- Definitions
- Nature and implementation
- Territorial scope
- Principles
- Legitimate grounds

- GRPR – To do list
- GDPR Compliance
- GDPR Subjects Relations
- GDPR – 4 Pillars
- GDPR Penalties & Fines
- Question & Answers

The origins of privacy

Warren and **Brandeis**, in their iconic article ”**The right to Privacy**”, published on the Harvard Law Review, for the first time investigate the existence of «*a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds*», and more in general, a **«right to be let alone»**.

Right to privacy

Art. 12 (Universal Declaration of Human Rights)

1. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Right to privacy

Art. 8 (European Convention on Human Rights)

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Right to protection of personal data

Art. 8 (Charter of Fundamental Rights of the European Union)

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.

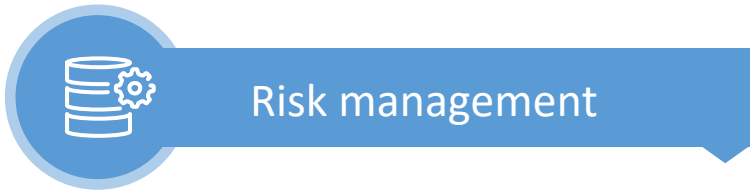
Possible limitations

Art. 52 (Charter of Fundamental Rights of the European Union)

1. **Any limitation** on the exercise of the rights and freedoms recognized by this Charter **must be provided for by law** and **respect the essence of those rights and freedoms**. Subject to the **principle of proportionality**, **limitations** may be made **only if they are necessary and genuinely meet objectives of general interest** recognised by the Union **or the need to protect the rights and freedoms of others**.

[…].

The main pillars of the European approach



Balancing of Interest

Careful! ECtHR is not part of the EU!

Balancing of Right

The role of the
European courts
(ECJ/CJEU and ECtHR)

CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2014

Mr Costeja Gonzalez lodged with the Spanish Data Protection Authority a complaint against La Vanguardia, which publishes a daily newspaper with a large circulation, and against Google Spain and Google Inc.

The complaint was based on the fact that, when an internet user entered Mr Costeja name in the Google search engine, he would obtain links to two pages of La Vanguardia, of 19 January and 9 March 1998 respectively, on which an announcement mentioning his name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

Balancing of Interest

Costeja Gonzalez requested:

LA VANGUARDIA

to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data.

Google

to remove the personal data relating to him. He stated in this context that the attachment proceedings concerning him had been **fully resolved** for a number of years, and that reference to them was now **entirely irrelevant**.

Balancing of Interest

By decision of 30 July 2010, the Spanish Data Protection Authority **rejected the complaint in so far as it related to La Vanguardia**, taking the view that the publication by it of the information in question was legally justified and was intended to give maximum publicity to the auction in order to secure as many bidders as possible.

On the other hand, **the complaint was upheld in so far as it was directed against Google Spain** and Google Inc. The Authority considered that operators of **search engines are subject to data protection legislation given that they carry out data processing for which they are responsible** and act as intermediaries in the information society.

Balancing of Interest

Court of Justice

«As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, **those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name**.

However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question»

Balancing of Interest

ECtHR, ***Mosley v. the United Kingdom****, No. 48009/08, 2011*

A British national weekly newspaper, *News of the World*, published a front page article about **Max Mosley**, a well-known figure in the International Automobile Federation and Formula One, reporting his alleged “Nazi” sexual activities and including intimate photographs, taken from secretly recorded video.

The Court recognizes that the private life of celebrities have become a lucrative commodity for certain sectors of the media. The publication of news about such persons contributes to the variety of information available to the public and, although generally for the purposes of entertaining rather than education, it benefits from the protection of **freedom of expression**.

However, such protection **may cede to** the requirements of the **right to privacy, where the information at state is of a private and intimate nature and there is no public interest in its dissemination**.

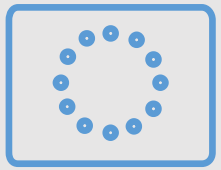
GDPR Definition

GDPR

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the **collection and processing of personal information from individuals** who live in the European Union (EU)

What?

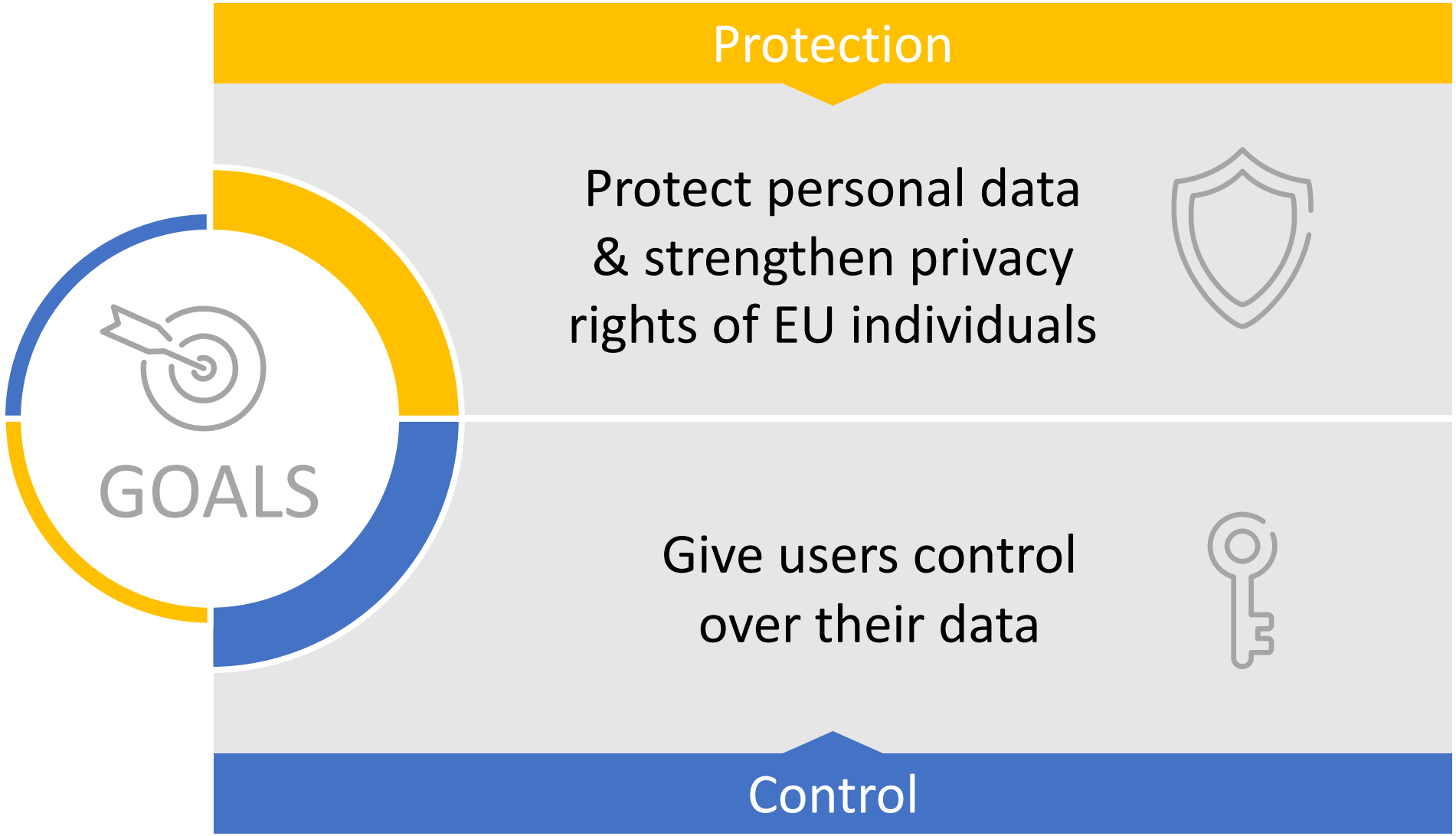
The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy



When?

Starting:
May 25, 2018

Goals of EU's General Data Protection Regulation



Goals of EU's General Data Protection Regulation

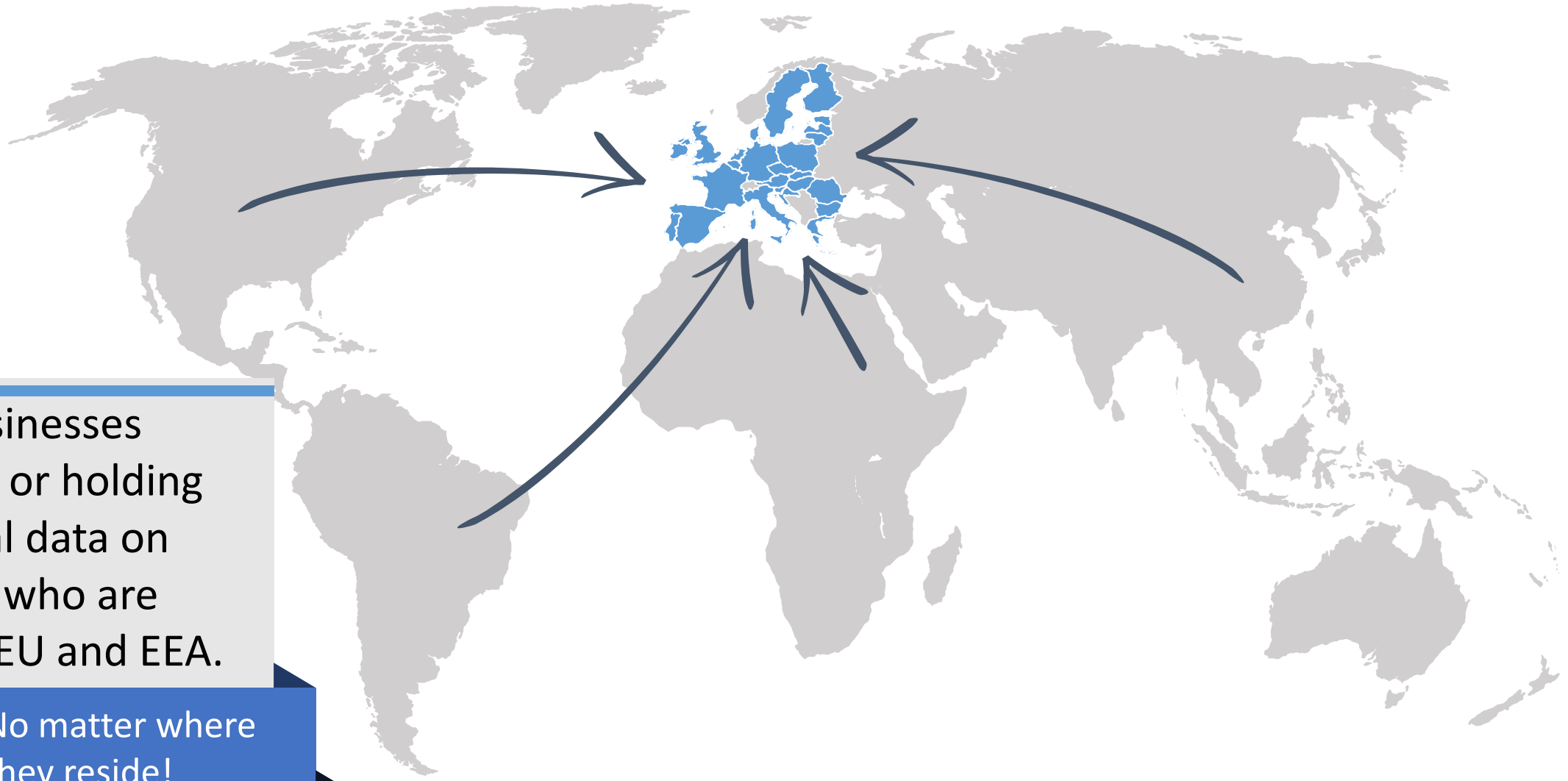
Art. 1 General Data Protection Regulation

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.

Who is affected by GDPR?

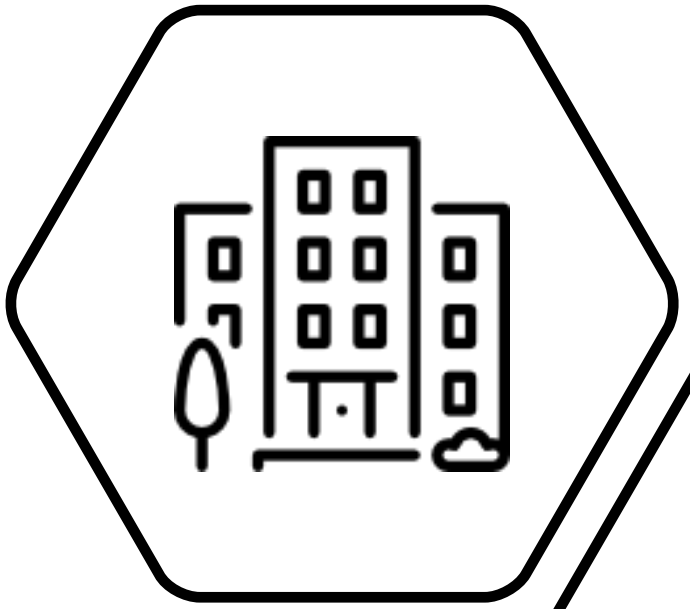


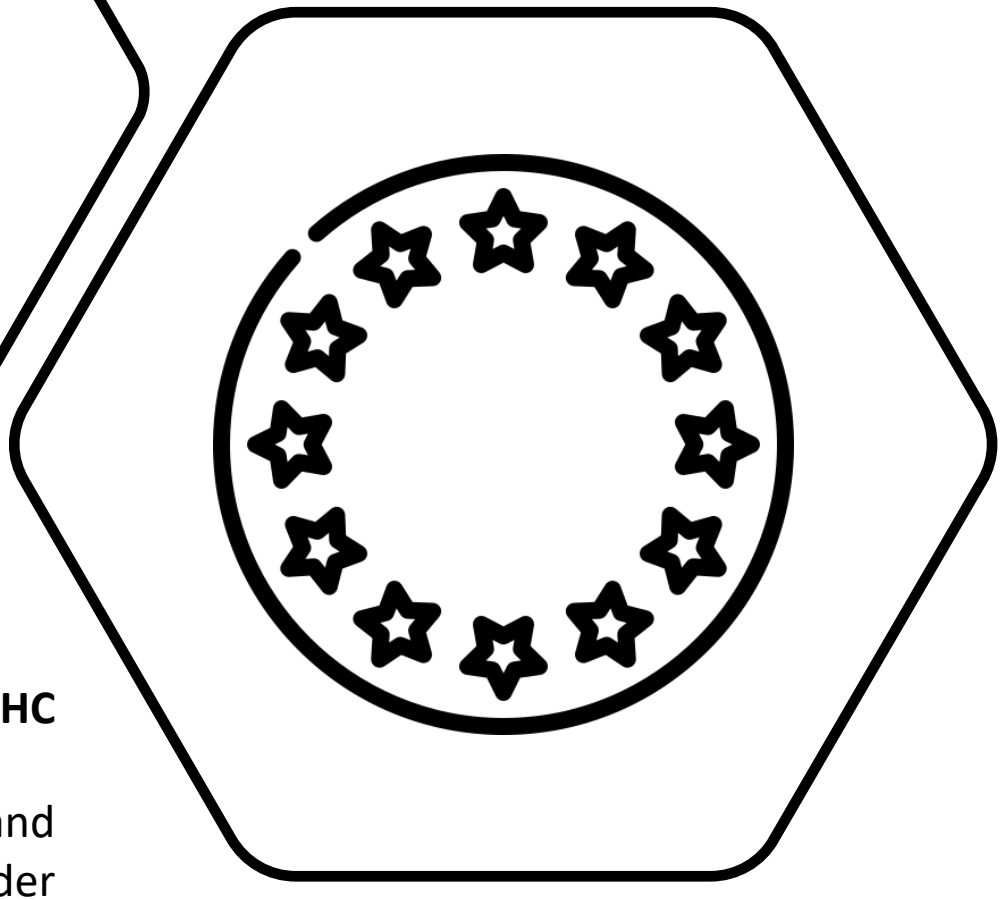
All businesses collecting or holding personal data on people who are located in EU and EEA.

No matter where they reside!

Nor their citizenship

Territorial Scope





Companies that are not established in the Union but are subject to the GDPR shall **designate a representative** in the Union (Article 27 GDPR).

UK- Sanso Rondon v LexisNexis Risk Solutions UK Ltd (2021) EWHC 1427 (QB):

The High Court of England and Wales held that controllers and processors outside of the EU that nominate a representative under Article 27 GDPR do not outsource liability for breaches of the GDPR. A representative can only be held responsible for its own obligations.

Territorial Scope

Art. 3 General Data Protection Regulation

(1) 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**.

C-131/12 - Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, paragraph 55

*"the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that **has its seat in a third State but has an establishment in a Member State**, is carried out '**in the context of the activities**' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable"*

Territorial Scope

Art. 3 General Data Protection Regulation

(2) This Regulation applies to the processing of personal data of **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.

Personal Data Definition

Personal Data

Personal data is any information relating to an identified or identifiable natural person

Article 4 GDPR - *Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is 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 physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*

Personal Data Definition

Personal Identifiable Information

… which is different from PII (Personal Identifiable Information):

According to US legislation - *limited scope, e.g. name, address, birth date, Social Security numbers, banking information, ZIP Code, etc.*

According to ISO standards - *any piece of information that confirms an individual's identity.*

Types of Personal Data

Personal Data

- Name
- Address
- Phone
- Bank / Credit cards
- Email address
- IP address
- Cookies
- Online identifiers
- …

special categories of Data

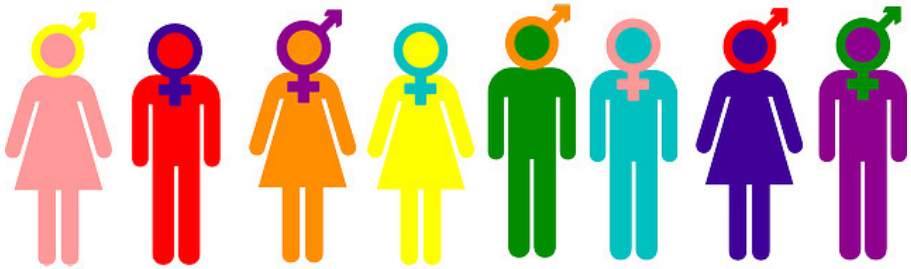
- Biometric data
- Genetic data
- Health data
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership,

Personal Data Definition: sexual orientation

Personal Data

C-184/20 – OT v Vyriausioji tarnybinės etikos komisija (Chief Official Ethics Commission)*: personal data is "not only of inherently sensitive data, but also of data revealing information of that nature indirectly, following an intellectual operation involving deduction or cross-referencing". Therefore, "the publication of personal data that are liable to disclose indirectly the* ***sexual orientation of a natural person constitutes processing of special categories of personal data****".*

Lithuanian case concerning national anti-corruption legislation. A person subject to this legislation was obliged to make a "declaration of private interests" to the Lithuanian administrative authorities, including information about his acquaintances and relatives for the purpose of identifying potential conflicts of interest.



Personal Data Definition: IP Address

Personal Data

ART29WP: "without even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer requires the disclosure of his or her identity in the narrow sense". WP 4/2007,155".

C-70/10 - Scarlet Extended v SABAM

«*It is common ground, first, that the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content and the collection and identification of users' **IP addresses** from which unlawful content on the network is sent. **Those addresses are protected personal data because they allow those users to be precisely identified**.*»

Personal Data Definition: a broad definition

Personal Data

C-582/14 Breyer v Bundesrepublik Deutschland

«It *must be determined whether the possibility to* ***combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject***.

it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored.»

Personal Data Definition: a broad definition

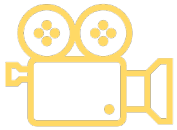
Personal Data

- ✓ Facial recognition systems
- ✓ Smart devices (voice, temperature, energy consumption, etc.)
- ✓ Smart cities
- ✓ Broad notion and new technologies (e.g. wi-fi spectrum)

GDPR, Recital 26

"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 whether means are reasonably 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."

Personal Data Definition: a common case



Personal Data

C-212/13 František Ryneš v Úřad pro ochranu osobních údajů (Office for personal data protection)

Mr. Rynes installed a **camera system** on his family home **which recorded** the entrance to his home, the **public foot path and the entrance to the house opposite his home**. The dispute in question is **whether the operation of a home camera system which** records people for purpose of protecting the property but **monitors a public space amounts to processing of personal data**.

The Court held that **the image of a person recorded by a camera system constitutes personal data, in as much as its possible to identify a person**.

Personal Data Definition: non-personal data

Personal Data

✓ Non-personal data

Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the EU; "data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679"

✓ Anonymous data

GDPR Recital 26

"The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable"

Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques

Personal Data Definition: non-personal data

Personal Data

No EU prescriptive technical standards for anonymisation

Contextual analysis:

- ✓ Anonymous information / anonymised data (legal basis for data processing)
- ✓ Reasonableness (all the means reasonably likely to be used)
  - Costs
  - Amount of time required for identification
  - Technology available at the time of the processing
  - Technological development
- ✓ Assessment of the risk of re-identification

Encrypted data / anonymous data

Aggregate data

Main Principles

Lawfulness, Fairness and Transparency

Personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject

Purpose limitation

Personal data should be collected for specified, explicit and legitimate purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, not be considered to be incompatible with the initial purposes

Data minimisation

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Accuracy

Personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

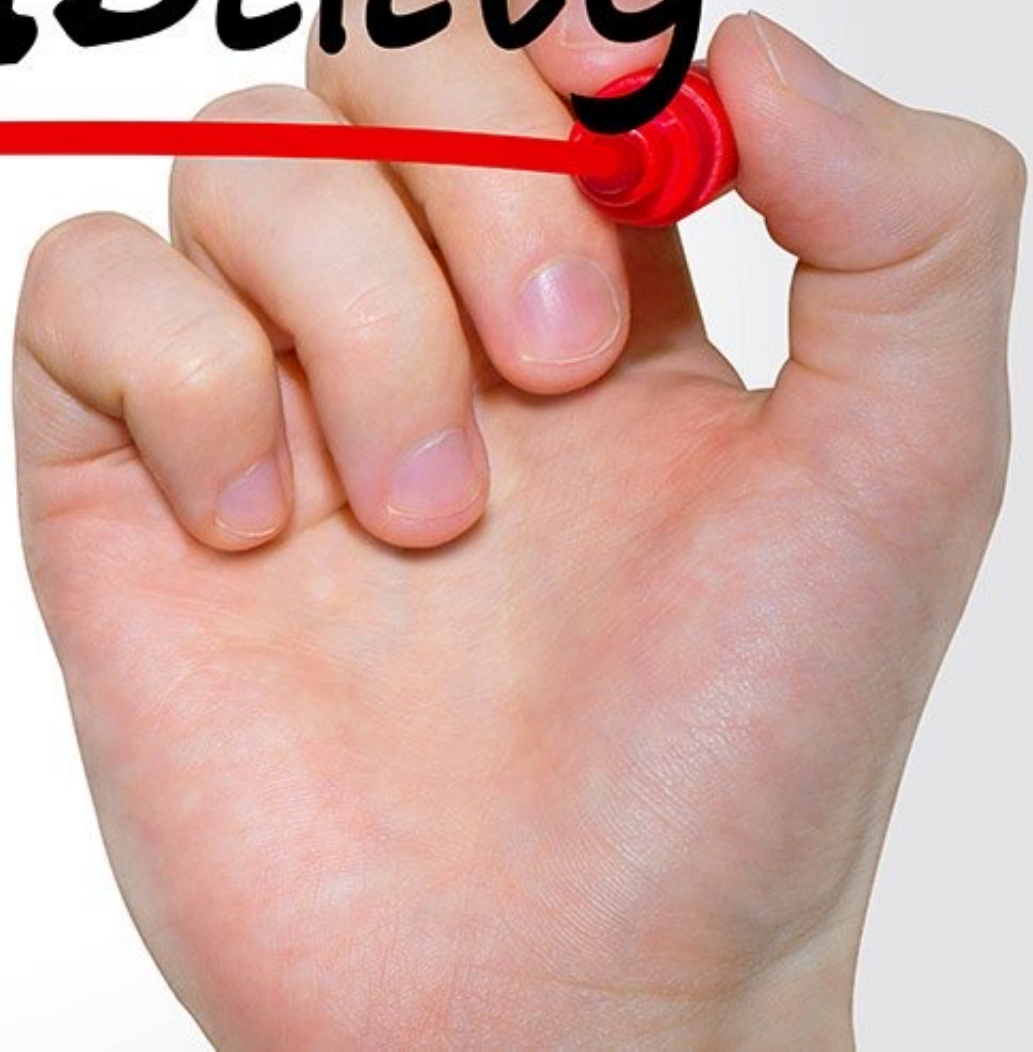
Storage limitation

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed and may be stored for longer periods solely for archiving purposes in the public interest, scientific or historical or statistical purposes

Integrity and confidentiality

Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Accountability



The controller shall be responsible for and be able to demonstrate compliance with the above principles

Data Processing

Data Processing

Data processing

*"(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise makin*g available, alignment or combination, restriction, erasure or destruction"

Data processing regarding a **purely** personal or household activity carried out by private individuals does not fall under the GDPR.

However, the so-called «household exemption» is interpreted narrowly.

Household activity

CJEU, C-101/01, Case Bodil Lindqvist

- Mrs Lindqvist worked as a catechist in Sweden. She followed a data processing course on which she had to set up an internet web page. So, she created an internet pages at home, on her PC, in order to give useful information to church goers.
- This web page included personal information about her catechist colleagues, who were not aware (and did not appreciate).
- She was **criminally accused for illegal processing of personal data**.
- She claimed that the household exception applied.
- The CJUE excluded the exception, stating it relates **only to activities carried out in the course of private or family life**, and never through publication of data on the internet so that are made accessible to an indefinite number of people.

Household activity

CJEU, C-101/01, Case Bodil Lindqvist

«The act of ***referring, on an internet page, to various persons and identifying them by name or by other means****, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46/EC.*

Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46*»*

Household activity

CJEU, C-345/17, "Buivids" Case

Mr Buivids taped police officers, at a police station, and uploaded the video on Youtube.

The Latvian DPA ordered to remove the video because he had infringed data protection law. He appealed up to the Latvian Supreme Court which referred the following core question to the CJEU: Does data protection law apply in this case? Was it household activity or not?

The CJEU stated that Mr Buivids's activity was not "household activity" – hence no household exemption applicable – since the video was uploaded on the internet.

GPDR - 4 Pillars

Records of processing activities

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility

Data Processors

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures

DPIA

Where a type of 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 processing operations on the protection of personal data

Data Breach

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

GDPR - Personal Data Processing Activities

Lawfulness of Data processing

Processing shall be lawful only if and to the extent that at least one of the following applies:

- The consent of the individual concerned
- A contractual obligation between you and the individual.
- To satisfy a legal obligation.
- To protect the vital interests of the individual.
- To carry out a task that is in the public interest.
- For your company's legitimate interests, but only after having checked that the fundamental rights and freedoms of the individual

Personal data relating criminal convictions

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when

- the processing is authorized by Union or
- Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Processing of special categories of personal data

Processing of special categories of data shall be lawful only if one of the following applies:

- The consent of the individual concerned
- Processing is necessary for social security and social protection law
- Processing is necessary to protect the vital interests of the data subject
- Processing carried out in the course of its activities by a foundation, association or any other not-for-profit body
- Personal data which are manifestly made public by the data subject
- Processing is necessary for the exercise or defence of legal claims
- Pprocessing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine

Legal Grounds

Art. 7 General Data Protection Regulation – Condition for consent

- The controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data
- Written declaration: the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
- Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment (Recital 42)
- Consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller (Recital 43)
- Right to withdraw the given consent at any time, but the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal

la Repubblica

I ricavi ottenuti dalla pubblicità personalizzata ci aiutano a supportare il lavoro della nostra redazione che si impegna a fornirti ogni giorno una informazione di qualità. Per questo chiediamo il tuo consenso all'utilizzo di cookie o tecnologie simili per finalità diverse da quelle strettamente necessarie, come specificato nella Cookie Policy.
Sei libero di rifiutare in qualsiasi momento, ma in tal caso ti chiederemo di acquistare uno dei nostri abbonamenti.

ACCETTA

RIFIUTA E ABBONATI

Sei già abbonato? ACCEDI

Cliccando autorizzi l'utilizzo di tutti i cookie di profilazione indicati nella Cookie Policy e potrai navigare sul nostro sito, con accesso ai titoli degli articoli pubblicati, al contenuto degli articoli non Premium e ai video.
Se accetti l'uso di tutti i cookie di profilazione, noi e terze parti selezionate potremo archiviare e/o accedere a informazioni sul tuo dispositivo e trattare i tuoi dati personali - incluse la geolocalizzazione e l'identificazione attraverso la scansione del dispositivo - per finalità di profilazione attraverso le seguenti attività: annunci e contenuti personalizzati, valutazione degli annunci e del contenuto, ricerche di mercato e sviluppo di prodotti.
Accedendo al pannello delle preferenze pubblicitarie, potrai invece selezionare le singole finalità connesse con la profilazione. In caso di rifiuto di una o più finalità richieste per l'accesso ai nostri servizi senza abbonamento e contraddistinte mediante asterisco nella Cookie Policy, potrai fruire dei servizi solo acquistando uno dei nostri abbonamenti, incluso l'abbonamento Base che ti offre un servizio equivalente a quello ottenibile accettando i cookie di profilazione.

Consent

Newspapers and paywalls

In October 2022, several sites of the major Italian newspapers and magazines - those of the GEDI group (Repubblica, la Stampa, and several local dailies) have introduced a message, asking visitors who are not subscribers to **subscribe** or to **accept cookies** or other profiling technologies designed to offer them more personalised advertising in order to access all the pages of the site.

The Italian Data Protection Authority has opened an investigation into use of these paywalls.

Consent

Newspapers and paywalls

Note:

- a **cookie wall** is a mechanism that allows a user to access a website in only one way: by giving consent to all cookies. Cookie walls are prohibited. The EDPB: “In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user”.
- A **paywall** is a mechanism whereby the user is given an alternative to access content, such as a payment or subscription, instead of giving consent to cookies.

Are paywalls legitimate?

Consent

Newspapers and paywalls

It’s a matter of CONSENT.

Is consent, given as an alternative to the payment of a sum of money, really free?

The Austrian and French authorities have already stated that the cookie paywall system is a valid solution if the subscription proposed by the site has a moderate cost so as not to restrict the user's freedom.

The decision of the Italian Data Protection Authority on Paywalls, on the other hand, is still awaited.

Legal Grounds

Careful! It only applies to information society services!

Art. 8 General Data Protection Regulation – Child's Consent

16 years old, **but** **Member States may provide by law for a lower age** for those purposes provided that such lower age is **not below 13 years**. Reasonable efforts to verify by data controllers.

Legitimate interest

Art. 6(1), lett. f) GDPR – Legitimate Interest

Legitimate interests pursued by the controller or by a third party, except where such **interests are overridden by the interests or fundamental rights and freedoms of the data subject** which require protection of personal data, in particular where the data subject is a child (Article 6.1.f). Legitimate interest is not applicable to processing carried out by public authorities in the performance of their tasks

Balancing test

- Assessing the legitimate interest of the controller (lawful, sufficiently clearly articulated, real and present)
- Impact on the data subject (nature of the data, methods of data processing, reasonable expectations of the data subject, the status of data subject/controller)
- Additional safeguards to prevent any undue impact on the data subjects

Legitimate interest

Case Study

Claudia orders a pizza via a mobile app on her smartphone but does not opt-out of marketing on the website. Her address and credit card details are stored for the delivery. A few days later Claudia receives discount coupons for similar products [legitimate interest, impact] from the pizza chain in her letterbox at home [impact].

Brief analysis: the pizza chain has a legitimate, but not particularly compelling, interest in attempting to sell more of its products to its customers. On the other hand, there does not appear to be any significant intrusion into Claudia's privacy, or any other undue impact on her interests and rights. The data and the context are relatively innocent (consumption of pizza). The pizza chain established some safeguards: only relatively limited information is used (contact details) and the coupons are sent by traditional mail. In addition, an easy-to-use opportunity is provided to opt-out of marketing on the website [additional safeguards].

On balance, and considering also the safeguards and measures in place interests *the interests and rights of the data subject do not appear to override the legitimate interests of the pizza chain* to carry out this minimal amount of data processing.

Legitimate interest

Video Surveillance

Large application of the legitimate interest legal base:

- applicable in imminent danger situation, such as banks or shops selling precious goods (e.g. jewellers), or areas that are known to be typical crime scenes for property offences (e. g. petrol stations)

- Balancing the interests is still mandatory. The controller needs to consider: 1) to what extent the monitoring affects interests, fundamental rights and freedoms of individuals, and 2) if this causes violations or negative consequences with regard to the data subject's rights.

GDPR – Individual User Point of View

For individual must be ensured

- Getting consent to process personal data
- Right to be forgotten
- Right to modify personal data
- Transparency - right for get information
  what data are collected, how data are going to be used
  (where stored, who will have access)
- Can request data in portable format

GDPR – Individual's Rights

Right to Access

Information if personal data are processed, the purpose, what data types, the period of storage

Right to Rectification

Correction of inaccurate personal data concerning him, without any delay.

Right to Erasure

Right to be forgotten, to erase all personal data if no necessary anymore or if the users withdraws consent.

Right to Restriction of Processing

If the data accuracy is contested, unlawful or not need anymore

Right to Data Portability

To receive user's concerning personal data, in a structured format.

Right to Object

Stop processing of personal data on request, unless the controller demonstrates compelling reasons overriding the individual's interests and rights.

Right of access – art. 15 GDPR

CJEU C-154/21 – Österreichische Post

A data subject asked Österreichische Post (Austrian postal service company) for access to the personal data concerning him which were being stored or had previously been stored by said company and, if the data had been disclosed to third parties, for information as to the identity of the recipients.

Österreichische Post gave a generic response and did not disclose to RW the identity of the specific **recipients of the data**.

Right of access – art. 15 GDPR

CJEU C-154/21 – Österreichische Post

The CJEU declared that the data subject's right of access to the personal data entails an obligation on the controller to **provide the data subject with the actual identity of those recipients**, **unless**:

- it is **impossible** to identify the recipients, or
- the controller demonstrates that the data subject's requests for access are manifestly **unfounded or excessive**,

in which cases the controller may indicate to the data subject **only the categories** of recipient in question.

Right to erasure (“right to be forgotten”) – art. 17 GDPR

Italian DPA case no. 305/2022 – BPER Banca S.p.A.

On **12 January 2019**, a **data subject emailed BPER Banca** (data controller) **requesting to erase his professional profile**. Few days later, the Bank asked for the data subject’s ID to enable his identification. The data subject immediately sent the requested information. However, the Bank took no further action.

The data subject **submitted reminders both in April and in May 2019**.

Only on **17 June 2019** (**five months after the request!**), **the Bank confirmed the erasure**.

The **Italian DPA** concluded that **the controller's late and inadequate response** to the request for erasure submitted by the data subject **was unlawful and issued a 10,000 euros fine**.

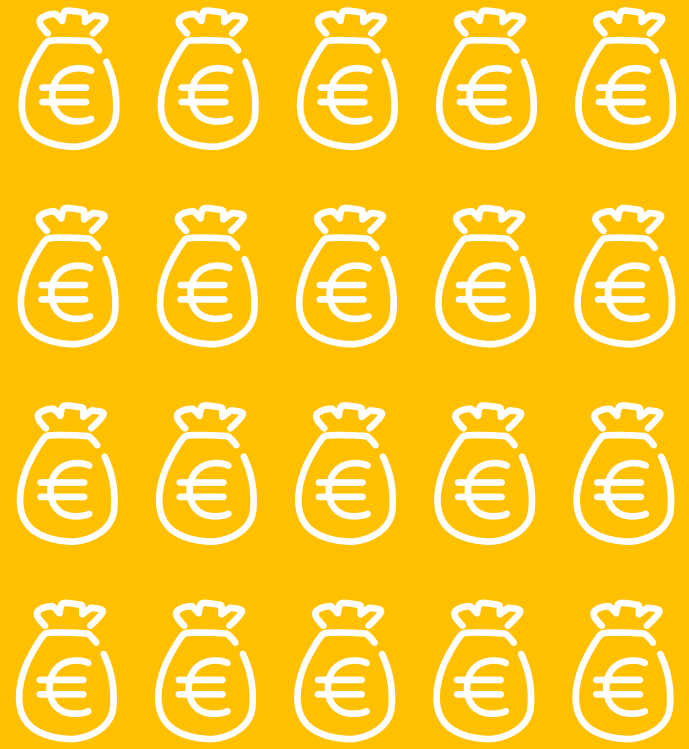
Data Protection Authority Judgement

GDPR FINES

Face a fine up to

20M € or 4%

global turnover



Caffeina Media: data transfers to the US

Injunction order against Caffeina
June 9, 2022

- **Object of the investigation**: a complaint alleging the company was sending data to Google LLC, in the US, without the safeguards required by Chapter V of the GDPR.
- **Alleged infringement**: the company was using on its websites Google Analytics, a tool allowing statistical analysis to optimise their services and monitor their marketing campaigns. While the data was officially transferred to Google Ireland, the Italian Authority held that the use of GA entailed the transfer of the personal data to the parent company Google LLC, based in the United States.

Caffeina Media: data transfers to the US

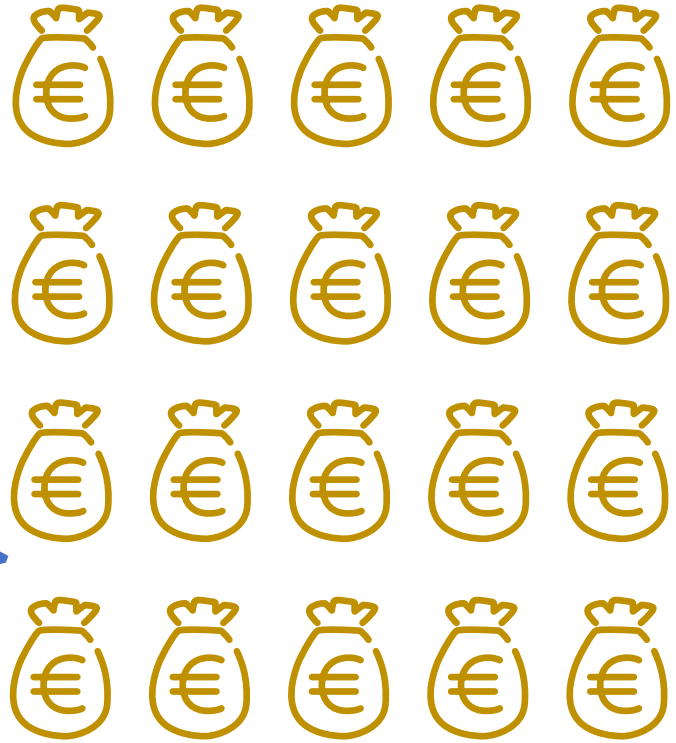
Injunction order against Caffeina
June 9, 2022

- In the absence of an adequacy decision with the US, such transfer is only possible if appropriate safeguards are adopted, which was not the case, according to the Authority.
- **Consequences:** the company was not fined immediately, but the decision had far-reaching consequences in the world of privacy compliance, causing all companies to re-evaluate their analytics tools and the data transfers of big tech companies to the US, even when there is a screen company in the EU.

OneDirect: inability to exercise rights

Injunction order against OneDirect
March 25, 2021

- **Object of the investigation**: two complaints alleging the receipt of promotional emails sent by the company, without consent and despite the opposition of the recipients expressed via email.
- **Alleged infringement**: the absence of clear indications on how to contact the company, the lack of adequate technical and organizational measures to enable the operation of the unsubscribe button to work and the monitoring of the email inbox, have made it impossible for complainants to exercise their rights.
- **Amount of penalty***: **30.000 euros**

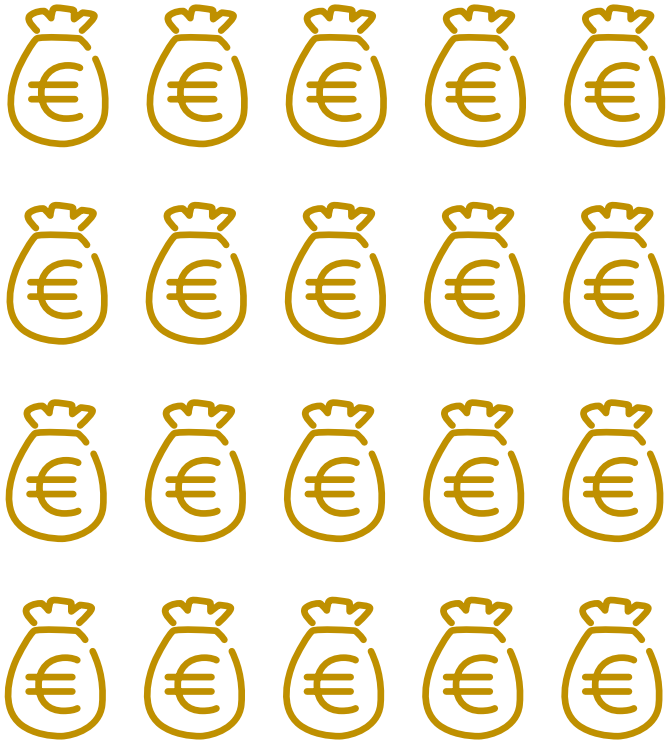


Vodafone: aggressive telemarketing

Financial penalty against Vodafone
November 16, 2020

- **Object of the investigation**: unlawful processing of personal data of millions of users for telemarketing purposes.
- **Alleged infringement**: (i) not only of the obligation to give consent, but also of the fundamental principles of accountability and implementation of privacy protections; (ii) the use of fictitious numbers or numbers not recorded in the Register of Communication Operators to make promotional contacts; (iii) management of name lists to be contacted acquired from external suppliers without the necessary free, informed and specific consent of users; (iv) inadequate security measures relating to customer management systems.

- **Amount of penalty**: **12.251.601 euros**

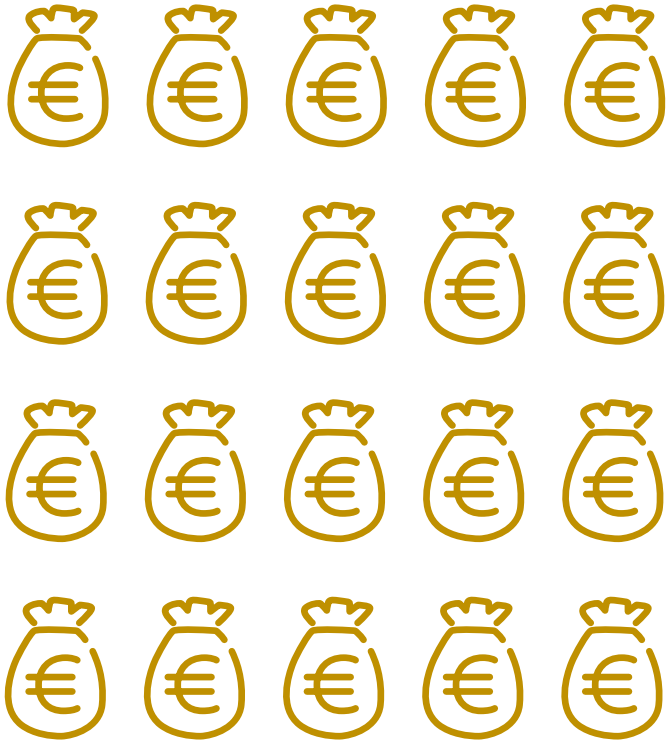


WindTre: overly aggressive marketing

Financial penalty against WindTre
July 13, 2020

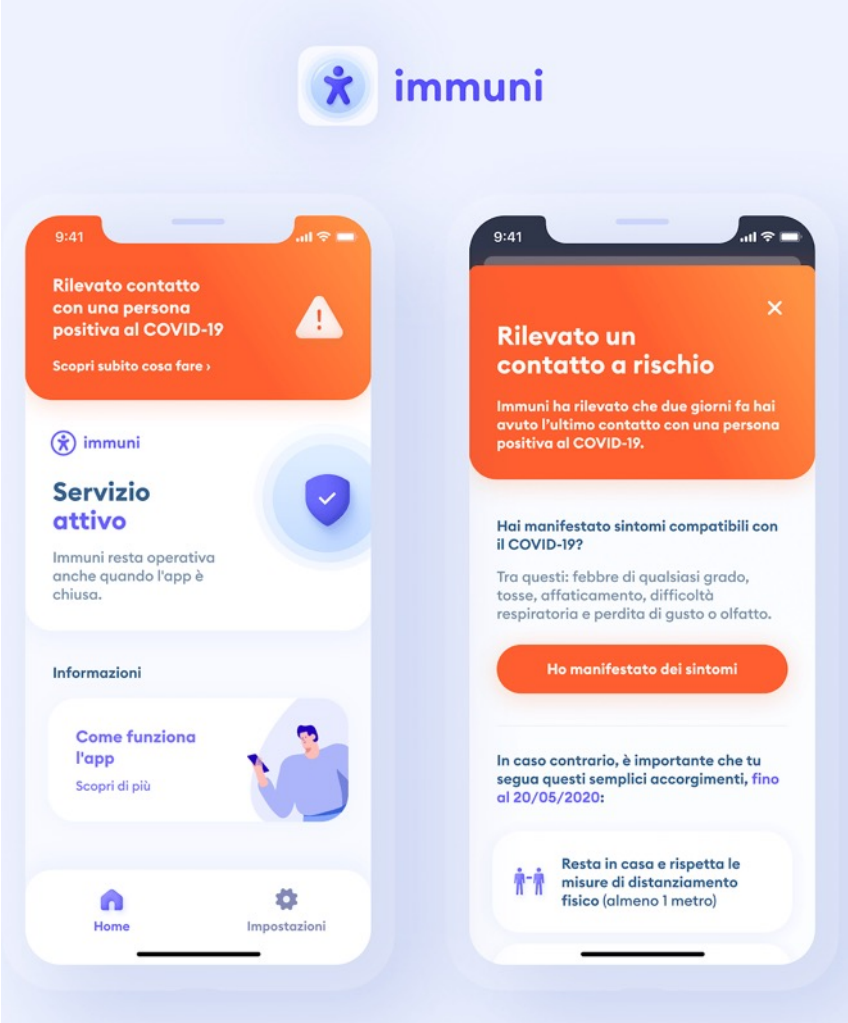
- **Object of the investigation**: a large number of unlawful treatments of its users personal data, mainly linked to promotional activities, such as the sending of unwanted advertisements, carried out without the users' consent (so-called "wild marketing").
- **Alleged infringement**: processing of users' personal data carried out without their consent and the non-adoption of appropriate technical and organizational measures for effective control of the partner supply chain and to respect users' wishes, as required by the GDPR.

- **Amount of penalty**: **17 million euros**



Case Study: Immuni

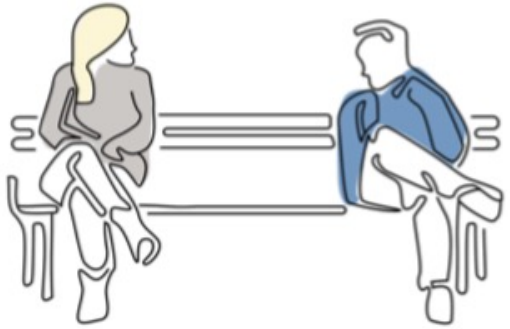
Legislative decree 28/2020 – Article 6



- **SUBJECT:** Single national platform for the management of the alert system of subjects who have installed, on a voluntary basis, a specific app
- **PURPOSE:** Public health purposes (alerting people who have come into close contact with subjects tested positive), statistical purposes and scientific research
- **LEGAL BASIS**: Public health and … consent
- **DATA CONTROLLER:** Ministry of Health
- **PROCESSED DATA:** Proximity data of the devices, made anonymous or, where this is not possible, pseudonymized**.**
- **STORAGE:** For the period strictly necessary whose duration will be established by the Ministry of Health. In any case, all data will be deleted at the end of the state of emergency and in any case no later than December 31, 2020.

Contact Tracing System

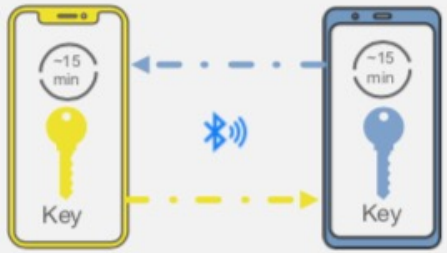
Alice and Bob don't know each other, but have a lengthy conversation sitting a few feet apart



Bob is positively diagnosed for COVID-19 and enters the test result in an app from his public health authority

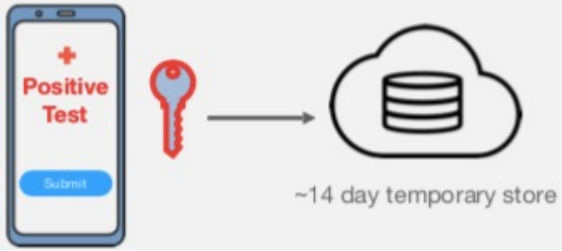
A few days later...

Their phones exchange beacons with random Bluetooth identifiers (which change frequently)



With Bob's consent, his phone uploads the last 14 days of keys for his Bluetooth beacons to the server

Apps can only get more information via user consent



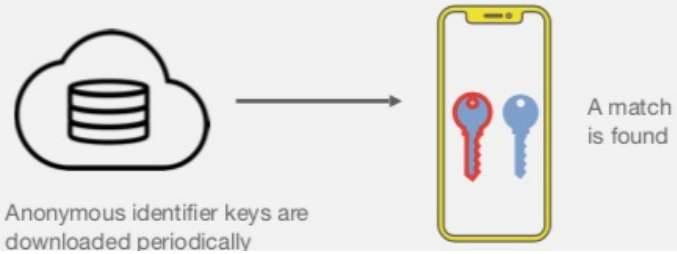
Contact Tracing System

Alice continues her day unaware she had been near a potentially contagious person

Alice sees a notification on her phone

Sometime later...

Alice's phone periodically downloads the Bluetooth beacon keys of everyone who has tested positive for COVID-19 in her region. A match is found with Bob's random Bluetooth identifiers.

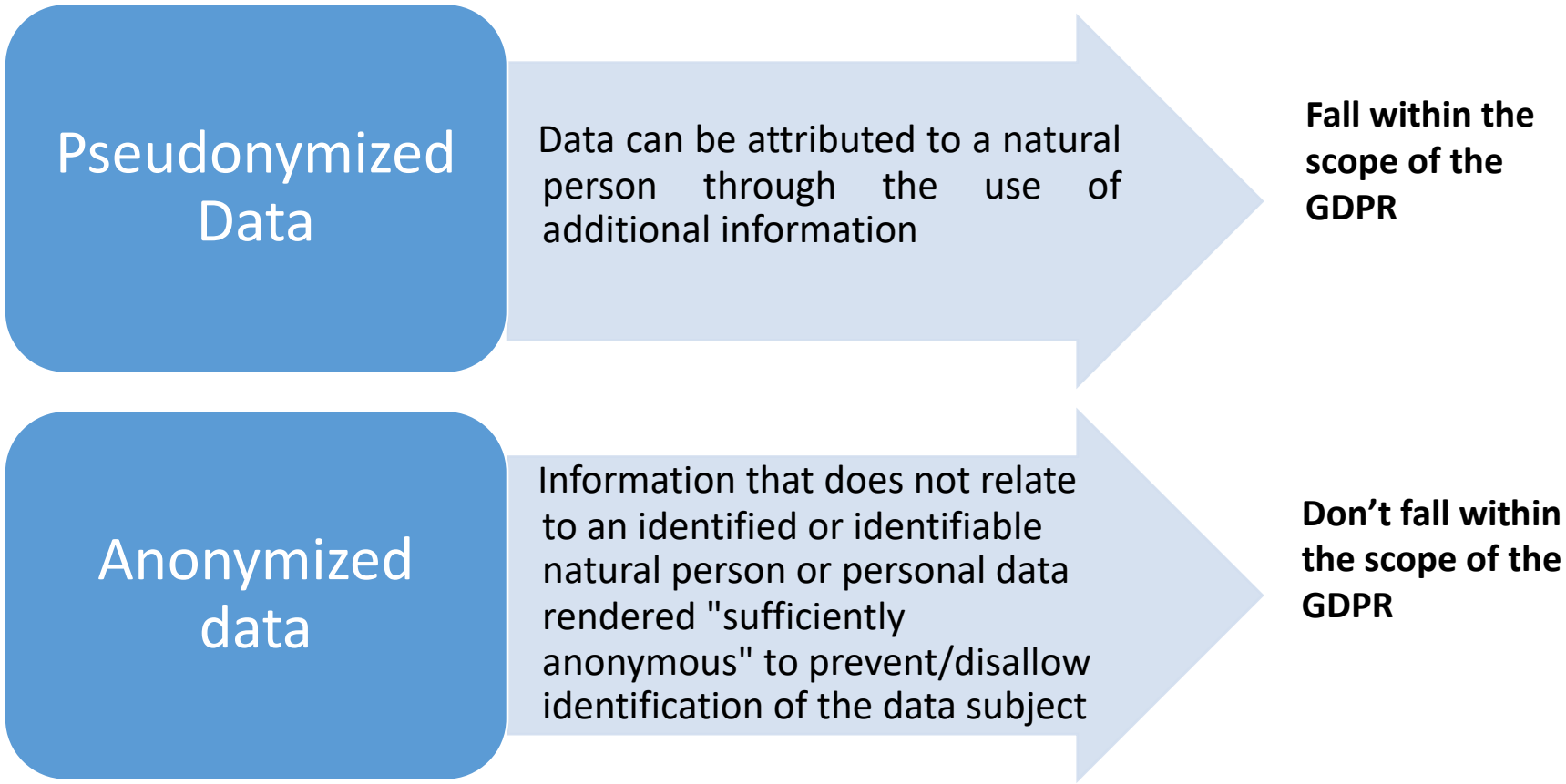


Anonymous identifier keys are downloaded periodically

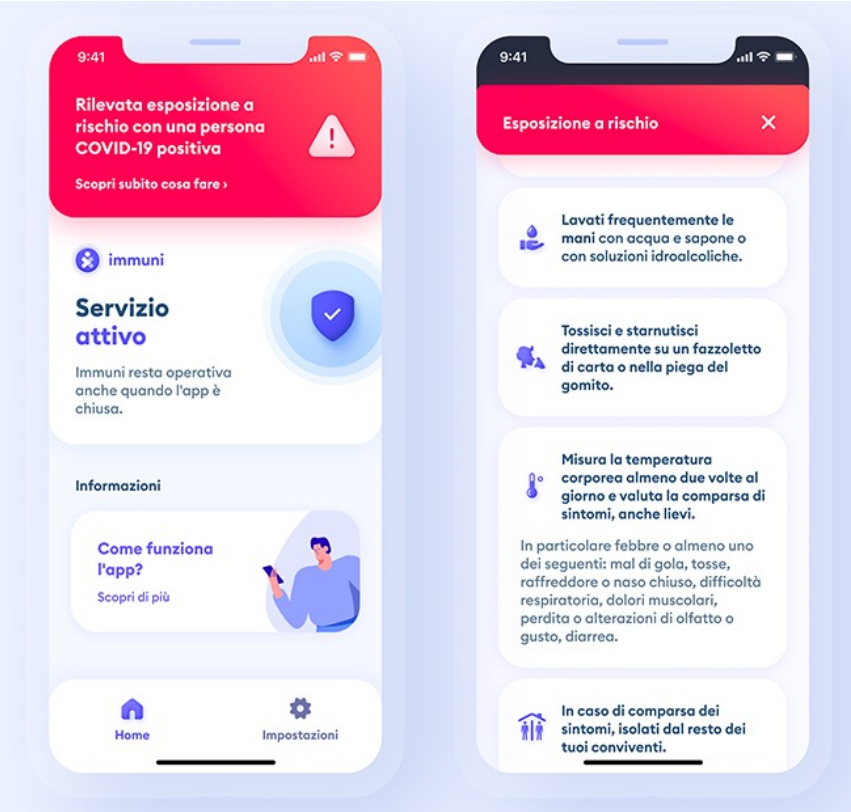
Alice's phone receives a notification with information about what to do next.

Additional information is provided by the health authority app

GDPR - Whereas 26



How to limit risks to stakeholder



A. EPIDEMIOLOGICAL STANDARDS: Design the App according to the best standards in the epidemiological field

B. TECHNICAL FEATURES: Accuracy (tracking contacts with one-meter accuracy), completeness (history of all relevant contacts), information integrity (collection of concrete risk events), scalability of the solution, and security of the technology and infrastructure

C. INTEROPERABILITY: Interoperability with solutions developed in other EU countries

D. COMPUTER SECURITY: Appropriate measures to address cyber risks and possible misuse of the application

E. GUARANTEES: 1) Cosent; 2) Temporary nature of the measure ("gentle self-dismantling"); 3) Retention period based on necessity and proportionality; 4) Compliance with privacy and confidentiality regulations; 5) Location data is neither necessary nor recommended

GDPR Compliance

Analyze what you collect & where is data stored.
(Processing Activity Register)

1

Check if the **time you store** personal data is relevant.
If not, remove data (Data Retention and Disposal policy)

2

Inform your clients how they can modify or delete their data.
Privacy Policy webpage

3

Monitor who has access to personal data.

4

Processing Activity Register

Business Function	Name of Business Process	Owner of Process	Functional Description of Processing	Purpose of Processing	Basis for Processing	Type of Processing*	Data and Data Subjects Used	Data Subject Categories	Storage
Identification of Business Process *Name of Process Owner* *(In the column below, the name of the processing activity is repeated for the purpose of the readability of the registry.)*	Report the name and description of the business process.	Identify the owner(s) (role) of the business process that the processing activity is part of.	Identification of and information about the processing activity *number , functional description , finality, legal basis, type of processing and functional description*	Enter the purpose of the processing activity. A list with types (indicative list of purpose types) with some standard purposes has been included on the Lists tab. Note: This list does not cover all situations. For instance, the DPA could decide that more precise information is required for a specified processing activity.	Provide the legal basis for the processing activity. A list of possible legal bases for processing, as mentioned in GDPR Article 6, is provided in the Lists tab. Clarify, if necessary (e.g. reference the statute, if the legal basis is statutory).	Indicate what type of processing is involved: Mention the types that are relevant to the processing activity (see the list 'Processing Types' in the Lists tab). Enter 'Normal' if the type is not one listed under 'Processing Types' (see the Lists tab).	Details about the data being processed and the data subjects whose data are being processed. *functional category, sensitive category of data processing, data subject category, classification level, retention period, original source*	Indicate the data subject categories.	Indicate where the data is currently being stored: Paper records (internal and external) Emails Share folders Desktops Mobile phones

Retention Period	Disposal	Original Source	Third party/outsourcing contractor	Name	Data Transfer	Technology	Description	Comments
Provide the retention period for the processed data.	Indicate if any data destruction/disposal is currently taken place after the retention period. If yes, please explain what data is being deleted and why.	Indicate the source of the data if not the data subjects themselves.	Identify the sub processor (outsourcing contractor) involved in the processing activity *name, no. of data processing contract*	Enter the name of the processing activity.	Information about possible data transfers to third Countries *data categories, recipient categories, third country/ international organization, documentation of appropriate safeguards*	Description of the technologies, applications, and software employed in the processing activity (other than Microsoft Office).	Indicate how the processing activity will be performed. Which technologies (e.g. cloud based, block chain, etc.), applications or software are employed for the processing activity?	Write down any comments/points of action regarding the processing activity.

CNIL: Record of processing activities model: https://www.cnil.fr/en/record-processing-activities

M2. GDPR: Task distribution (DC, DP, JC, DPO), Accountability

- GDPR
- Task distribution
- Accountability

- Data Controller
- Data Processor
- Joint Controller
- Data Protection Officer

Stakeholders of GDPR

Data Subject

An **individual person**, resident of European Union countries, the subject of the personal data.

Data Controller

Institution, business or a person **processing the personal data** e.g. e-commerce website.

Data Protection Officer

Person appointed by the Data Controller responsible for overseeing data protection practices.

Data Processor

Subject (company, institution…) **processing a data on behalf of the controller** e.g. Google, Facebook, CRM app…

Data Authority

Public institution monitoring implementation of the regulations in the specific EU member country.

Stakeholders of GDPR

DATA CONTROLLER

The data controller determines the purposes for which and the means by which personal data is processed.

So, if your company/organisation decides 'why' and 'how' the personal data should be processed it is the data controller.

DATA PROCESSOR

The data processor is the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Processors act on behalf of the relevant controller and under their authority.

JOINT-CONTROLLER

two or more data controllers that jointly decide why and how to process personal data are collectively known as "joint controllers." The joint controller relationship arises more commonly than many people realize

In case of doubt, see **EDPB Guidelines 07/2020** on the concepts of controller and processor in the GDPR.

Task Distribution

Data Processor

The decision-making power over data processing is the criterion for distinguishing between controller/processor

Different level of control over data processing and different accountability/liability:

Quality of data processor: The processor must provide **sufficient guarantees** to implement **appropriate technical and organisational measures** in such a manner that processing will meet the requirements of the GDPR (Article 28.1)

Contractual relationship between controller and processor ("a contract or other legal act", Article 28.3) regarding

- the subject-matter and duration of the processing
- the nature and purpose of the processing
- the type of personal data and categories of data subjects
- the obligations and rights of the controller

Case

Lack of Data Processing Agreement

Giessegi Industria Mobili S.p.A. - 15 december 2022: Giessegi was a data controller, and it was in a contractual relationship with a processor (Verizon) who provided geolocation devices. The controller installed these devices to track vehicles delivering goods on its behalf. These vehicles were not directly owned by the controller, but rather by a third company, to which the controller outsourced certain services. The data subject was a driver employed by this third company, and he had no direct contractual relationship with the controller.

No controller-processor agreement existed between Giessegi and Verizon.

The Italian DPA fined a Giessegi €50,000.

Task Distribution

Sub-Processor

The processor can engage another processor with prior specific or general written authorisation of the controller (Article 28.2)

- The same obligations as set out in the contract or other legal act between the controller and the processor are imposed on sub-processor (contract or other legal act)
- Guarantees to implement appropriate technical and organisational measures
- The initial processor remains fully liable to the controller for the performance of sub-processor's obligations (Article 28.4)

Case

Lack of authorization to engage a sub-processor

ISWEB S.p.A. - 7 aprile 2022: ISWEB was a provided a web application provider, who entered an agreement with a group of hospitals to create the application for collecting and managing **employees' whistleblowing reports**. ISWEB contracted the company Seeweb for hosting the whistleblowing application.

ISWEB did not ask the prior written authorisation from the controller for engaging a sub-data processor, and did not formalise its processor-sub-processor relationship with Seeweb through a contract or other legal act.

ISWEB claimed that the object of its contract with the hospitals was only the provision of technological infrastructure, arguing that neither ISWEB nor Seeweb processed data which would allow users to be identified or made identifiable, because the whistleblower reports were encrypted with a key exclusively available to the hospitals. Therefore, ISWEB claimed that it was not required to obtain authorisation from the hospitals nor contractually impose the same data protection guarantees on Seeweb.

The Italian Authority didn't agree with the allegations, and fined a processor €40,000 for violating Article 28(2) GDPR.

Task Distribution

Joint-Controller

Joint-controllership (Article 26): two or more controllers jointly determine the purposes and means of processing.

- Formal agreement between joint-controllers
- Determine respective responsibilities and obligations in particular as regards the exercising of the rights of the data subject and their duties to provide the information (so-called privacy policy) to the data subjects
- The data subject may exercise his or her rights under in respect of and against each of the controllers.

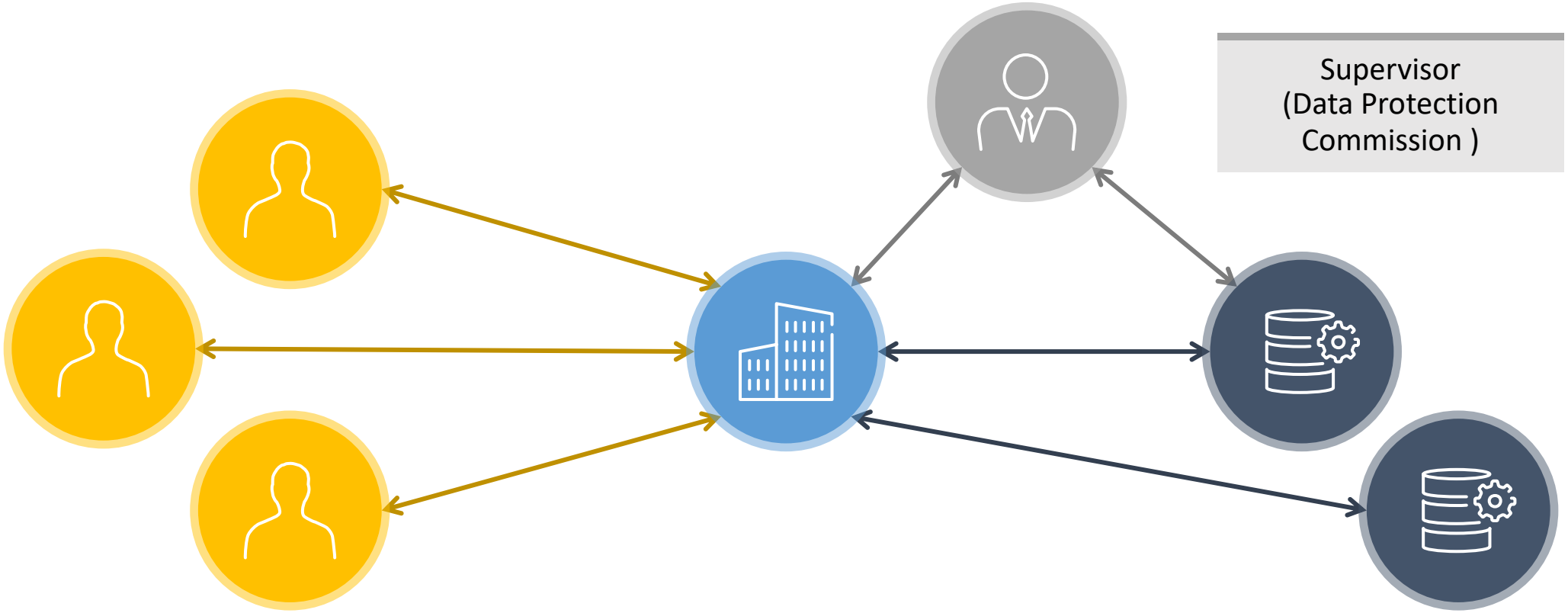
Case

Joint-Controller

C-25/17, Jehovan todistajat: Jehovah's Witness Community collect personal data during their door-to-door activities, including names and addresses of persons unknown to them without their knowledge or consent. Both the members and the community were involved in the activities, that were aimed at engaging in preaching, keeping records about preachers and distributing community publications.
They were forbidden from doing so, unless the legal requirements for processing were satisfied.

The Court held that «*a religious community is a controller, jointly with its members who engage in preaching, for the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, without it being necessary that the community has access to those data, or to establish that that community has given its members written guidelines or instructions in relation to the data processing*».

GDPR Subjects Relations Diagram Example




Accountability

Accountability

General Principles

- Obligations of the data controller/processor
- Security measures
- Risk management
  - ✓ Reporting obligations
  - ✓ Data breach, Business continuity, and Disaster recovery plans
  - ✓ DPIA
  - ✓ Codes of conduct, certifications, seals and marks

Accountability

Data Protection Strategy

- Mapping data flows and processing activities
- Mapping task distribution
- Assessing potential risks
- Defining procedural and technical measures
- Increase accountability
- Define a data protection strategy, identifying weaknesses and priorities
- DPO and team of experts

Accountability - Case

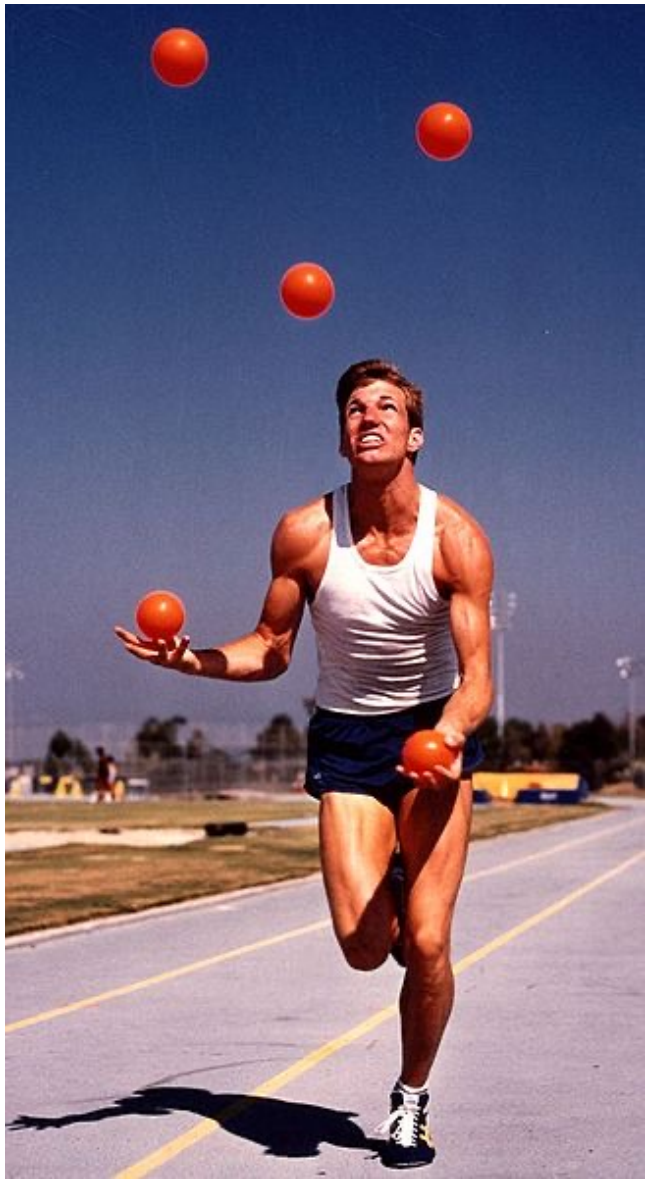
Enel Energia is an important Italian energy providers. The Italian Authority received hundreds of reports from users who received unwanted promotional phone calls. The phone calls were often made by partner companies, not by Enel itself.

Citizens reported a persistent and disturbing sense of interference in their sphere of privacy due to these practices, which are often not only invasive, but also particularly aggressive.

The Authority established:

- Violation of Article 5(2) GDPR and Article 25(1) GDPR, for **not having taken effective action against undue promotional contacts made in its name** by exercising its duties of accountability and privacy by design (through elements of prevention, functionality, security, transparency of treatment and centrality of the person concerned).
- Violation of Article 5(2) GDPR, for **failing to provide evidence of compliance with data protection legislation** in the case of unsolicited promotional communications by a business partner.
- Violation of Article 5(2) and Article 24 GDPR, for **failing to control the activities of its business partners**, including through appropriate technical and organisational measures.

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

Data Protection Officer

Professional qualities

- 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
- 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

Data Protection Officer

Independency

- 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 personally responsible for non-compliance with data protection requirements

Data Protection Officer

GLOVO Spain

The Spanish Data Protection Authority imposed a fine of € 25.000 on Glovo for the **non-compliance of its duty to appoint a Data Protection Officer** (DPO).

The defendant answered stating that not to be included among the mandatory appointers according to Article 37 GDPR, so it did not have the need to appoint a DPO.
Glovo also stated that, despite these facts, it had an internal data protection board with exactly the same role and functions as a DPO, and that such board effectively develops the activity of a DPO.
The AEPD did not accept these allegation and therefore started the sanction procedure. Later, Glovo stated that, in 2019, it had formally appointed a DPO, but it had decided not to make this appointment public until 2020, because the board and the legal department of Glovo had been already developing such functions effectively.
The Spanish Authority ultimately imposed a fine of € 25.000.

M3. Security, accountability risk assessment

Security

Security measures (Article 32 GDPR)

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

Security

Security measures (Article 32 GDPR)

- ✓ Security obligations: Controller/processor (Articles 24 and 28.3.c)
- ✓ The controller/processor **must ensure that any natural person acting under their** authority does not process personal data except on instructions from the controller, unless required by law (Article 32.4)
- ✓ **Focus on risk**
  - Likelihood/severity for the rights and freedoms of natural persons
  - Examples: accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Security

Security measures (Article 32 GDPR)

- ✓ Appropriate [to the risk] technical and organisational measures
  - Nature, scope, context and purposes of processing
  - Risks for the rights and freedoms of natural persons (likelihood/severity)
  - The state of the art and costs of implementation
  - An open list

- ✓ Examples
  - Pseudonymization
  - Encryption of personal data
  - Measures to ensure confidentiality and integrity
  - Measures to ensure availability, business cortinuty and resilience
  - Testing tools

Technical measures – 2021 ENISA 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**, and (iv) publish cybersecurity policies.

2

Training courses

According to ENISA, they should have two main features: (i) they should be **customized**, with reference to content, for small and medium-sized enterprises and their reality, and (ii) 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 a **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, ENISA encourages: (i) to use a **passphrase** (three unfamiliar or little-used words that create an easy-to-remember phrase), (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.

Technical measures – 2021 ENISA report

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 l**ocked** or carried always with you, (iii) **do not use** suspicious **USB** drives, and (iv) enable **automatic device lock**, (etc.).

9

Backup security

Backups 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 a regular basis, simulating attacks in order to to identify, for example, any potential weaknesses 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.

Organisational measures – 2021 ENISA report

1

Organisational model

- Internal contacts
- Staff in charge of processing
- System administrators
- DPO

2

Privacy policies

- Candidates and Employees
- Website
- Suppliers
- Video surveilance

3

Policies

- Data retention
- Data breach
- Risk and privacy assessment

4

Privacy by design

Implement appropriate technical and organisational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects

5

Consents

- Marketing
- Profiling
- Geolocation
- Communication

6

Documentation

- Record of processing activities
- Data Processing Agreement

Takeaway on Security

STANDARDS

- Good procedures, schemes and toolkits
- Measures to prevent and respond to incidents

REPORT

- Report from providers to authorities on annual or shorter interval
- …in order to rise awareness on specific risks

COOPERATION

- Notifications from providers to authorities
- Notifications between several, even international, authorities

TIMING

- Undue delay - in order to avoid possible lack of awareness of cybersecurity threats

Rousseau: unsuitability of the platform

Financial penalty against Rousseau Association – Italian DPA (Garante)

April 4, 2019

- **Object of the investigation**: critical aspects regarding the protection of users' personal data relating to online voting carried out on the platform managed by Wind Tre at its own data centre. The Italian privacy authority inspection revealed that the authentication credentials of the system administrators (Wind Tre employees) were shared by a number of operators, thus making it impossible to attribute the actions carried out in the system to a specific person.

- **Alleged infringement**: non-adoption of security measures which the data controller and processor are required to take in order to ensure an adequate level of security, as required by Article 32 of the GDPR.

- **Amount of penalty**: **50.000 euros**

GIE INFOGREFFE: password security

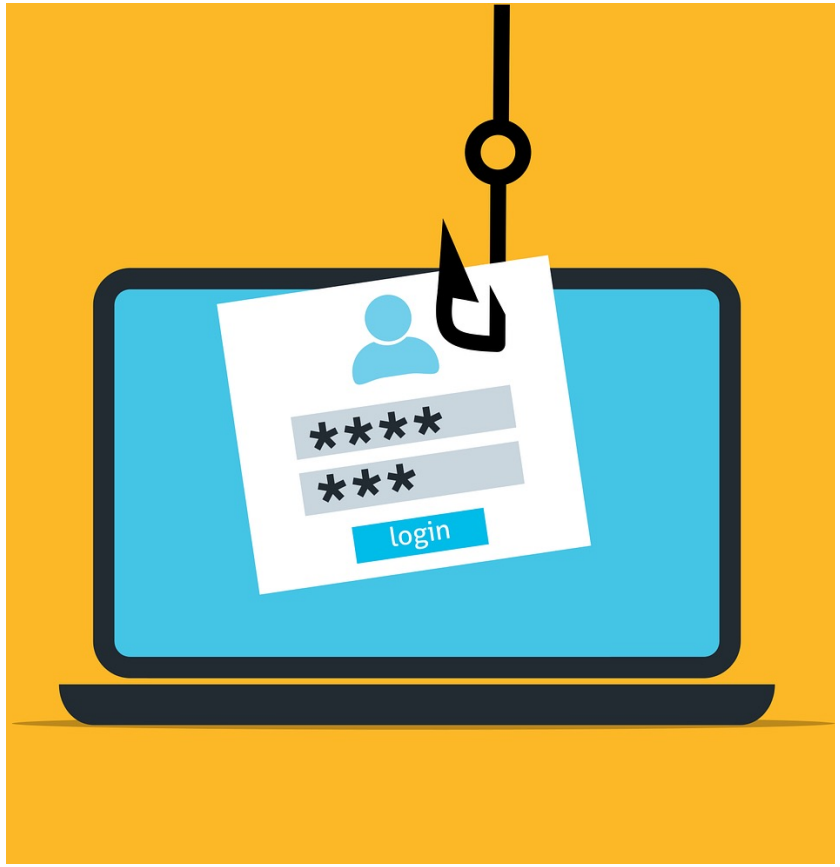
Financial penalty against GIE INFOGREFFE – French DPA (CNIL)

September 8, 2022

- **Object of the investigation**: the data controller has a website which allows consultation of legal information on companies. A data subject filed a complaint at the CNIL, stating that he was able to get a password on the phone only by telling his name. The data subject also complained that the website stored user passwords in plain text.

- **Alleged infringement**: article 32 GDPR was violated because of several security problems: the controller stored passwords in plain text in a database; users were not allowed to create a password of more than 8 characters, without any complexity requirements and other security measures; passwords were transmitted in plain text during email conversations with users; users were not warned when their password was being changed, thus not ensuring a safe level security against identity theft.

- **Amount of penalty**: **250.000 euros**



Marriott: lack of security measures

Financial penalty against Marriott International – UK DPA (ICO)

September 30, 2020

- **Object of the investigation**: the ICO began investigations following notification of an attack on Marriott's IT systems that took place between may and September 2018. As a result, the attacker had access to vast amounts of costumers' personal data: Marriot estimated that they accessed 339 million guest records.

- **Alleged infringement**: there were many failures in placing the technical and organizational measures to safeguard personal data in Marriott's system: insufficient monitoring of privileged accounts and their user activity, insufficient monitoring of databases, poor control of critical systems and systems that have access to large amounts of personal data, and the fact that only certain type of sensitive data was encrypted (e.g. credit card numbers) but not all (e.g. many passport numbers). The ICO took into account mitigating factors such as the efforts that Marriott made to inform and help the victims.

- **Amount of penalty**: **20.7 million euros**

Risk assessment

General Principles

A three-step strategy

- ✓ Preliminary analysis
- ✓ Data strategy and data management
- ✓ Data minimization and by-design approach

Risk assessment

Risk assessment and management

- ✓ Self-assessment + supervision of SAs
- ✓ Three-stage model
  - General assessment (24 and 32) and by design/default approach (25)
  - Formal assessment (35 – High risk)
  - Prior consultation (36)
  - Compliance and enforcement (83.4.a)

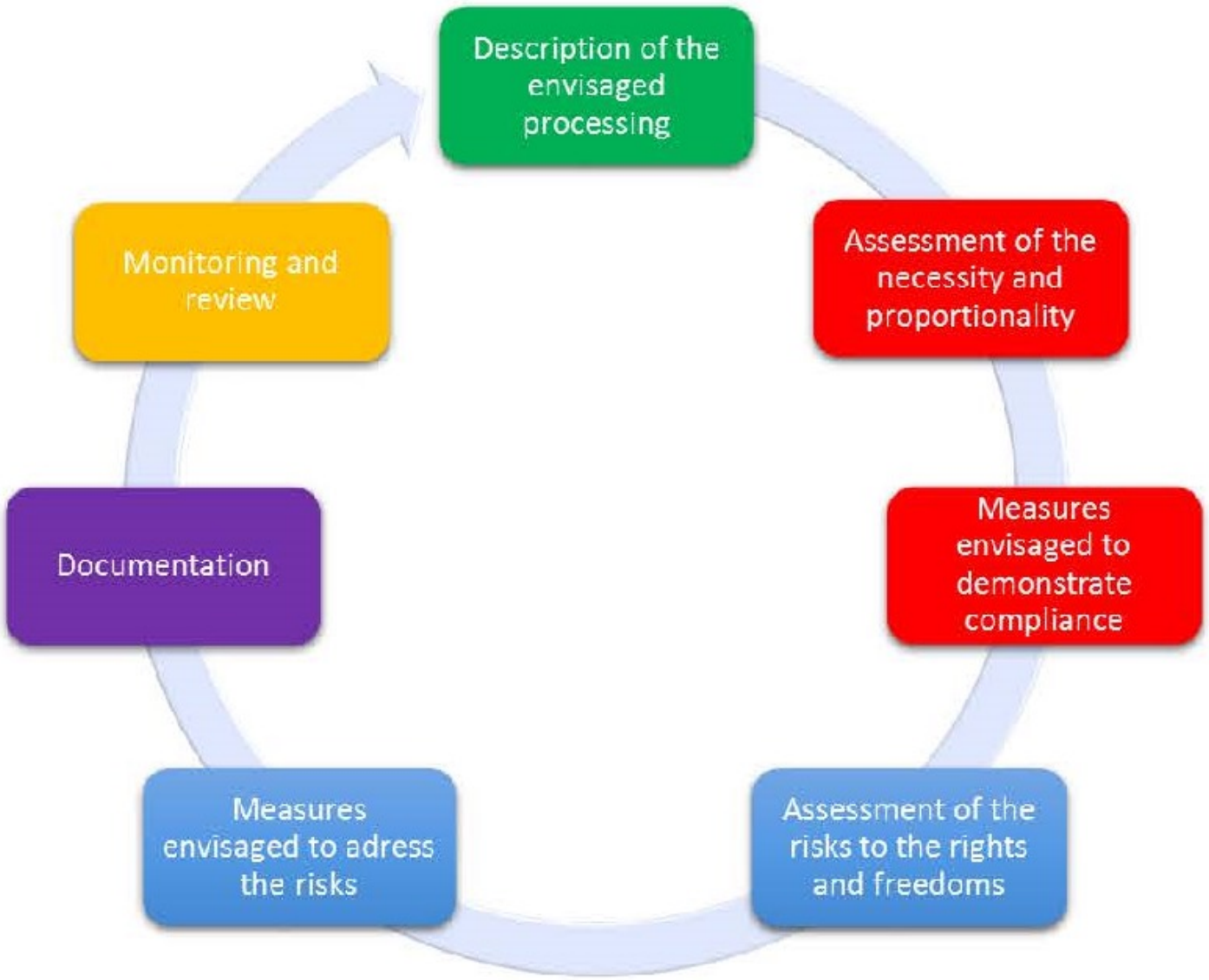
Risk Assessment

General assessment

- ✓ See above the criteria to comply with Article 32
- ✓ Security risks (e.g. accidental/unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise process) and impacts on the rights and freedoms
- ✓ Assessment: Likelihood and severity of risks
- ✓ Adoption of appropriate technical and organizational measures
- ✓ State of the art and the costs of implementation
- ✓ Circular approach (assessment – measures – testing)

M4. DPIA

DPIA


Description of the envisaged processing
Assessment of the necessity and proportionality
Measures envisaged to demonstrate compliance
Assessment of the risks to the rights and freedoms
Measures envisaged to adress the risks
Documentation
Monitoring and review

DPIA

Content

- ✓ 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 processing operations in relation to their 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 the GDPR

DPIA

Nature

- ✓ A question-base assessment
- ✓ Context-based analysis
- ✓ Different nature of assessment in case of security and impact on rights/freedoms

Approach

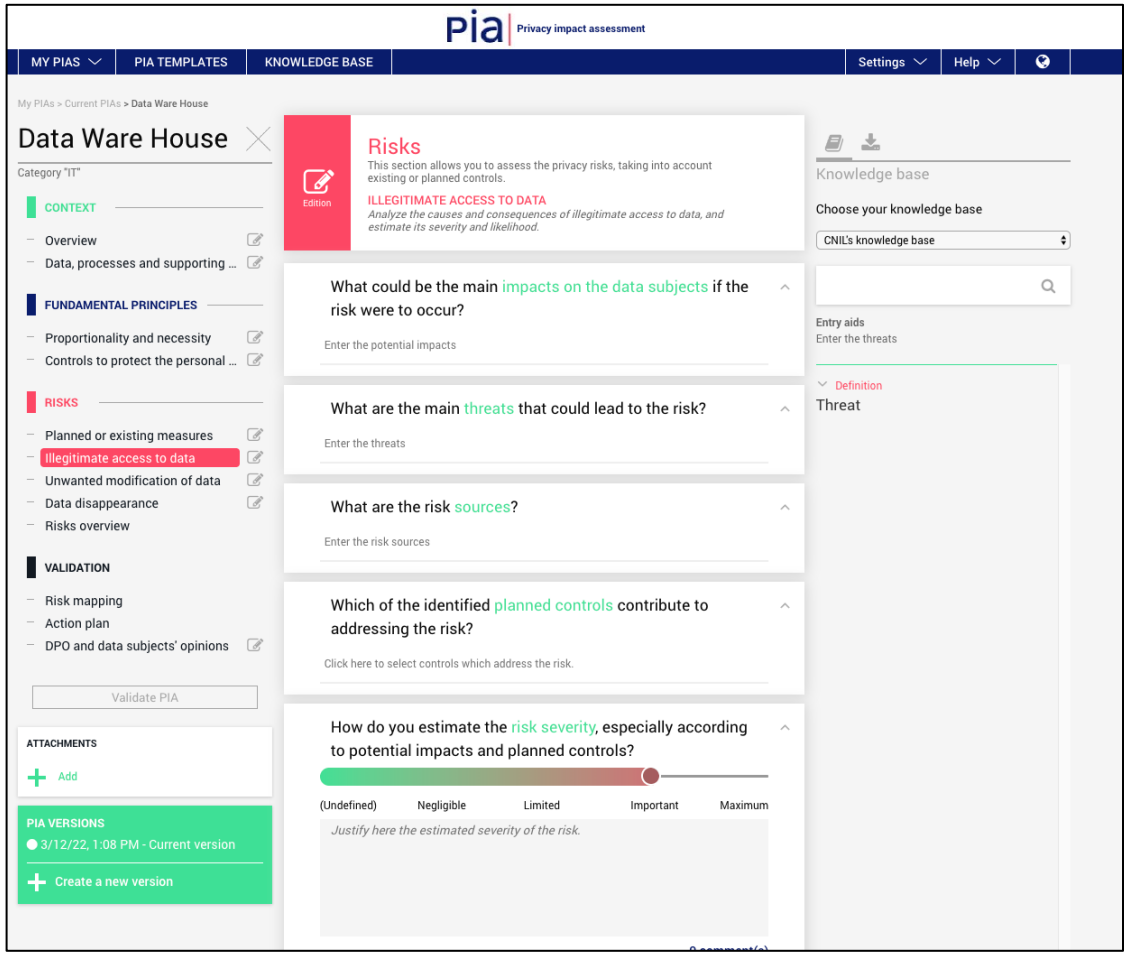
- ✓ Interdisciplinary team
- ✓ Analysis starting from the design phase
- ✓ Periodic verifications
- ✓ By-design/default approach (Article 25)

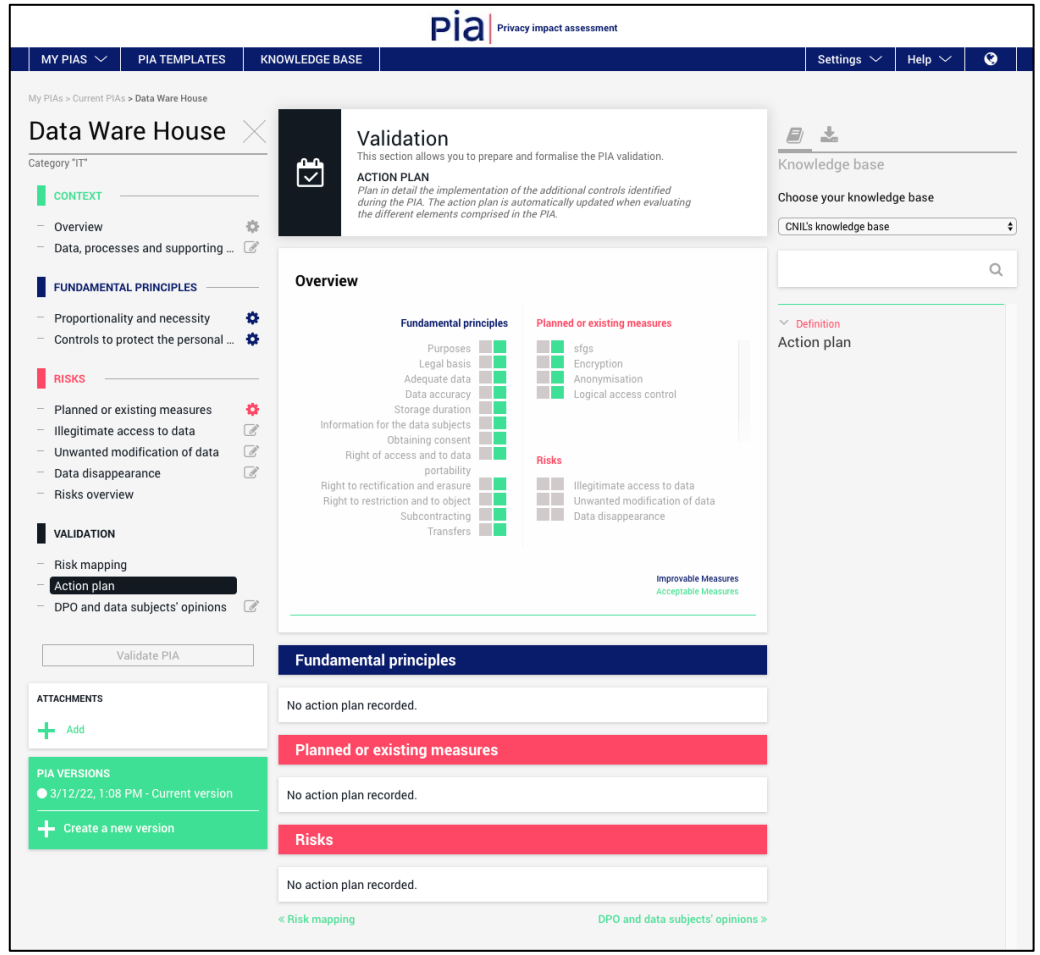
DPIA

Prior consultation

- ✓ A single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks
- ✓ The publication of a DPIA is not a legal requirement of the GDPR, but ART29WP/EDPB suggests considering the publication of at least parts, such as a summary or the conclusion of the DPIA
- ✓ Prior consultation (Article 36) - High residual risk
- ✓ Possible outcomes:
  - Further implementation of DPIA and/or envisaged measures
  - Stop data processing due to the lack of available mitigation measures

DPIA


pia
Privacy impact assessment
MY PIAS
PIA TEMPLATES
KNOWLEDGE BASE
Settings
Help
My PIAs > Current PIAs > Data Ware House
Data Ware House
Category "IT"
CONTEXT
Overview
Data, processes and supporting ...
FUNDAMENTAL PRINCIPLES
Proportionality and necessity
Controls to protect the personal ...
RISKS
Planned or existing measures
Illegitimate access to data
Unwanted modification of data
Data disappearance
Risks overview
VALIDATION
Risk mapping
Action plan
DPO and data subjects' opinions
Validate PIA
ATTACHMENTS
Add
PIA VERSIONS
3/12/22, 1:08 PM - Current version
Create a new version
Edition
Risks
This section allows you to assess the privacy risks, taking into account existing or planned controls.
ILLEGITIMATE ACCESS TO DATA
Analyze the causes and consequences of illegitimate access to data, and estimate its severity and likelihood.
What could be the main impacts on the data subjects if the risk were to occur?
Enter the potential impacts
What are the main threats that could lead to the risk?
Enter the threats
What are the risk sources?
Enter the risk sources
Which of the identified planned controls contribute to addressing the risk?
Click here to select controls which address the risk.
How do you estimate the risk severity, especially according to potential impacts and planned controls?
(Undefined)
Negligible
Limited
Important
Maximum
Justify here the estimated severity of the risk.
Knowledge base
Choose your knowledge base
CNIL's knowledge base
Entry aids
Enter the threats
Definition
Threat


pia
Privacy impact assessment
MY PIAS
PIA TEMPLATES
KNOWLEDGE BASE
Settings
Help
My PIAs > Current PIAs > Data Ware House
Data Ware House
Category "IT"
CONTEXT
Overview
Data, processes and supporting ...
FUNDAMENTAL PRINCIPLES
Proportionality and necessity
Controls to protect the personal ...
RISKS
Planned or existing measures
Illegitimate access to data
Unwanted modification of data
Data disappearance
Risks overview
VALIDATION
Risk mapping
Action plan
DPO and data subjects' opinions
Validate PIA
ATTACHMENTS
Add
PIA VERSIONS
3/12/22, 1:08 PM - Current version
Create a new version
Validation
This section allows you to prepare and formalise the PIA validation.
ACTION PLAN
Plan in detail the implementation of the additional controls identified during the PIA. The action plan is automatically updated when evaluating the different elements comprised in the PIA.
Overview
Fundamental principles
Purposes
Legal basis
Adequate data
Data accuracy
Storage duration
Information for the data subjects
Obtaining consent
Right of access and to data portability
Right to rectification and erasure
Right to restriction and to object
Subcontracting
Transfers
Planned or existing measures
sfgs
Encryption
Anonymisation
Logical access control
Risks
Illegitimate access to data
Unwanted modification of data
Data disappearance
Improvable Measures
Acceptable Measures
Fundamental principles
No action plan recorded.
Planned or existing measures
No action plan recorded.
Risks
No action plan recorded.
« Risk mapping
DPO and data subjects' opinions »
Knowledge base
Choose your knowledge base
CNIL's knowledge base
Definition
Action plan

Data Protection By Design and By Default

By Design

- ✓ Criteria: the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks
- ✓ Appropriate technical and organisational measures designed to implement data protection principles in an effective manner
- ✓ Integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

By Default

- ✓ Appropriate technical and organisational measures
- ✓ Ensuring that, by default, only personal data necessary for each specific processing purpose (amount of data collected, scope of processing, storage and accessibility) are processed

Foodinho & Deliveroo

Financial penalties against food delivery services – Italian DPA (Garante)

2021

- **Object of the investigation**: the Italian authority investigated on food delivery platforms, typically employing gig workers who deliver food orders by bike. Their apps for riders failed to provide transparent information about the algorithms used to manage work shifts, and their reputational rating system enabled discriminatory ratings that would exclude riders from job opportunities.

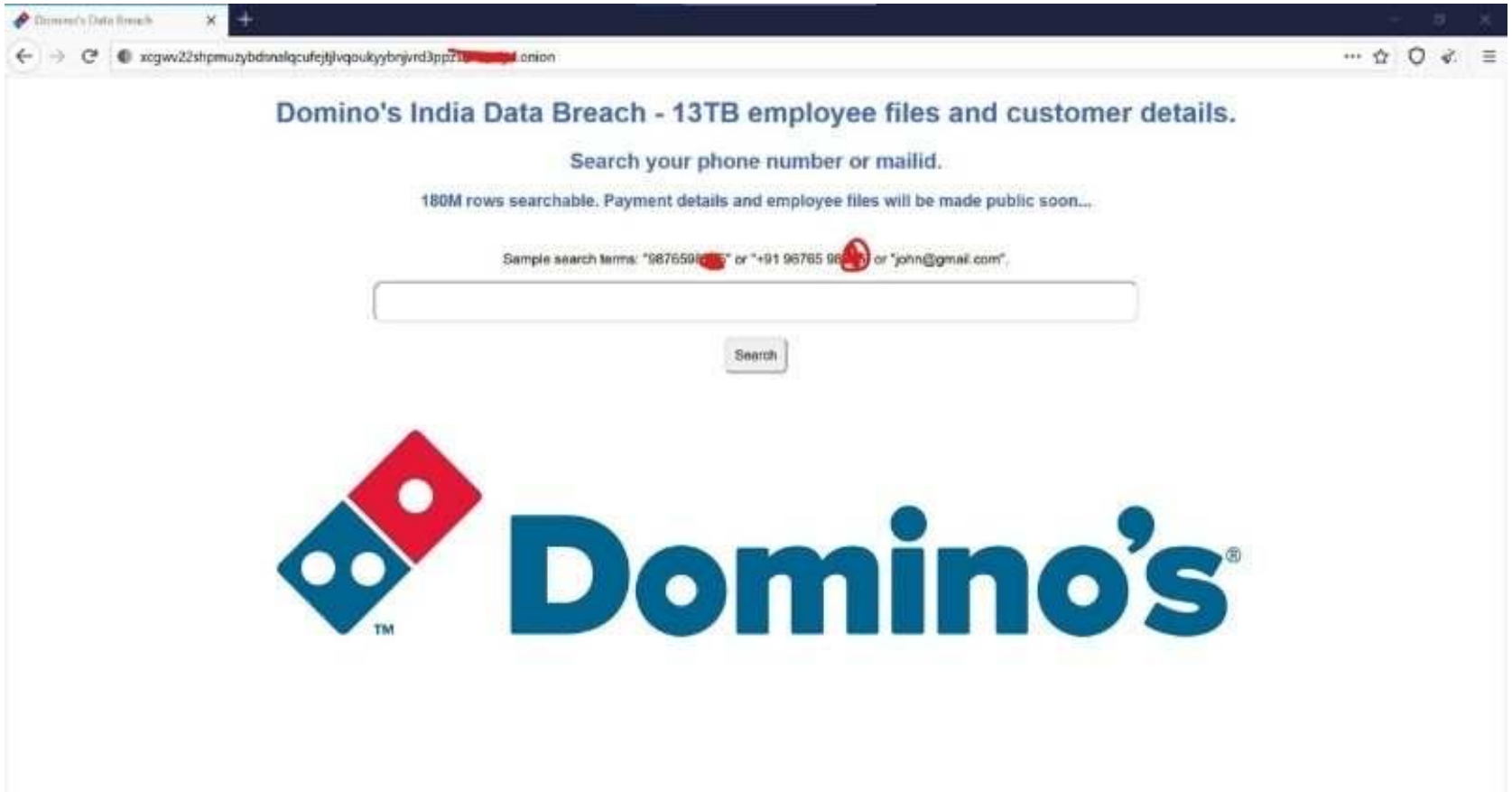
- **Alleged infringement**: The Garante della Privacy held that the companies violated the principle of data minimization and protection by design and by default. The app systems were configured to collect and store all data relating to the management of the order, and to allow authorized operators to pass simple functions from one system to another, with consequent sharing of the data collected across the various systems.

deliveroo

FOODINHO

M5. Data Breach


540 million
records compromised


Domino's India Data Breach - 13TB employee files and customer details.
Search your phone number or mailid.
180M rows searchable. Payment details and employee files will be made public soon...
Search
Domino's

Data Breach Definition

Article 4 of the GDPR defines data breach as a "personal data breach," which is a **security breach** that **accidentally or unlawfully** results in the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data that has been transmitted, stored, or otherwise processed.

Data Breach Classification

(i) "**Confidentiality Breach**", when there is accidental or abusive access to personal data;
(ii) "**Availibility Breach**", when there is an accidental or unauthorized loss or destruction of personal data;
(iii) "**Integrity Breach**", when there is an accidental or unauthorized alteration of personal data.

Loss of an unencrypted device	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.
A device is infected by ransomware	A ransomware is a type of malware that restricts access to the device it infects, requiring a ransom to be paid to remove the restriction
Loss of availability of personal data	A potential example of loss of data availability is when personal data is accidentally sent to an unauthorized third party.

Data Breach Obligation

- Obligation to notify the Data Protection Authority "without undue delay" and, where possible, within 72 hours ex art. 33 of the GDPR.

- Obligation to notify data subjects when the personal data breach is likely to present a high risk for the rights and freedoms of individuals

The Notification Procedure - Actors in the Process

	Planning	Response
Information security	Provide guidance regarding detection, isolation, removal and preservation of affected systems	Address data compromises; carry out forensic investigations
Legal	Limit liability and economic consequences	Advise on response requirements
HR	Provide an employee perspective	Serve as information conduit to employees
Marketing	Advise about customer relationship management	Establish and maintain a positive and consistent message
Business development	Represent knowledge in handling and keeping the account	Notify key accounts

Risk to the rights and freedoms of individuals

Factors determining the presence of risk to the rights and freedoms of individuals

a) **The type of "breach":** it is clear that the type of breach determines a parameter for assessing the risk. A breach of the health data of all patients in a hospital is quite different from the loss of a patient's health data;

b) **The nature, number, and degree of sensitivity of the Personal Data breached:** access to the name and address of a child's parents is a different risk than access by birth parents of the name and address of adoptive parents;

c) **Ease of associating the violated data with a natural person:** it often happens, in fact, that the violated data is not easily traceable to a specific natural person;

d) **Severity of the consequences for the Data Subjects:** when the Data Controller perceives the risk that the Personal Data subject to the breach may be immediately used against the Data Subject (e.g. in the case of fraud or substitution of person);

e) **Number of Data Subjects exposed to risk:** it is clear that a parameter to be taken into account is the number of Data Subjects potentially involved;

f) **Characteristics of the Data Controller:** the graduation of risk must be different according to the type of subject affected. For example, an attack on a hospital structure is one thing, another is an attack on the server of a one-room flat used by the company as a guesthouse.

Bank of Ireland: 22 data breach notifications (!)

Financial penalty against Bank of Ireland – Irish DPA (DPC)
March 14, 2022

- **Object of the investigation**: inaccurate customer data was uploaded to the Central Credit Register (CCR) by the controller "which gave an erroneous view of BOI's customers' finances and credit history".

- **Alleged infringement**: the controller contravened failed to report 17 personal data breach without undue delay and to provide the information required under Article 33(3) GDPR. The controller also contravened Article 34 GDPR as it did not inform the data subjects about the personal data breaches without undue delay at least in 14 cases.

- **Amount of penalty:** **463,000 euros**

Enel Energie Muntenia SA: wrong e-mail recipient

Financial penalty against Enel Energie Muntenia SA (Enel) – Romanian DPA (ANSPDCP)

August 25, 2022

- **Object of the investigation**: customer data was sent via e-mail to a wrong recipient, a different customer. The recipient, when he saw personal data of a different customer, filed a complaint with the DPA.

- **Alleged infringement**: Enel (controller) did not adopt sufficient security measures and failed to notify the breach within 72hrs from the moment it became aware thereof.

- **Amount of penalty: 10,000 euros for the breach; a "warning" for the failed notification to the DPA**

Vastaamo – a deep shock for Finland

Facts

Vastaamo was a Finnish private psychotherapy service provider which operated as a sub-contractor for Finland's public health system.

October 2020: Vastaamo (controller) announced that its patient database had been hacked. It was used in an attempt to extort the controller by demanding tens of bitcoins.

The attackers threatened to publish the records if the ransom was not paid. To add pressure to their demands, the extorters published hundreds of patient records on a Tor message board, containing full names, addresses, social security numbers and therapists' and doctors' notes from each session.

There was a huge public scandal.

The company refused to pay. Hence, the extorters sent requests to patients asking to pay ransoms in order to avoid publication of their data. Such data was found to be protected by insufficient security measures: no encryption, no anonymization.

The patient records were first accessed by the criminals in November 2018 and then again in March 2019.

Vastaamo – a deep shock for Finland

The Vastaamo Case shook Finland. Thousands of victims have suffered anxiety, insecurity and stress.

This created a national opportunity for public discussion about mental health issues. Moreover, it served as a wake-up call for Finland's cyber security who then increased.

In addition, the Finnish DPA started taking the violations of the GDPR more seriously and increased enforcement activities.

A suspect was arrested in France in February 2023.

Vastaamo was declared bankrupt in February 2021.

Vastaamo – GDPR sanctions

The Finnish DPA found that Vastaamo had violated several GDPR provisions, including Articles 33 and 34 for having failed to report in due time the data breaches to the DPA and to the data subjects, respectively.

Moreover, the controller had failed to implement appropriate security measures and to embed core GDPR principles (accountability, data protection by design and data protection by default).

Amount of the penalty: 608,000 euros (approx. 4.2% of the firm's 2020 turnover).

Content of the notice to the DPA

The notice must contain:

- **Nature of the personal data breach**, including the categories and number of data subjects and the type and number of records involved
- **Disclose** the contact details of the data protection officer
- **Describe** the likely consequences of the breach
- **Describe** the measures taken or to be taken to remedy the breach and counteract its adverse effects.

Severity Assessment

When it is not necessary to notify the data subject

Notice must also always be made to the data subject in "plain and simple language" except:

A) when the data controller has implemented appropriate technical and organizational measures;

B) when the holder has subsequently taken measures to prevent the occurrence of high risks to the rights and freedoms of data subjects;

C) when such communication would require disproportionate efforts, so it may be replaced by a public communication.

Content of the notice to the DPA

Data Controllers are, therefore, required to maintain a log of Data breaches that must contain the following information:

- the details relating to the Data breach (i.e. the cause, the place where it occurred and the type of Personal Data breached);

- the effects and consequences of the breach and the intervention plan prepared by the Data Controller.

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:

(i) the Owner decided not to proceed with the notification;
(ii) the Data Controller has delayed the notification procedure
(iii) the Data Controller has decided not to notify the Data Breach to the Data Subjects.

How to manage the databreach process

Preparedness: be ready to handle it through an incident response plan

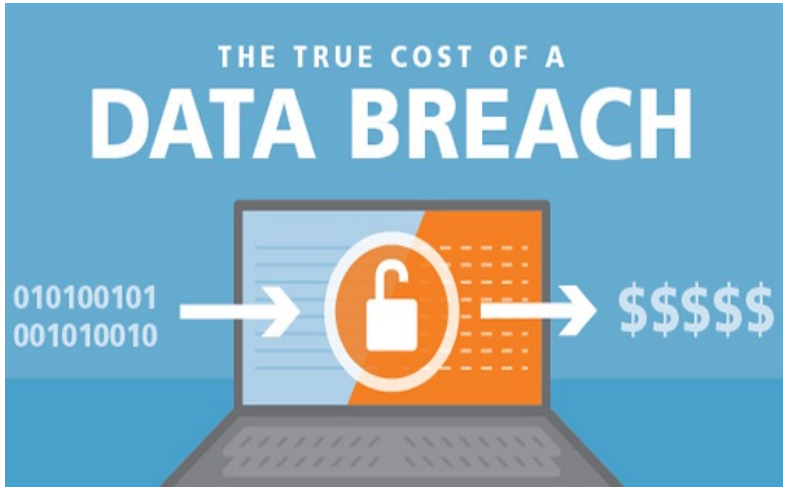
Define roles and responsibilities by involving primarily affected business functions (including CEO!);

- ❑ Perform simulations and continuous program updates;
- ❑ be very concrete and effective;
- ❑ detail how you will interact with authorities.

Prevention - reduce the chances of a breach happening:

- ❑ training and awareness raising;
- ❑ Improve security measures, controls and safeguards - manage cyber risk wisely.

What are the costs of a Data Breach?



- Direct damage: loss of data or money
- Abnormal customer turnover
- Reputational damage and loss of customer confidence
- Help desk activities
- Activities of internal investigation
- Legal expenses
- Costs for the restoration of the information system

Notification procedure – practical aspect

- Verify legally required notifications to authorities or stakeholders;
- analyse assumptions carefully;
- carry out notification according to templates (if any) and official channels.

Notification procedure – practical aspect

Although the responsibility for the protection of personal data and related security and notification obligations rests with the Data Controller, the Data Processor must also be considered part of the process.

In particular:

- Art. 28.3 specifies that a contract or other act having contractual force governs the relationship between the parties
- Art. 33.2 clarifies that the Responsible Party must notify the Data Controller if it becomes aware of an incident "without undue delay

Remediation Plan

- Correct the vulnerability that allowed the incident to occur;
- **Lesson learnt: improve your approach to information security through experience;**
- Share information with relevant stakeholders to reinforce your organization's perimeter;
- If human error was the cause of the incident, reinforce training actions.

Data Breach Register

There are two tools to use:

- Incident log - concise, but comprehensive and updated 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

Art. 33.5, GDPR
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.

The only real safe system is a shut down system, locked in a concrete casting, sealed in a lead-lined room, protected by armed guards. But even then I have my doubts.

Eugene Spafford