---

## Communicate (2)

### From controller to DPA


- Art. 33(1) GDPR : In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent ...
  - unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. [...].
- Art. 33 (4) GDPR : Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay

# Data breach management framework

---

Communicate (3)

Notification to DPA

- Nature of the breach, categories and approximate number of data subjects, categories and approximate number of personal data records concerned.
  - Name and contact information of DPO or other contact point.
  - Likely consequences of the breach.
  - Description of the measures taken or proposed to be taken in order to address the breach, as well as measures for the mitigation of possible adverse effects of the breach.
  - Additional information
- 

# Data breach management framework

---

## Communicate (4) to the data subjects

- Art. 33 (3) GDPR : When the breach is likely to result in high risk for the rights and freedoms of natural persons the data controller shall communicate the breach to the data subject without undue delay.
- BUT with exceptions
  - The data controller has implemented appropriate technical and organisational measures, and those measures were applied before the breach, in particular measures that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.
  - The data controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.
  - The communication involves disproportionate effort (public communication instead).



# Data breach management framework

---

Communicate (5) to the data subjects

Information to be provided to individuals

- Name and contact information of DPO or other contact point.
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

# Data breach management framework

---

Communicate (5) to the public

- Is there a legal obligation to communicate with a broader public?
- Data breach transparency
  - As an element of trust in relation between data subjects and controllers,
  - As a part of organization's assets (consider the compliance framework as an element affecting the worth of the company in case of an e. g. take over)
  - As a protection of organization's reputation