

The Duties of the Controller and Processor (II)

Elisa Spiller, Ph.D.

University of Padova | Dept. of Mathematics

Course of Law and Data 2022-2023



Learning objectives

- Duties, in general
- Risk and DPIA
- Data breaches

Problem solving

Due to the pandemic crisis, GreatCompany Corporation launched a new corporate welfare program for all its employees. To benefit of the program, you have to download the app of a new business partner, WeCare Inc. Once register and obtain your personal account, you have to enter all the data concerning your health and wellbeing, and the app will provide you a series of target discounts for medical visits and exam.

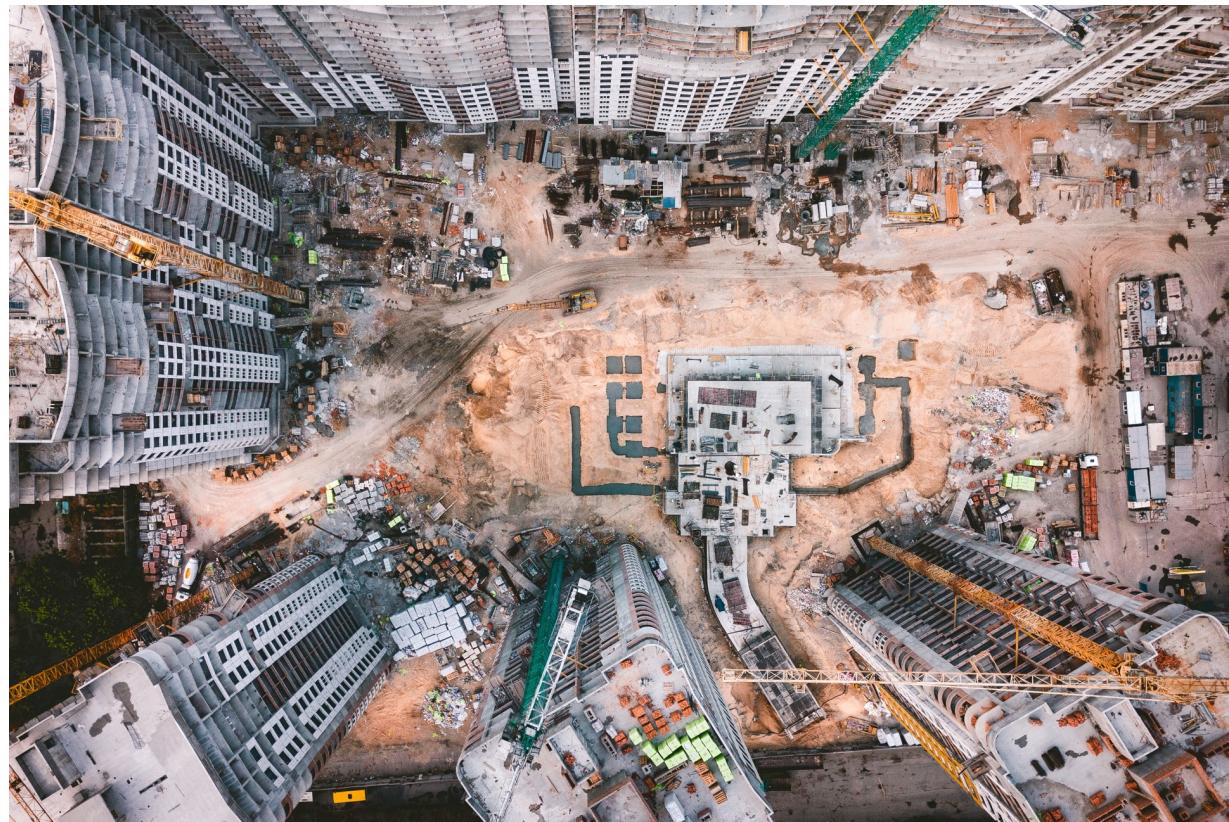
Considering the categories of data at issues, what are the problematic aspects of this policy?

1



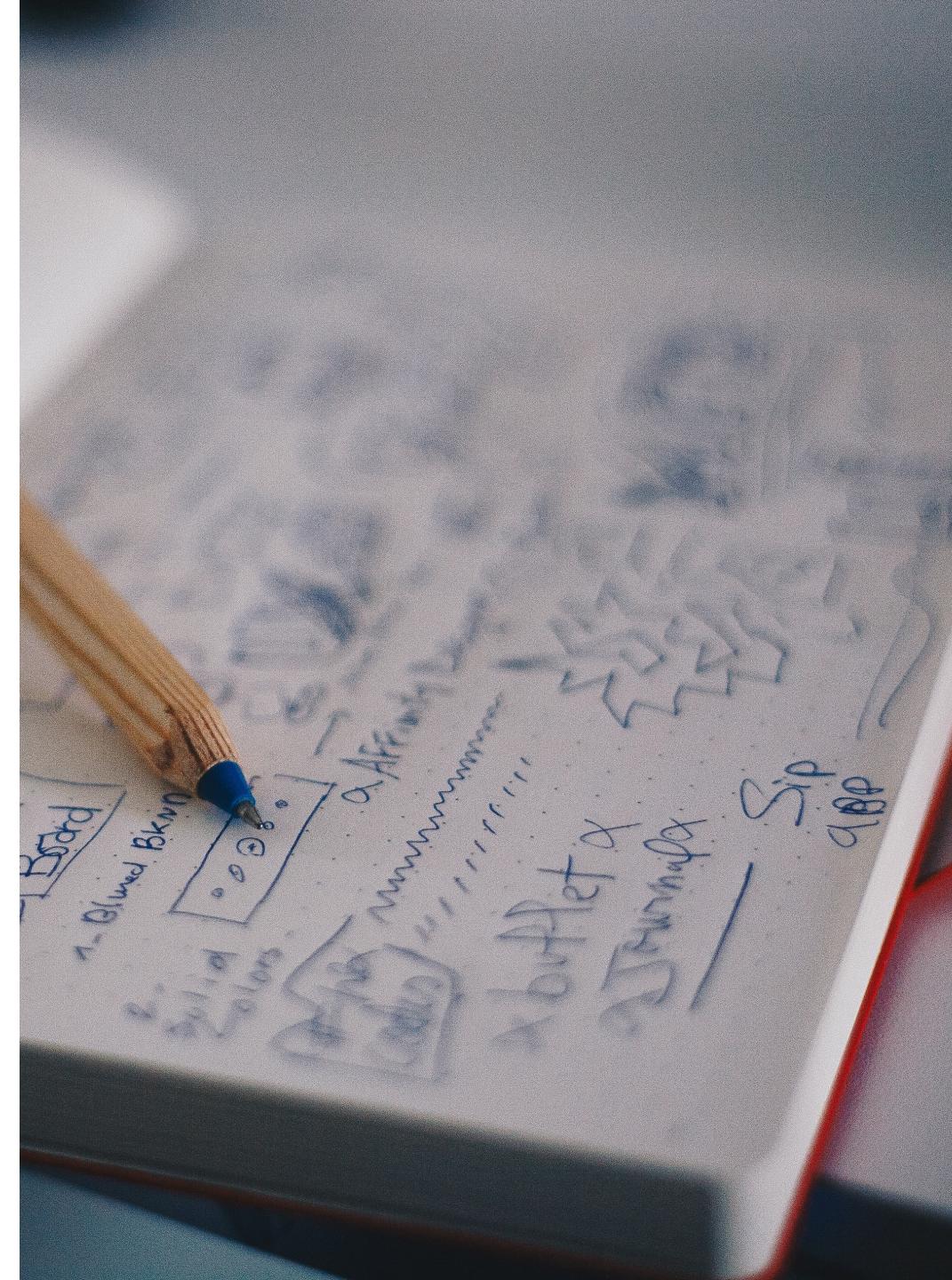
Duties

IN GENERAL



DOCUMENTAL DUTIES

- Internal policies on the protection of personal data
- Records of processing activities
- Cooperation with the supervisory authority
- **Notification and communication of a personal data breach**
- Codes of conduct

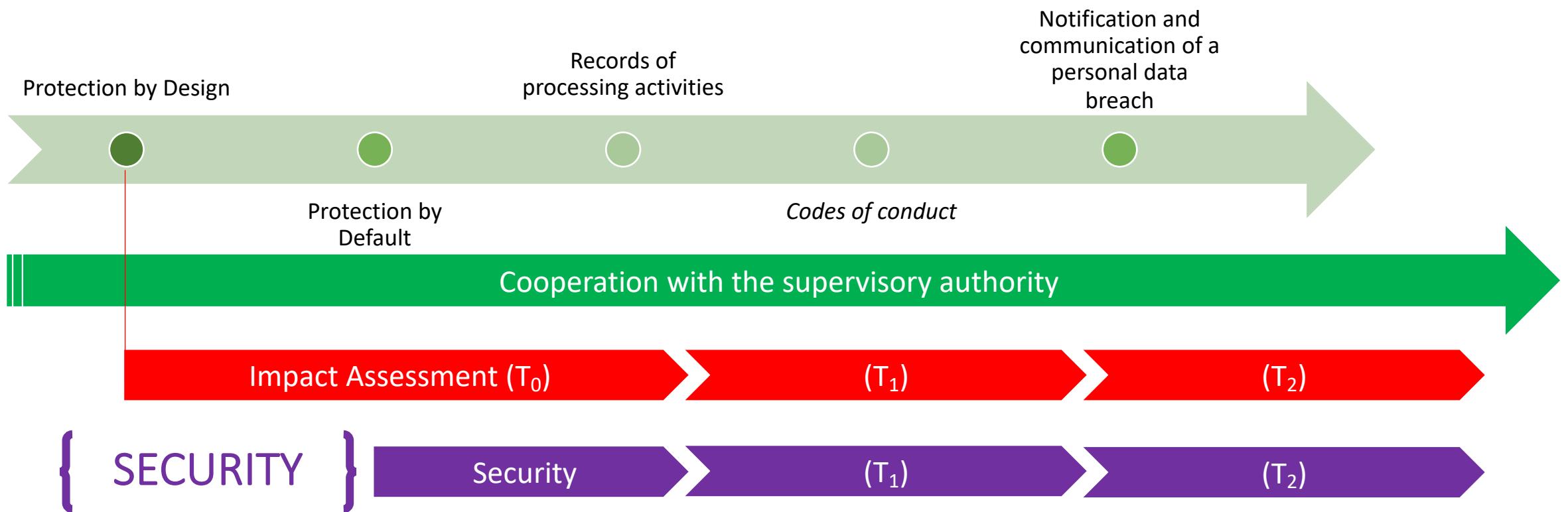


OPERATIVE duties

- Protection by Design
- Protection by Default
- Impact Assessment
- Security of processing



Processing over time





Risk in data protection law

Processing of personal data is a risky activity

Data protection law contains several risk criteria pertaining to the consequences. The GDPR, for instance, refers to “data processing which could lead to **physical, material or non-material damage**”.

These material and moral damages include *discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage*.

It then rehearses risk criteria concerning risk factors related to the type of data processed. It provides criteria concerning the risk factor related to the types of data subjects and ends with risk criteria concerning the risk factor related to the scale of the processing operation (amount of data and amount of data subjects).

Proactive protection

PRECAUTIONARY APPROACH

the act of caring in advance of
a **plausible but uncertain** danger

- ❖ The precautionary principle enables decision-makers to adopt precautionary measures **when scientific evidence about an environmental or human health hazard is uncertain and the stakes are high.**
- ❖ The precautionary principle divides opinions. **To some, it is unscientific and an obstacle to progress.** To others, it is an approach that protects human health and the environment.
- ❖ Different stakeholders, experts and jurisdictions apply different definitions of the principle, **mainly depending on the degree of scientific uncertainty required for the authorities to take action.**
- ❖ Although most experts agree that the precautionary principle does not call for specific measures (such as a ban or reversal of the burden of proof), **opinions are divided on the method for determining when to apply precautionary measures.**

PREVENTIVE APPROACH

the act of preventing or hindering
a **probable and well-defined** risk

- ❖ The preventive approach enables decision-makers to adopt preventive measures **based on solid scientific evidence about an environmental or human health hazard.**
- ❖ Usually, **it is more accepted than precautionary approach**, since it is based on solid and shared scientific evidence and protocols.
- ❖ It is now not only a question of repairing damages after they have occurred, but to prevent those damages occurring at all. **This principle is not as far-reaching as the precautionary principle. It means in short terms: it is better to prevent than repair.**
- ❖ Different stakeholders, experts and jurisdictions apply different definitions of the principle, **mainly depending on the degree of security/prevention expected**



2. impact assessment methodologies

DPIA

Article 35

Data protection impact assessment

1. 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.
2. *The controller shall seek the advice of the data protection officer (DPO), where designated, when carrying out a data protection impact assessment.*

a high risk to the rights and freedoms of natural persons

in particular using new technologies

legal and technological consultation under the guidance of the DPO

DPIA

Article 35

Data protection impact assessment

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
- 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;
 - 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.

a systematic and extensive evaluation of personal aspects

processing on a large scale of special categories of data

a systematic monitoring of a publicly accessible area on a large scale

DPIA

Article 35

Data protection impact assessment

7. The assessment shall contain at least: →

[...]

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

a systematic description of the envisaged processing operations

- and the purposes of the processing,
- including, where applicable, the legitimate interest pursued by the controller;

an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

an assessment of the risks to the rights and freedoms of data subjects

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.

prior consultation

Article 36

Prior consultation

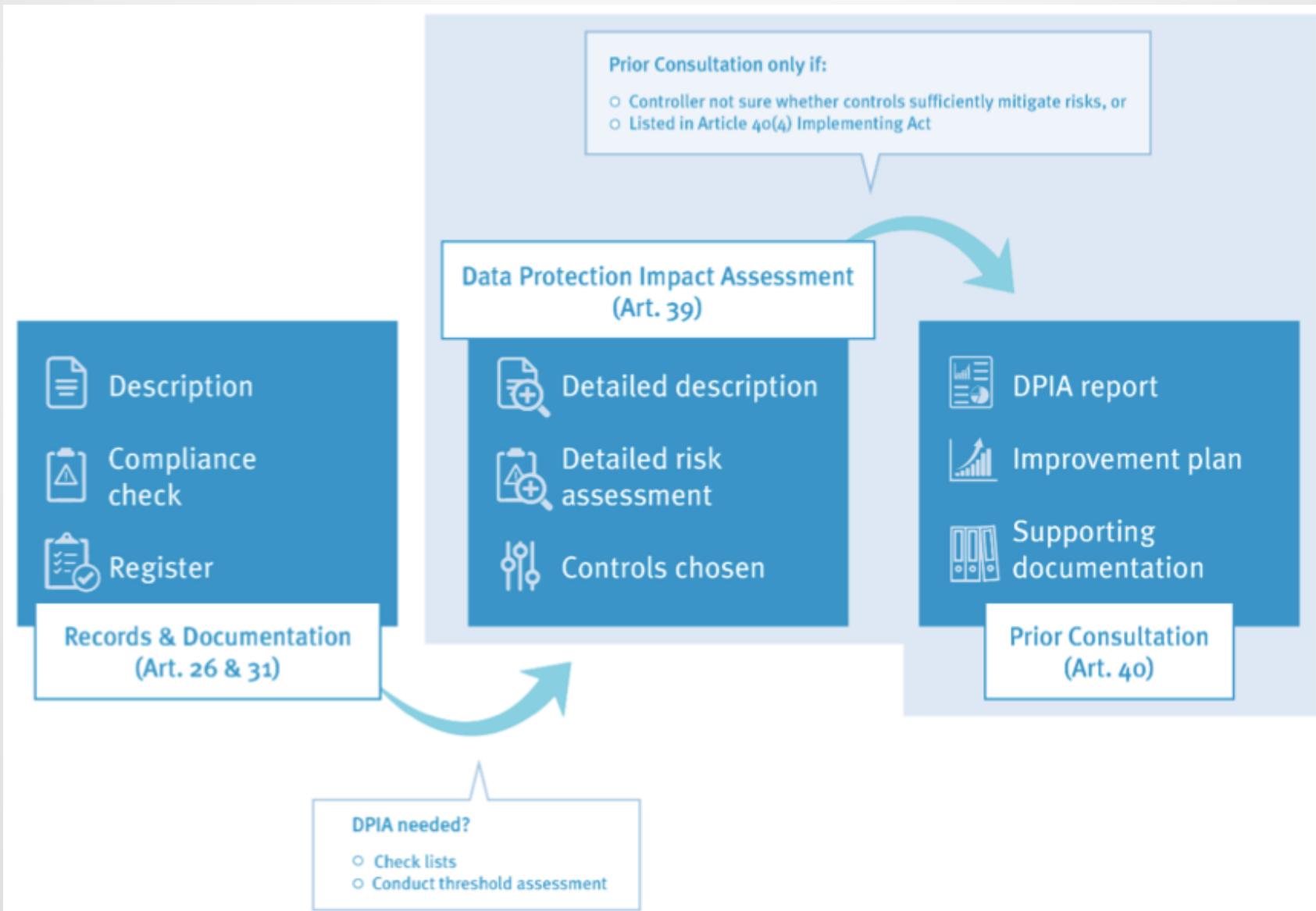
1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

where the controller has insufficiently identified or mitigated the risk

within period of up to eight weeks of receipt of the request for consultation

provide written advice to the controller and, where applicable to the processor

that period may be extended by six weeks, taking into account the complexity of the intended processing



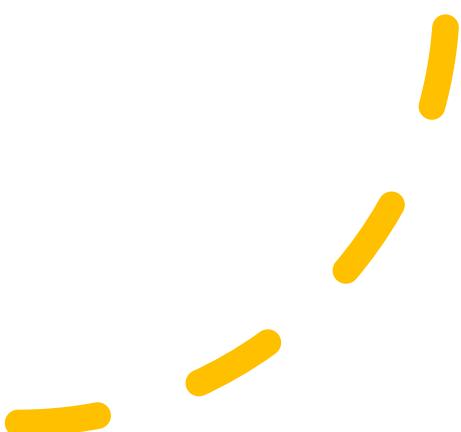


Security first!

The **Essence** of the right to the protection of personal data

«Nor is that retention of data such as to adversely affect the **essence** of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because [...], in relation to data protection and data security, [...] certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.»

EUCJ (2014), *Digital Rights Ireland*, § 40



GDPR – Article 32

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:

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

Taking into account...

the state of the art

the costs of implementation

the nature, scope, context and purposes of processing

the risk of varying likelihood

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

pseudonymization and encryption

confidentiality, integrity, availability and resilience of processing systems and services

availability and access in a timely manner in the event of a incident

regularly testing, assessing and evaluating the effectiveness of the security measures

GDPR – Article 32

Security of 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.
3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

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.

(3) Data breaches

```
    mirror_mod.mirror_object  
    operation == "MIRROR_X":  
        mirror_mod.use_x = True  
        mirror_mod.use_y = False  
        mirror_mod.use_z = False  
    operation == "MIRROR_Y":  
        mirror_mod.use_x = False  
        mirror_mod.use_y = True  
        mirror_mod.use_z = False  
    operation == "MIRROR_Z":  
        mirror_mod.use_x = False  
        mirror_mod.use_y = False  
        mirror_mod.use_z = True
```

```
selection at the end -add  
    _ob.select= 1  
    mirr_ob.select=1  
    context.scene.objects.active  
    ("Selected" + str(modifier))  
    mirror_ob.select = 0  
    bpy.context.selected_objects  
    data.objects[one.name].sele
```

```
    int("please select exactly one object")  
- OPERATOR CLASSES -----
```

```
types.Operator):  
    X mirror to the selected object.mirror_mirror_x"  
    "mirror X"
```



GDPR – Article 4 no. 12

«‘Personal Data Breach’ means 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»

...(consequences)

GDPR – Recital 85

A personal data breach may, if not addressed in an appropriate and timely manner, result in

physical damage

material damage

non-material damage

loss of control over their personal data

limitation of their rights

discrimination

identity theft or fraud

financial loss

unauthorised reversal of pseudonymization

damage to reputation

loss of confidentiality of personal data protected by professional secrecy

or any other significant economic or social disadvantage to the natural person concerned.

Notification to the supervisor authority

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, **the controller**
 2. **The processor** shall notify the controller without undue delay after becoming aware of a personal data breach.
- [...]
5. *The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.*

without undue delay notify to the competent national supervisory authority the personal data breach occurred

- where feasible, not later than 72 hours after having become aware of it
- where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

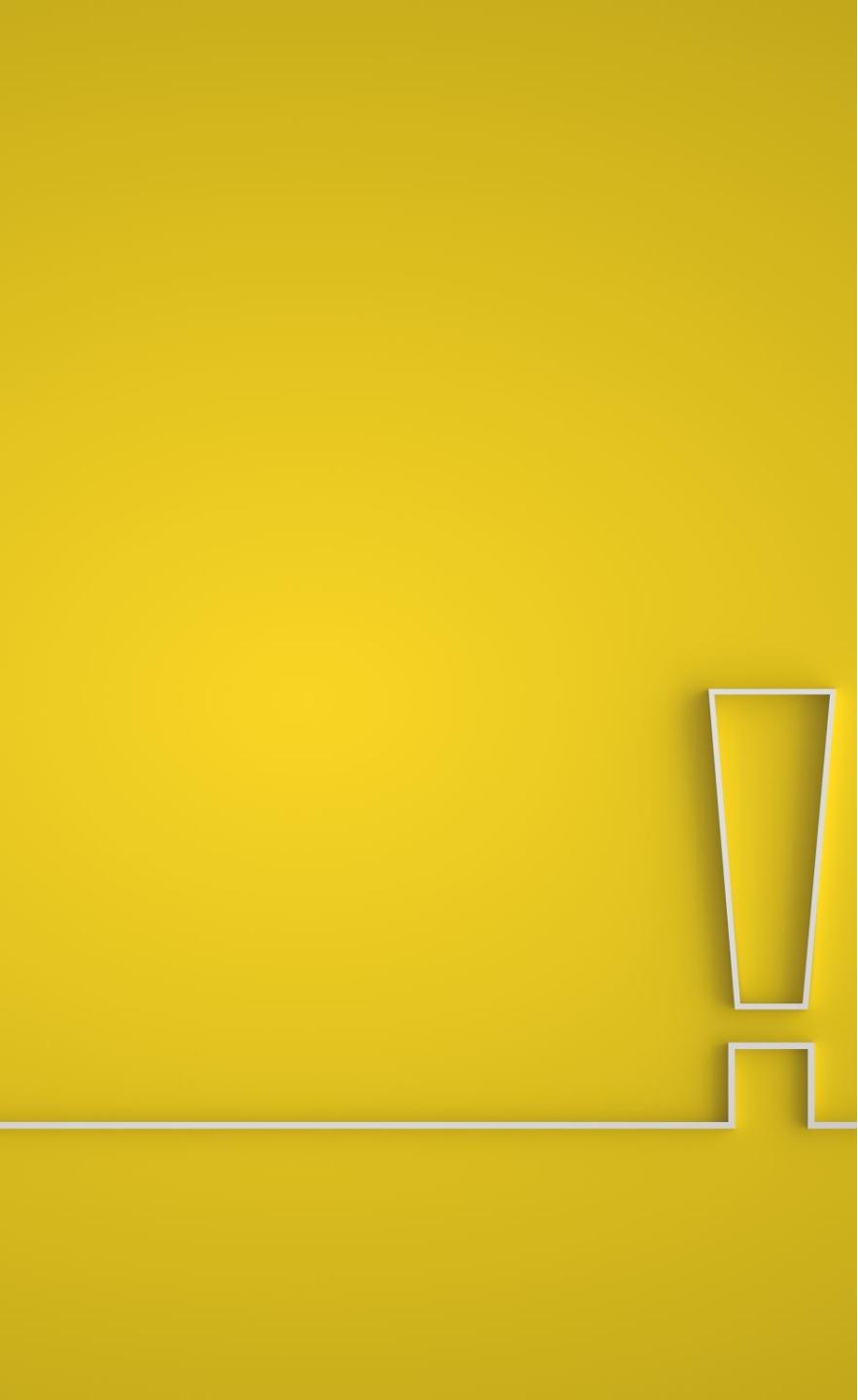
unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

Contents of the notification

Breach	Contacts	Consequences	Mitigations
<p>describe the nature of the personal data breach</p> <ul style="list-style-type: none">• including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned	<p>communicate the name and contact details of the data protection officer</p> <ul style="list-style-type: none">• or other contact point where more information can be obtained	<p>describe the likely consequences of the personal data breach</p>	<p>describe the measures taken or proposed to be taken by the controller to address the personal data breach</p> <ul style="list-style-type: none">• including, where appropriate, measures to mitigate its possible adverse effects

...WHAT ABOUT
THE DATA
SUBJECT?





Communication to the data subject

Article 34

Communication of a personal data breach to the data subject

1. When the personal data breach is **likely to result in a high risk to the rights and freedoms** of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
3. [...] not be required if any of the following conditions are met:
 - a. the controller has implemented **appropriate technical and organisational protection measures**, and those measures were applied to the personal data affected by the personal data breach, in particular those that **render the personal data unintelligible to any person who is not authorised to access it**, such as encryption;
 - b. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred [...] is **no longer likely to materialise**;
 - c. **it would involve disproportionate effort**. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner
4. *If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions [...] are met.*