General Data Protection Regulation (GDPR)

UMBERTO FONTANA

Notes from the lectures of Data Ethics and Data Protection Year 2021/2022

INTRODUCTION TO GDPR

The GDPR (General Data Protection Regulation) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. Article 8 of the **Charter of Fundamental Rights of the European Union** quotes:

1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for specified purposes and on the basis of the **consent of the person concerned or some other legitimate** basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
3. *Compliance with these rules shall be subject to control by an independent authority.*

By equalizing the rules for data protection, the GDPR shall lead to more legal certainty and remove potential obstacles to the free flow of personal data. The starting date of the GDPR is May 25, 2018.

GOALS OF EU'S GDPR

The main objective of the GDPR is:

- **Protection**: to protect personal data and strengthen privacy rights of EU individuals
- **Control**: Give users control over their data

Art. 1:

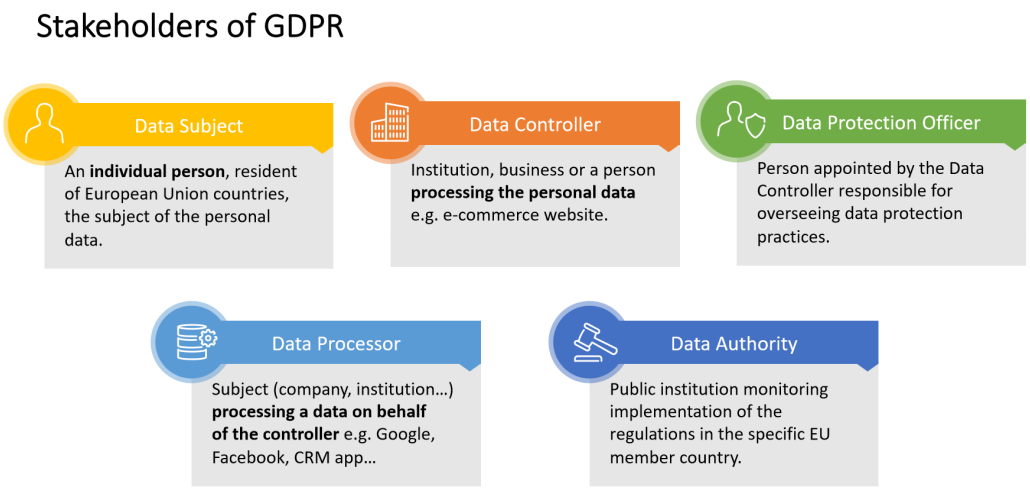
1. *This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data*
2. *This Regulation protects **fundamental rights and freedoms** of natural persons and in particular their right to the protection of personal data*
3. *The **free movement of personal data** within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data*

TO WHOM DOES THE REGULATION APPLY?

The GDPR applies to anyone *processing or controlling* the processing of personal data. Especially companies will be affected by the GDPR. It is important to define 2 figures: a **Controller** and a **Processor**.

- **Controller**: natural or legal person, public authority, agency or other *body* that, alone or jointly with others, determines the purposes and means of the processing of personal data, Art. 4 No. 7 GDPR. The importance of body the body definition is the following: each company within a group structure is solely responsible for the data processing taking place under its controllership. As a consequence, each entity is considered a controller. Joint controllership may take different forms: the relevant entities might have a very close relationship (e.g., sharing all purposes and means of a processing) or a more lose relationship (e.g., partially sharing purposes).

- **Processor**: is defined as a natural or legal person, public authority, agency or other body that processes personal data *on behalf* of the controller, Art. 4 No. 8 GDPR. Thus the existence of the processor depends on a decision taken by the controller, who can process data within its organisation (e.g., its own employees) or delegate all or part of the processing activities to an external organisation. It should be, to be considered a processor, a separate legal entity/individual with respect to the controller and it should process personal data on behalf of the controller.



The GDPR affects **All businesses collecting or holding personal data on EU citizens**, no matter where they reside! So, for example, if you process data of european citizen but not from europe, you must attempt to the right to be forgotten

TERRITORIAL SCOPE

Art. 3

This Regulation applies to the processing of personal data ***in the context*** *of the activities of an establishment of a controller or a processor in the Union,* ***regardless of whether the processing takes place in the Union or not***. ***Data subjects*** *who are in the Union by a controller or processor not established [Art. 4 No. 16] in the Union, where the processing activities are related to:*

- *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
- *the monitoring of their behavior as far as their behavior takes place within the Union.*

A case study: Entity J is located in Hong Kong and sells trend-oriented furniture and home accessories online. The products can only be paid in US dollar, and delivery to Europe is not offered. However, J wants to analyse the European market as it is considering expanding its business. Anyone calling up the website needs to accept the usage of cookies, and J analyses the IP geolocation data to determine the country where the user is located. J processes the obtained data in order to find out how many European customers from which Member States visit the website and what they are mainly interested in. In this example, J is using web tracking to analyse the preferences of customers located in the EU. Therefore, the GDPR applies.

A case study: Entity H is located in Australia and runs an online shop. The company has no subsidiaries or representatives abroad and the online shop is available in English only. H stores the customer data. Payment is accepted in Australian dollars, as well as euros, and deliveries

are possible to Germany, France and Italy. If customers from those EU Member States call up H's website, they are redirected from the domain 'H.au' to 'H.com/de', 'H.com/fr' and so forth. In this example, the separate domain name for European customers, the possibility of payment in euro and the possibility to deliver to certain EU Member States allow the conclusion that H addresses customers located in the EU. Therefore, the GDPR applies.

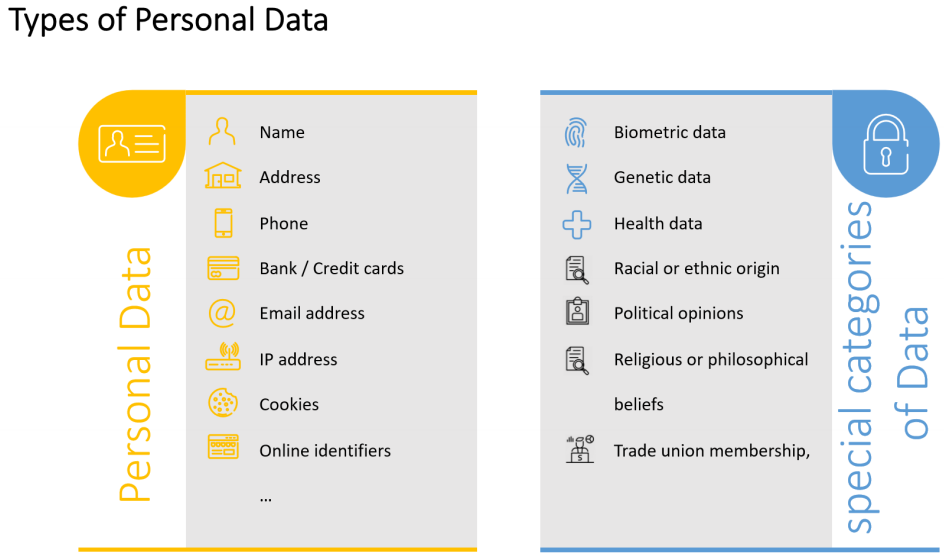
PERSONAL DATA

As shown above, any systematic handling of data corresponds to the notion of 'processing' under the material scope of the GDPR. However, data has to be personal in order to fall within said scope of application of the Regulation. Personal data does not apply to personal data of a deceased person. However, said data can be personal data of a relative or a descendant of the deceased (e.g., can give information on hereditary diseases of a descendant).

Art. 4

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is the 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 physiscal, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The IP address can be considered a personal identifier (static IP, the dynamic is not). In Italy you can track the person recurring to some legal actions, not like in Germany.



GDPR, Recital 26 (the recital is a statement explaining why they decided to create that article)

To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain (accertare) whether means are reasonambly likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

The **Anonymisation** is a way of modification of personal data with the result that there is/remain no connection of data with an individual. In case of effective anonyimisation, the GDPR *does not apply*. However, if the controller/processor can restore the anonymised information with reasonable likelihood, it will be deemed personal data under the GDPR.

The **Pseudononymisation** is a common tool to avoid the possibility to identify an individual through data. It is defined as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information,

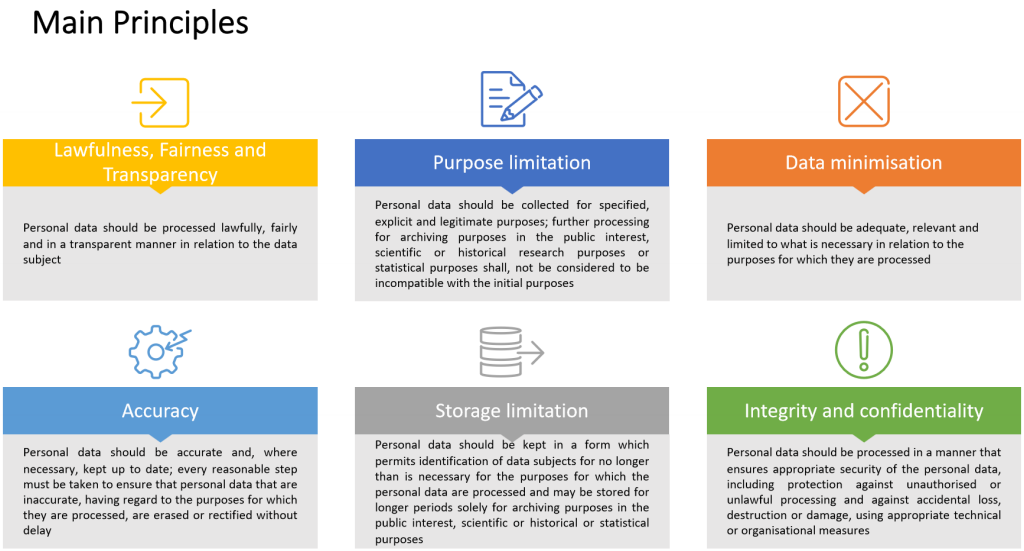


Fig. S1. Main principle when dealing with personal data

Art. 4 No. 5 GDPR. This could be achieved by replacing the name or other characteristics with certain indicators or by encoding the information an sharing the key with only few people. Unlike anonymous data, pseudonymised data still falls within the scope of application of the GDPR, as the risk of re-identification is higher with respect to the anonymous data.

ACCOUNTABILITY

The GDPR introduces the general *principle of accountability* in Art. 5 Sec. 2 GDPR, which imposes the *responsibility for the compliance* of processing with the GDPR and the *burden of proof* for said compliance onto the controller. In this prospective, *the controller shall be responsible for and be able to demonstrate compliance with the above principle*. In particular the contoller must justify the decision made. Even if the GDPR is not respected, this choose must be justified and well motivated.

The general accountability principle is *directly enforceable* and can be fined with up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover (Art. 83 Sec. 5 lit. a GDPR). This increase the pressure on controllers to implement appropriate measures for data protection.

Upon request of Supervisory Authorities, controllers must be able to prove their compliance with the GDPR under the accountability principle. In order to be able to fulfil their burden of proof, the controller's records of processing activities are likely to prove very helpful as details on the entity's data flows will be included in the records.

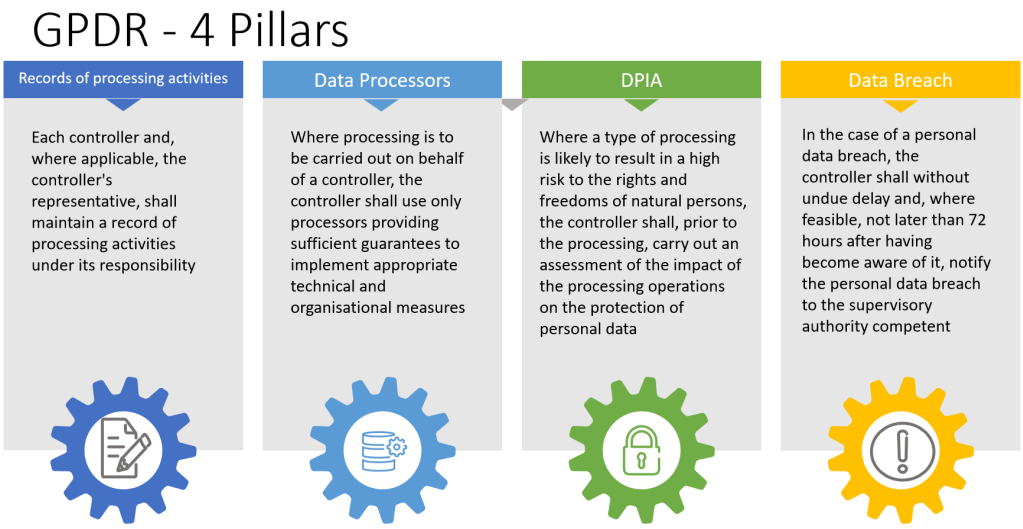
The general organisational data protection obligations for controllers and processors are laid out in Arts. 24 to 31 GDPR.

DATA PROCESSING

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data (even the reading), whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrival, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

GDPR PILLARS

- **Records of processing activities**: the requirements as to the content of the Records differentiate between the ones for controllers and for processors. The general responsibility for data protection under the GDPR lies with the controller, and the records shall demonstrate



compliance with the Regulation. Records shall be maintained *in writing*, including *electronic form*, Art. 30, Sec. 3 GDPR. Not all entities are obliged to do so. Art. 30 Sec. 5 GDPR provides for an exemption for any enterprise or organisation employing less than 250 persons. They will, most likely, not have sufficient financial and human resources to fulfil the obligation. The income though can make an exception; entities with an *annual turnover* exceeding EUR 50 million and/or an annual balance sheet total exceeding EUR 43 million do not benefit from this exemption.

- **Data Processors**: the controller is responsible and liable for data protection obligations. This does not mean that the controller has to carry out data processing itself as it can use a processor to act on its behalf. Processing by the processor shall only take place upon *instruction of the controller*, Art. 29 GDPR. The processor is not a 'third party' to the data processing under the GDPR. A third party is legally defined as a person 'other than the data subjectm controller, processor [...]', Art. 4 No. 10 GDPR. According to Art. 28 Sec. 1 GDPR, if the controller chooses to involve a processor, it must engage a suitable processor in order to guarantee a high level of data protection. The processor has several obligation: implement *technical and organizational measures*, appoint (nominare) a *representative* withing the EU if the processor is located outside the EU, maintain a record of processing activities (less comprehensive than the one that must be maintained by the controller), cooperate with the Supervisory Authorities, designate a *Data Protection Officer*. Upon writter authorisation of the controller, the processor can designate a sub-processor.

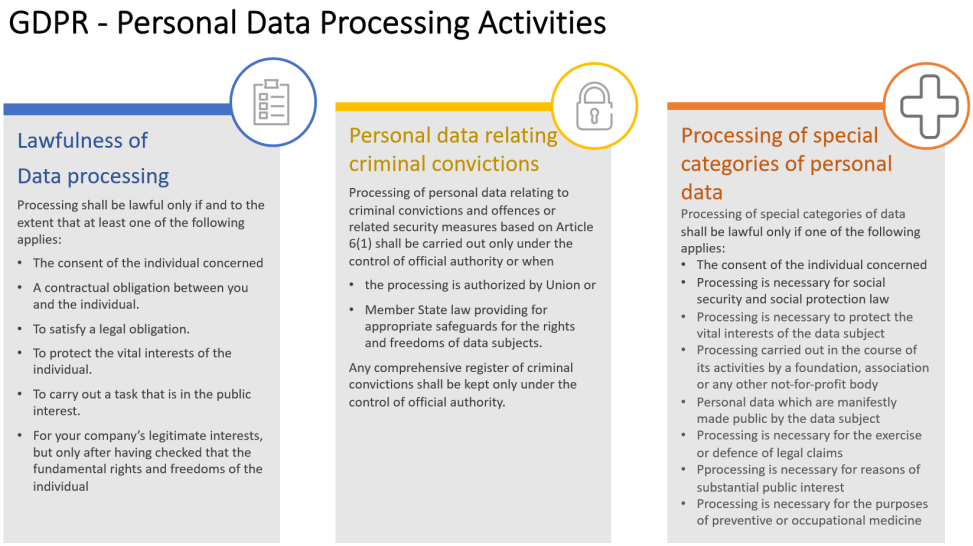
- **DPIA**: the controller needs to make a prognosis on the impacts of its future data processing activities if it identifies the likeliness of a high risk. A lot of processing activities involving considerable amounts of data will require a Data Protection Impact Assessment. High-risk processing operations regarding the rights and freedoms of data subjects might require DPIA. An example: An entity wants to introduce a data loss prevention application to scan the entity's entire email traffic for possible leakage of trade secrets. As all emails, which qualify as personal data of the respective communication parties, are scanned, this might constitute a processing activity that involves a systematic and extensive evaluation of personal data by automated means (¼ the security application). Thus, a Data Protection Impact Assessment might have to be carried out.

- **Data Breach**: a data breach according to Art. 4 No. 12 GDPR, is 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. In case of a personal data breach,

the controller shall notify the competent Supervisory Authority without undue delay and, if possible, not later than 72 h after becoming aware of the data breach, Art. 33 Sec. 1 GDPR. The failure to do so is punishable with fines of up to EUR 10,000,000.00 or 2% of the total worldwide annual turnover. Notice that the processor must notify *only* the controller without undue delay of the data breach. The controller is obliged to document any personal data breaches, including the facts relating to the breach. When identifying the likeliness of a high risk of the data breach to the rights and freedoms of individuals, the controller shall communicate the personal data breach to the involved data subjects without undue delay, Art. 34 Sec. 1 GDPR. The notification shall allow the data subjects to take the necessary precautions and should describe to them the nature of the personal data breach, as well as recommendations for the data subjects to mitigate potential adverse effects.

GDPR PERSONAL DATA PROCESSING ACTIVITIES

According to Art. 4 Sec. 11 GDPR, consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which it signifies agreement to the processing of its personal data.



Condition for consent

The controller shall be able to demonstrate that the data subject has consented to the processing, Art. 7, Sec. 1 GDPR. Thus, it bears the burden of proof, for example, if a data subject claims to have given no valid consent. This corresponds to the controller's accountability.

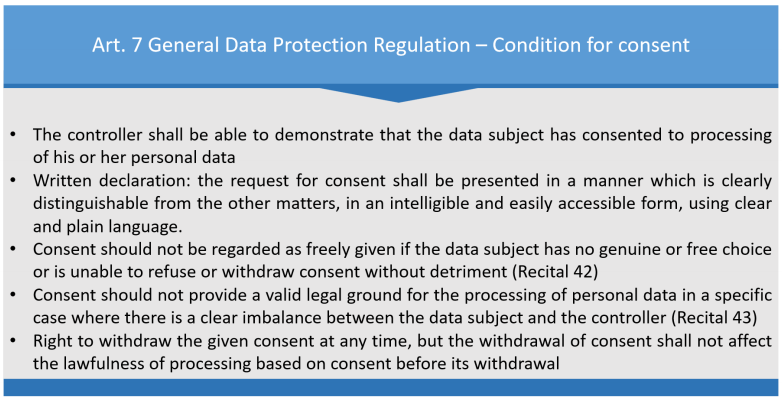
If the consent is given in the context of a written declaration, the request for consent shall be presented in a manner that is clearly distinguishable from the other matters. The safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given and permit to ensure unambiguity.

Consent has to be freely given. This will not be the case if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment (danno).

When talking about *clear imbalance*, the imbalance is likely in a specific situation where the controller is a public authority. This though is to be identified on a case-by-case basis.

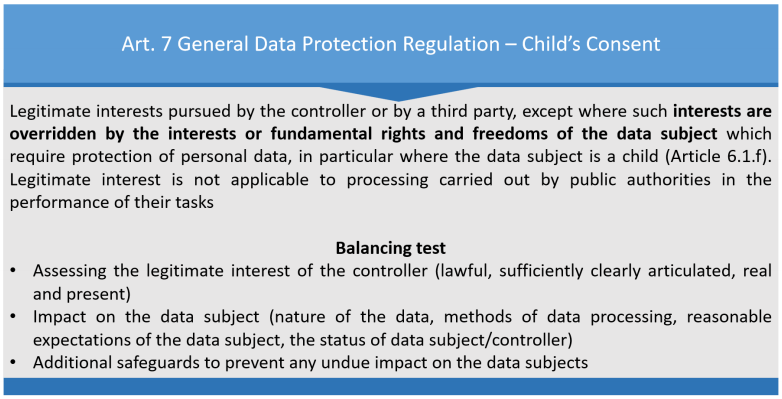
According to Art. 4 Sec. 11 GDPR, consent requires a specific and informed affirmation by the data subject of the processing of its personal data. Thus, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data is intended. When the processing has multiple purposes, consent must be obtained for all of them.

Legal Grounds



Art. 7 Sec. 3 GDPR explicitly provides for the data subject's right to withdraw its consent at any time but it does not affect the lawfulness of processing based on consent before its withdrawal.

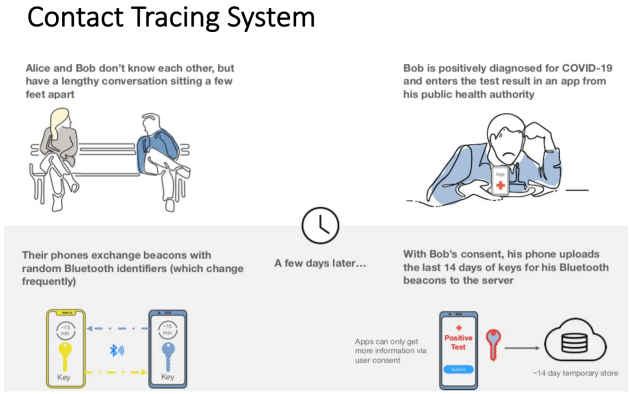
Legitimate interest

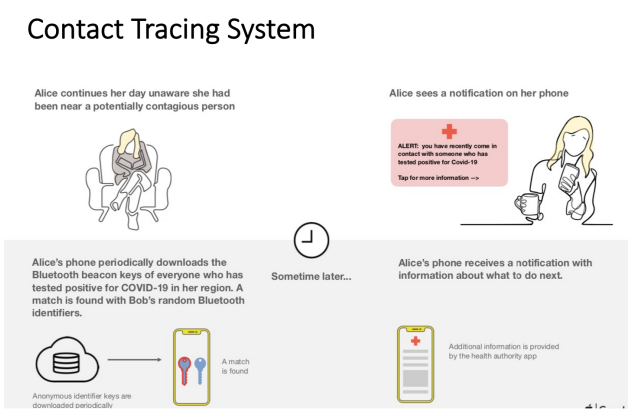


As children merit specific protection. Art. 8 GDPR introduces special conditions applicable to a child's consent in relation to information society services. For children under age 16, processing shall only be lawful if and to the extent that consent is given or authorised by the holder of parental responsibility, Art. 8 Sec. 1 phrase 2 GDPR. However EU Member State legislation may provide for a lower age for those purposes provided that it is not below 13 years old. Pursuant to Art. 8 Sec. 2 GDPR, the controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility, but it remains unclear what efforts are to be considered reasonable. Thus, Supervisory Authorities and courts will adopt a case-by-vase approach.

IMMUNI CASE STUDY

The **data subjects** where the citizen who have installed, on voluntary basis, the Immuni App. The purpose of the app was to alert people who have come into close contact with subjects tested positive, to formulate some statistics and was used for scientific research. It relied on consent and public health emergency in order to have a legal ground. The **Data Controller** role was assumed by the Ministry of Health. The storage lasted for the period strictly necessary whose duration was established by the Ministry of Health. All data would have been deleted at the end of the state of emergency and in any case no later than December 31, 2020.





DATA PROTECTION OFFICER

Art. 37 GDPR lays down in which cases the obligation to designate a DPO applies. The obligation to designate a DPO under Art. 37 GDPR is connected to the nature of the data processing activity and not to quantitive characteristics of the controller/processor itself.

According to Art. 37 Sec. 1 lits. b, c GDPR, *private entities* are obliged to designate a DPO in any case (public entities are also obliged to designate a DPO with some exceptions such as courts and independent judicial authorities) where the following is present:

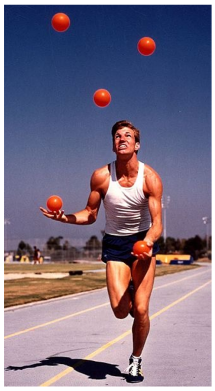
- *regular and systematic monitoring*: the core activities consist of processing that requires the regular and systematic monitoring of data subjects on a large scale.
- *special categories of personal data*: the core activities consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

The GDPR does not specify the notions of 'core activity' or 'on a large scale'. Art. 37 Sec. 4 GDPR allows entities to voluntarily appoint a DPO if they are not required to do so under Art. 37 Sec. 1 GDPR. Private entities should evaluate wheter they want to make use of this option given their economic situation and their data processing activities. If entities want to avoid that the voluntary DPO has to fulfil all obligations under the GDPR, they should not denominate this position DPO but, e.g., 'contact person'.

The professional qualities of the DPO are:

- Expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR.
- Understanding of the processing operations carried out.

Data Protection Officer



Art. 37 - GDPR

Designation of the data protection officer (internal or external)

Mandatory for

- Public authorities or bodies (a single data protection officer may be designated for several authorities/bodies)
- DC/DP whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale
- DC/DP whose core activities consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences

- Understanding of information technologies and data security.
- Knowledge of the business sector and the organisation.
- Ability to promote a data protection culture within the organization.

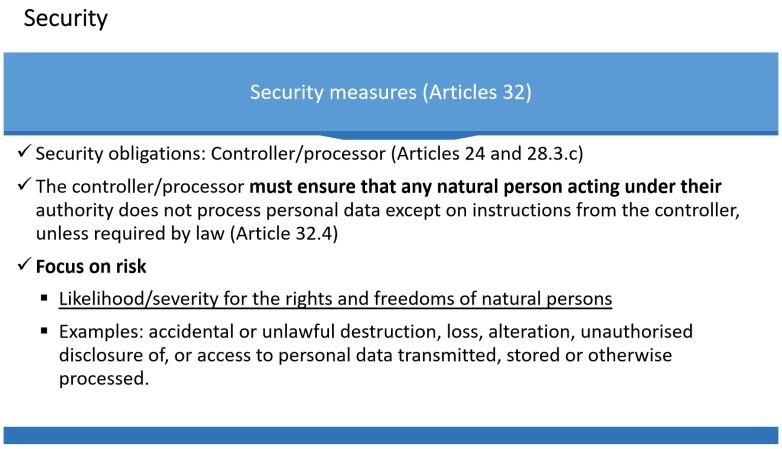
The data protection officer have some privileges of independence:

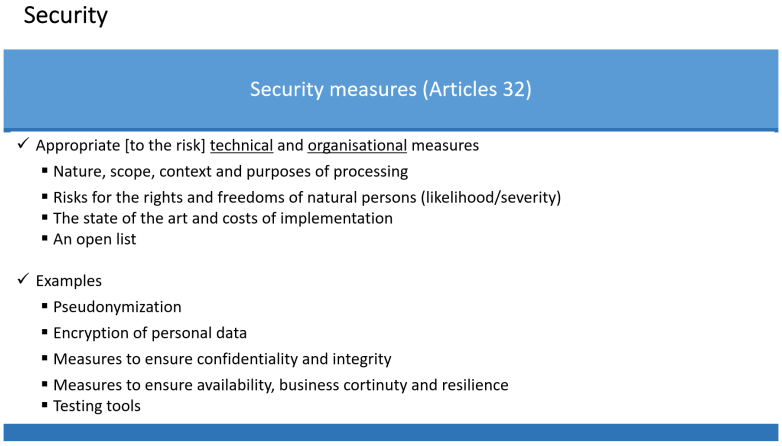
- Providing resources necessary to carry out DPO's tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
- No instructions by the controllers or the processors regarding the exercise of the DPO's tasks.
- No dismissal or penalty by the controller for the performance of the DPO's tasks.
- No conflict of interest with possible other tasks and duties.
- DPOs are not personal responsible for non-compliance with data protection requirements.

SECURITY MEASURES

Technical and organisational measures shall guarantee the safeguard of personal data. Art. 32 GDPR obliges the controller and the processor to undertake such measures. Whereas data protection through technology shall enforce data security in advantage of the processing, technical and organisational measures must be taken throughout processing.

Article 32 GDPR does not limit the scope of appropriate measures. Based on this open definition, a large vairety of measures is available, for example minimising the processing of personal data, pseudonymisation (as soon as possible), enabling the data subject to monitor the data processing, creating and improving security features, regular training of employees on data security, encoded data transfer, regular controls of the data security level and so forth.





Technical and organisational measures shall guarantee the safeguard of personal data. Art. 32 GDPR obliges the controller and the processor to undertake such measures.

Art. 32 sec. 1 GDPR sets out minimum requirements for the level of data security such as pseudonymisation and encription, ability to ensure ongoing confidentiality, integrity, availability and resilience of processing, ability to restore personal data in a timely manner in case of a physical/technical incident and process for regularly testing, assessing and evaluating effectiveness of technical and organizational measures.

Technical measures for security are (2021 ENISA - European Union Agency for Cybersecurity - report):

1. *Cybersecurity culture*: In order to develop it, it is necessary to: (i) appoint an internal professional specifically dedicated to the function, (ii) raise employee awareness, (iii) conduct audits (valutazioni), and (iv) publish cybersecurity policies.

2. *Training courses*: According to ENISA, they should have 2 main features: (i) they should be customized, with reference to content, for small and medium-sized enterprises and their reality, and (iii) they should be focused on real situations.

3. *Relations with third parties and cybersecurity*: There are third parties who are able to access company data in different ways. They are involved in the cybersecurity path/chain too, since vulnerability in their IT system may endanger the holding company's data.

4. *Data breach procedure*: It is necessary to develop a formal plan for response and reaction to incidents providing clear guidelines, precise identification of roles and responsibilities and, most importantly, documented.

5. *Security access to IT systems*: When authenticating, ENSA encourages: (i) to use a passphrase, and (ii) to avoid reusing passwords

6. *Device Safety*: It can be achieved through: (i) encryption, (ii) keeping devices constantly updated, (iii) being able to remotely erase data.

7. *Corporate network security*: Through the implementation of a firewall and constant review of all those solutions that allow remote access to the corporate network.

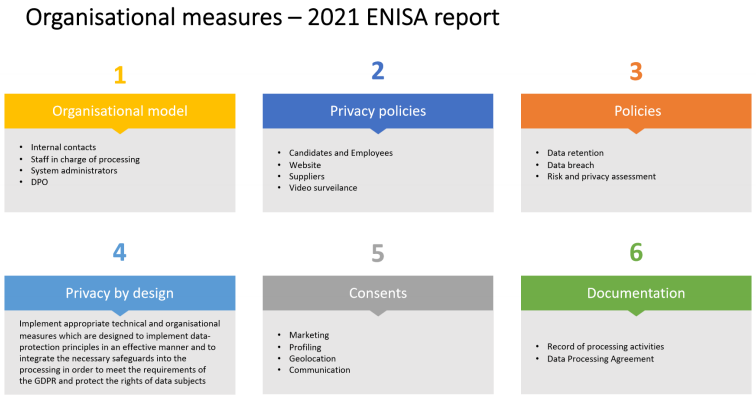
8. *Physical corporate security*: Proper behavior: (i) devices should never be left in the back seat or trunk of a car, (ii) computers should be locked or carried always with you, (iii) do not use suspicious USB drives, and (iv) enable automatic device lock, (etc.).

9. *Backup Security*: Backup must be: (i) done on a regular basis and automatic, (ii) immediately usable, (iii) separate from IT systems.

10. *Cloud*: Assess: (i) how the cloud itself is backed up, (ii) how authentication tools and steps are set up (i.e. the presence of any contractual constraints), (iii) the existence of disaster response or mitigation plans, (iv) the reliability and reputation of the vendor, etc.

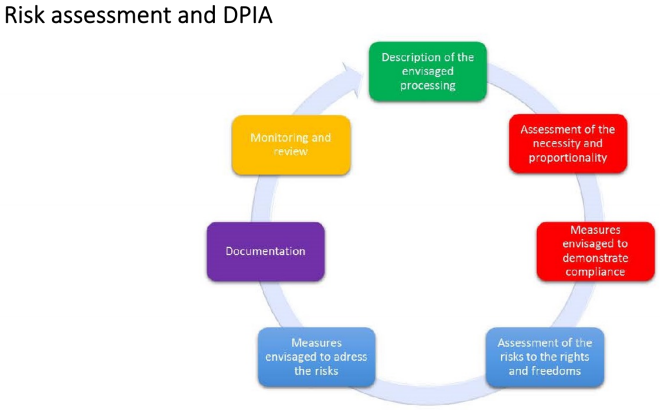
11. *Websites Security*: Carry out security tests on regular basis, simulating attacks in order to identify, for example, any potential weakness or insecurities, and perform ongoing checks on the update status of those sites.

12. *Search and share information*: Sharing as much information as possible is proven to be an effective tool to fight cybercrime, especially if the information that is shared pertains to exactly that area of business that we are interested in.



When assessing the measures for mitigating security risks, the controller should include safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation. Doing so, the controller needs to take into account the rights and legitimate interests of the data subjects and other persons concerned.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)



If a type of data processing is likely to result in a high risk to the rights and freedoms of individuals taking into account the nature, scope, context and purposes of the processing, the controller shall carry out an assessment on the impact of the envisaged (previsto) processing activities on the protection of personal data, Art. 35 Sec. 1 GDPR. It is a preventive data protection instrument.

The assesment is carried out in 2 steps:

1. the controller carries out the internal assessment; and
2. upon identification of a high risk, the Supervisory Authority potentially needs to be consulted.

In accordance with the general risk-based approach of the GDPR, the controller needs to make a prognosis on the impacts of its future data processing activities if it identifies the likeliness of a high risk.

The use of new technologies requires a careful assessment of the risk and impacts. The same goes for new kinds of processing operations and operations where no DPIA has been carried out before by the controller.

If designated, the controller shall seek the advice of the Data Protection Officer when carrying out the Data Protection Impact Assessment, Art. 35 Sec. 2 GDPR.

Art. 35 Sec. 10 GDPR provides for an exemption from the duty to perform a DPIA.

The Supervisory Authorities play a key role in the DPIA as they give advice to the controller on a case-by-case basis, as well as through general measures. According to Art. 35 Secs. 4, 5 GDPR,

each national Supervisory Authority shall issue so-called "black- and whitelists" which list the kinds of processing activities that do or do not require a DPIA. Thus, it will be the Supervisory Authorities' duty to specify what activities are deemed high risk. The adoption of a whitelist is mandatory while the blacklist is not.

DATA BREACH

According to Art.4 No. 12 GDPR, a personal data breach is 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. A personal data breach can occur by way of a technical or physical incident. The data concerned needs to be personal and has to be transmitted, stored or otherwise processed before the occurrence of the incident.

The Data Breach are classified in:

- *Confidentiality Breach* when there is accidental or abusive access to personal data. Even the simple loss of a business cell phone can be a valid reason for a data breach if it contains personal data and has not been properly encrypted.
- *Availability Breach* when there is an accidental or unauthorized loss or destruction of personal data. A potential example is when personal data is accidentally sent to an unauthorized third party or when a device is infected by ransomware.
- *Integrity Breach* when there is an accidental or unauthorized alteration of personal data. An example is if I change a file and I'm not authorized to do so.

In case of a personal data breach, the controller shall notify the competent Supervisory Authority without undue delay and, if possible, not later than 72 h after becoming aware of the data breach, Art. 33 Sec. 1 GDPR. The processor does not have an obligation to notify data breaches to the Supervisory Authorities but only to the controller. Nevertheless, the processor must inform the controller without undue delay of the data breach. It is not specified by law whether awareness of the processor will be attributed to the controller. If so, the notification period would start with the processors' awareness irrespective of when the controller becomes aware of the data breach.

Article 33 Sec. 3 GDPR sets out minimum requirements for the content of the notification. It must contain the following:

- the nature of the personal data breach (if possible, categories and approximate number of data subject and data records concerned);
- the name and contact details of the Data Protection Officer/other contact point;
- the likely consequences of the data breach;
- the measures (proposed to be) taken to address the data breach.

When identifying the likeliness of a high risk of the data breach to the rights and freedoms of individuals, the controller shall communicate the personal data breach to the involved data subjects without undue delay. The notification shall allow the data subjects to take the necessary precautions and should describe to them the nature of the personal data breach, as well as recommendations for the data subjects to mitigate potential adverse effects.

According to Art.34 Sec. 3 GDPR, a communication is not required if one of the following conditions is met:

- the controller has implemented appropriate technical and organizational measures, and they were applied to the affected personal data; or
- the controller has taken subsequent measures to ensure that the high risk to the rights and freedoms is no longer likely to materialise; or
- the communication would involve disproportionate effort (there shall instead be a public communication or similar information measure)

In addition to these aspects, the Data Controller should also justify the reason for the decisions taken as a result of the data breach with particular reference to the following cases:

- the Owner decided not to proceed with the notification;
- the Data Controller has delayed the notification procedure;
- the Data Controller has decided not to notify the data breach to the Data subject.

Art. 33 Sec. 5 GDPR asserts that the controller shall document any personal data breach, including the circumstances surrounding it, its consequences and the measures taken to remedy it. Such documentation shall enable the Supervisory Authority to verify compliance with this Article. In particular, there are 2 tools to use:

- Incident log - concise, but comprehensive and update in a timely manner
- Internal reports - with standard and easily accessible templates, approved, updated as action plans evolve with detailed risk assessment and documentation of decisions made within the organization.

NOTE

https://gdpr-info.eu/