GDPR & PUBLIC SAFETY

The GDPR came into force in May 2018. Public safety organisations are not exempt from this legislation and should make significant efforts to comply...

eena
EUROPEAN EMERGENCY NUMBER ASSOCIATION

Bird & Bird

GDPR & PUBLIC SAFETY

Title: GDPR & Public Safety

Version: 1.0

Revision date: 26/08/2019

Status of the document: APPROVED

Authors:

Merav Griguer, BIRD & BIRD

Julie Schwartz, BIRD & BIRD

Océane Faroy, BIRD & BIRD

Contributors:

Rose Michael, EENA

Cristina Lumbreras, EENA

EENA

European Emergency Number Association

EENA 112

Avenue de la Toison d'Or 79, Brussels, Belgium

T: +32/2.534.97.89

LEGAL DISCLAIMER:

This document is authored by EENA staff members with contributions from individual members of EENA and represents the views of EENA. This document does not represent the views of individual members of EENA, or any other parties.

This document is published for information purposes only and it does not declare to be a statement or interpretation of EU law or the national law of EU Member States. This document is entirely without prejudice to the views of relevant national statutory authorities and their legal functions and powers, whether under EU law or the national law of their Member State. Accordingly, under no circumstances may reliance be placed upon this document by any parties in compliance or otherwise with any applicable laws. Neither may reliance be placed upon this document in relation to the suitability or functionality of any technical specifications, or any other matters discussed in it. Legal advice, technical advice and other advice as relevant, may be sought as necessary.

EXECUTIVE SUMMARY

This document aims to support public safety organisations in their efforts to comply with the GDPR.

The General Data Protection Regulation ("GDPR") came into force on 25 May 2018 and required public and private companies to comply with its provisions regarding their processing of personal data.

One year after its entry into force, it appears that 100% GDPR compliance is difficult to achieve for companies and organisations. However, it is important to work towards compliance and at least implement compliance measures such as appointing a compliance pilot, mapping data processing, identifying actions that need to be prioritised, managing risks, organise internal procedures, document compliance.

Such difficult compliance work is particularly complicated in specific sectors such as public safety.

Indeed, the scope of the GDPR is extremely broad, covering private companies, public administrations, associations and non-governmental organisations, etc.: it is applicable to companies and organisations having an establishment in the European Union ("EU"), regardless of whether the processing takes place in the EU or not[1]. In addition, it is also applicable to companies and organisations not established in the EU, where the processing activities relate to the offering of goods or services (irrespective of whether a payment is required), or the monitoring of data subjects behaviour taking place within the EU.

Public safety organisations, emergency services, etc. which process personal data and even sensitive data, are therefore subject to the GDPR.

The purpose of this document is to present the fundamental principles related to the processing of personal data, but above all to support public safety organisations in their efforts to comply with the GDPR.

Using practical examples, this document is intended to present, step by step, the actions to be taken in order to comply with the regulations in force. Such steps include the different documents to be drafted, the practical way of mapping personal data, the identification of risks, the DPO governance within companies and organisations, how to choose appropriate partners offering sufficient guarantees in terms of compliance with the GDPR, etc.

Through the practical implementation and explanation of the different concepts, this document is intended to enable public safety organisations to review their compliance and thus anticipate the controls of the data protection authorities.

[1] Article 3.1 GDPR.

1 | INTRODUCTION

"1 year of GDPR, a new awareness" was the headline of the French data protection authority, the *Commission Nationale de l'Informatique et des Libertés* (hereinafter "CNIL") on 23 May 2019 in a press release on its website[2].

The CNIL noted that the GDPR, which came into force a year ago, created a particular dynamic with regard to the protection of personal data and the protection of privacy in general[3].

The GDPR is a European regulation that became effective on 27 April 2016 and came into force on 25 May 2018. Companies and organisations thus had two years to bring their processing of personal data into line with the applicable regulations.

In practice, the scope of the GDPR is very broad and concerns all companies that hold or process personal data. Thus, the GDPR does not exclude associations or Non-Governmental Organisations ("NGOs") from its scope, which must therefore also comply with the applicable regulations, as the GDPR drastically increases the amount of sanctions.

Fines can reach up to 2% of the total worldwide annual turnover or €10,000,000 in cases of violations regarding failures to establish a record of processing activities, notify security breaches, conduct Privacy Impact Assessments (PIA), designate a Data Protection Officer (DPO), etc.

They can also reach up to 4% of the total worldwide annual turnover or €20,000,000 in cases of violations such as unfair processing of personal data, lack of information notice, lack of legal basis for processing, non-compliance with individuals' rights or with rules on transfers of personal data to non-EU countries, or non-compliance with a Data Protection Authority's (DPA) injunction.

Thus, in order to understand the impact of the regulation particularly on public safety organisations, it is necessary to study the different fundamental principles applicable to personal data processing. These elements will allow a better understanding of the different compliance steps that public safety organisations will have to take in order to ensure their compliance with the GDPR and thus avoid sanctions.

[2] CNIL, 1 year of GDPR: a new awareness, May 23, 2019 -

[3] 70% of French people say they are now more sensitive to issues relating to the protection of personal data according to an IFOP survey conducted in April 2019, on a sample of 1,000 people out of a sample of people aged 18 and over.

2 | LEGISLATIVE BACKGROUND: GENERAL OUTLINE INTRODUCING THE GDPR & POLICE-JUSTICE DIRECTIVE

The Data Protection Reform Package consists of two texts:

- The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereafter, "**GDPR**"), directly applicable in the Member States as of 25 May 2018 and providing common principles to entities based or operating in the European Union (hereafter, "**EU**"); *and*

- The Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA(hereafter, the "**Police-Justice Directive**"), which needs a transposing law in each State Member to be applicable. .

In addition to this Data Protection Reform Package, there are guidelines from supervisory authorities and Article 29 Working Party ("**WP29**"), recently replaced by the European Data Protection Board[4] ("**EDPB**"), as well as Member States' national protection laws which adapt and complete the GDPR, and transpose the Police Directive.

[4] The EDPB works on the development of the common doctrine of the European Union data protection authorities through guidelines, advice, etc.

FOCUS ON THE POLICE-JUSTICE DIRECTIVE

The Police-Justice Directive sets out rules for the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection, prosecution or enforcement of criminal offences, including the protection against threats to public security and the prevention of such threats.

The Police-Justice Directive applies to data processing meeting the two following cumulative criteria:

1. **It pursues one of the purposes mentioned above, that is to say, prevention investigation, detection, (…) and the prevention of threats.**
   For example:
   - In "criminal matters": processing operations to manage measures to enforce sentences imposed by the judicial authority or activities carried out by the police;
   - Processing operations relating to police activities carried out prior to the commission of a criminal offence.

2. **It is carried out by a "competent authority"**
   - Any public authority (judicial authorities, police, any other law enforcement authorities, etc.) competent for the:
     - Prevention and detection of criminal offences
     - Investigations and prosecutions in criminal matters
     - Enforcement of criminal sanctions
   - Any other body or entity to which the law of a Member State entrusts the exercise of public authority and the prerogatives of public authority for the purpose of implementing processing operations covered by the Directive.

The GDPR and Police-Justice Directive have distinct fields of application, intended to be complementary.

3 | THE AIMS OF THE GDPR

At a glance, the GDPR aims to protect European Union (hereinafter "EU") citizens from privacy breaches in an increasingly data-driven world.

The GDPR is aimed at:

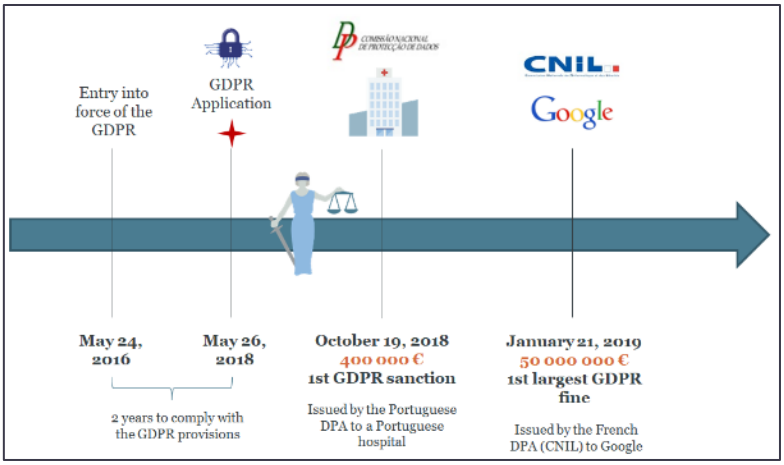
- **Modernising existing regulations** by replacing the 1995 Directive;
- **Giving better control** to EU citizens over their personal data; and
- **Unifying rules** allowing businesses, allowing for greater consumer trust.

The GDPR entered into force on May 24th, 2016, but it only applied starting May 25th, 2018, providing therefore companies and organisations with 2 years to become compliant with the GDPR provisions.

On October 19, 2018, the first GDPR sanction was issued by the Portuguese Data Protection Authorities to a Portuguese hospital which received a €400,000 fine for failing to comply with confidentiality and minimisation of data principles.

In January 2019 the French data protection authority issued a 50 million euros fine to Google for failing to comply with the transparency and legal basis requirements. To date, this is the largest GDPR sanction. For more clarity regarding the modernisation of the applicable data protection regulations, please find below a GDPR timeline. This timeline allows for a better understanding of transition period for the compliance of the various entities processing data and the first sanctions imposed under the GDPR.

For more information on sanctions issued by Member States' data protection authorities, please consult the comparative table available in **Appendix 1**[5]- **GDPR 1 year - Table of sanctions in the European Union**.



[5] Please note that this list is current as of June 2019 and is not exhaustive and only concerns sanctions made public by the supervisory authorities.

The GDPR also strengthens EU citizens' rights. Indeed, it provides for:

- **Clearer information** about the processing of their personal data;
- **New rights** to be exercised;
- **Higher sanctions** to be applied in case of breaches, etc.

Finally, the GDPR contains requirements to companies such as the **appointment of a Data Protection Officer** (hereafter, "**DPO**"), the respect for **accountability**[1] or the "**privacy by design/by default" principles**, etc.

4 | FUNDAMENTAL PRINCIPLES OF THE GDPR

The scope of the GDPR is very broad in practice and concerns all organisations that hold or use personal data.

Indeed, since 25 May 2018, the GDPR applies to all organisations, as long as they process personal data (**material scope**), whether they are established in the EU or outside the EU (**territorial scope**).

4.1 | MATERIAL SCOPE[6]

The GDPR is applicable to personal data processing completely or partly processed by automated means, such as, for instance, processing carried out with the use of computers containing digital databases.

Please note that the GDPR does not apply to the processing of personal data carried out in the course of activity which falls outside the scope of Union Law by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (that is activities relating to common foreign and security policy which are subject to specific rules and procedures), or by natural person in the course of a purely personal or household activity.

[6] Article 2 of the GDPR – material scope

4.2 | TERRITORIAL SCOPE[7]

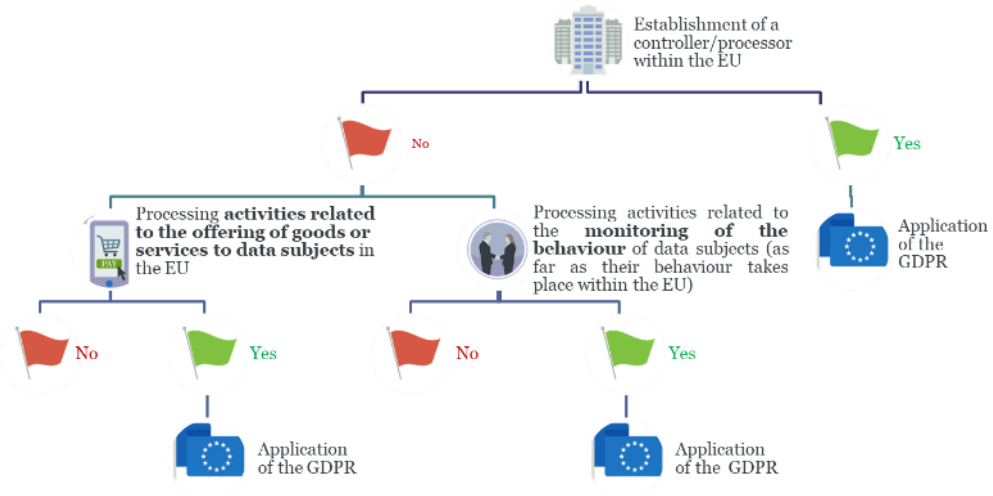
The GDPR applies in all cases where there is a processing of personal data in the context of the activities of a controller or a processor which **has an establishment within the EU**, regardless of whether the processing takes place within the European Union or not.

If there is **no** such **establishment** within the European Union, the GDPR may also apply in two types of situations:

1. Where the processing activities are **related to the offering of good and services** to data subjects who are **in the European Union**; or
2. Where the processing activities are **related to the monitoring of the data subject's behaviour** (as far as it takes place **within the European Union**).

> *Ex: A public safety provider established in Germany which processes personal data within the European Union in order to handle an emergency as fast as possible would be subject to the GDPR.*

If none of the above-mentioned conditions are met, the GDPR does not apply to the situation at stake. Please see schematic below that synthetises the territorial scope criteria:



Practical example - Is an emergency service subject to the GDPR?

An emergency service, located or not within the EU, aiming at providing persons in the European Union with emergency services, processes their personal data for this purpose

Therefore, it **is** subject to the GDPR.

[7] Article 3 of the GDPR – territorial scope

4.3 | MAIN DEFINITIONS OF THE GDPR

Article 4 of the GDPR provides definitions concerning the fundamental concepts concerning the GDPR such as personal data, data subject and processing.

i. Personal data (article 4.1 GDPR)

Personal data means "*any information relating to an identified or identifiable natural person*" (hereafter, "**data subject**").

Examples of Personal data processed by public safety organisations:

- Name
- Postal address
- Phone number
- E-mail address
- Geolocation data
- Heath data
- Photo, video
- IP address
- Etc.

ii. Data subject (article 4.1 GDPR)

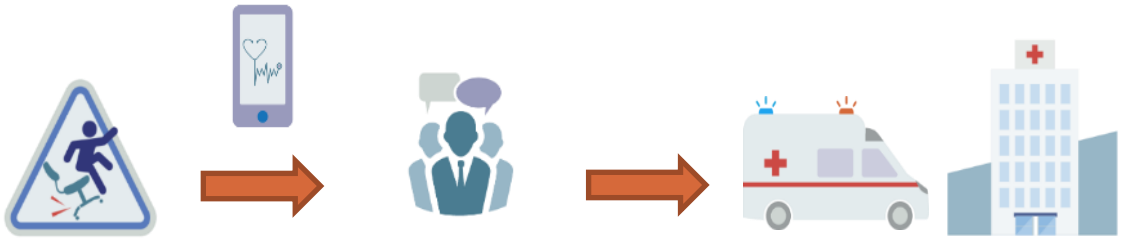
An identifiable natural person is one who can be "*identified, directly or indirectly, in particular by reference to an identifier".*

Examples of Data subjects involved in data processing carried out by public safety organisations:

- Persons in emergency situations
- Persons calling emergency call centres
- Staff of emergency centres
- Etc.

iii. Processing (article 4.2 GDPR)

Personal data 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 making available, alignment or combination, restriction, erasure or destruction*".



Emergency

Emergency call centre

Emergency services

For example:

A person in a situation of emergency would call an emergency call centre (by providing personal data for instance, his/her name, phone number, address etc.) that would process its personal data by recording the conversation in order to obtain information about the symptoms and the location of this person and send emergency services accordingly.

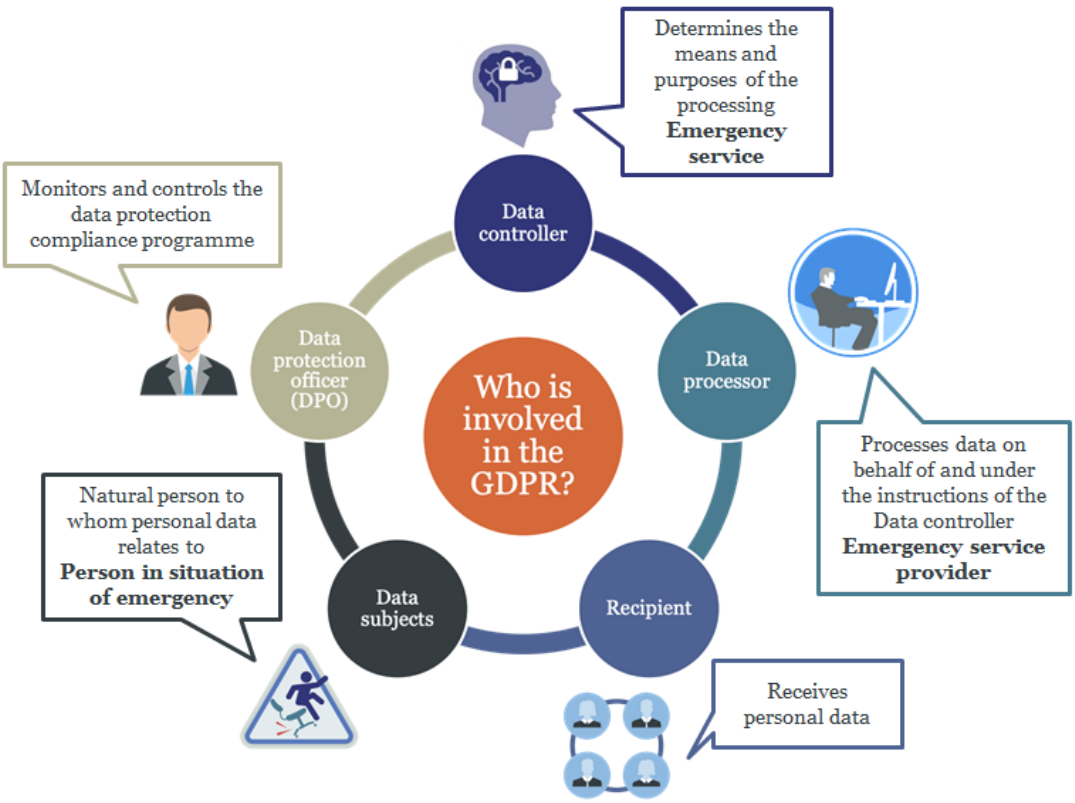
4.4 | ACTORS OF THE GDPR

The following persons are concerned and directly involved by the implementation of the GDPR:

- The **Data controller** is "*determin*[ing] *the purposes and means of the processing of personal data*".
- The **Data processor** is "*process*[ing] *personal data on behalf of the controller*".

  For instance, the data processor can be an emergency service provider.

- The **Recipient** is the person "*to which the personal data are disclosed, whether a third party or not*". The recipient receives the personal data at stake.
- The **Data subjects** are the person in situation of emergency.
- The **DPO** is the person monitoring and controlling the compliance of data controllers and processors with regards to the data protection regulation.



4.5 | COMMON BELIEFS AND MISUNDERSTANDINGS ABOUT THE GDPR

Be careful! There are some common beliefs and misunderstandings about the GDPR.

"**I am not concerned by the GDPR because**"

- ✖ *… I only have a paper file, I don't keep any personal data on my computer*
- ✖ *… I don't process any personal data, it is done by my service provider*
- ✖ *… I just read and consult the information*
- ✖ *… I don't use any software, only an Excel file or a Word document*
- ✖ *… I only scan the document and record it on my computer*
- ✖ *… I don't collect any sensitive or privacy-invasive data*
- ✖ *… I don't collect any first and last name*
- ✖ *… I only collect financial data*
- ✖ *… I only collect technical data (IP address, URL, connection data, etc...)*
- ✖ *… I anonymise data, since I only use a number/code*
- ✖ *... I am a public safety organisation*
- ✖ *…I am sure there is an exemption for my situation*

It is **common to believe that the GDPR would not apply** in cases where no electronic files are kept, where the information is only read and consulted, where only Excel files or Word documents are used, where sensitive personal data collected only consists in technical data, or where the data is believably anonymised but not sufficiently, and so on.

However, the wide article 4 GDPR-definition provides a broad definition for the processing of personal data which encompasses all these situations.

5 | BREACHES OF THE GDPR: FOCUS ON PUBLIC SAFETY ORGANISATIONS

Since the entry into force of the GDPR, stronger administrative fines can be imposed by any State-member's DPA. In this respect, fines must be effective, proportionate and dissuasive. They may be imposed on controllers as well as processors.

The legal risks relating to non-compliance with the GDPR obligations are such as to engage the **entity's liability**.

The table overleaf summarises all the sanctions that may be imposed in the event of failure to comply with the GDPR's obligations and non-compliance with the principles relating to the processing of personal data.

<table>
<tr><td>Criminal sanctions</td><td colspan="2">Criminal sanctions might be issued.

For instance, in France, failure to comply with the "Informatique et Libertés" Law obligations may result in a fine of up to €300,000 and 5 years' imprisonment (articles 226-16 to 226-24 of the French Criminal Code).</td></tr>
<tr><td rowspan="3">Administrative sanctions</td><td colspan="2">Pursuant to article 58 of the GDPR, the European Data protection authorities are entitled to:

• Issue a call to order;
• Order to ensure compliance of the processing activity, including under constraint;
• Temporarily or permanently limit a processing activity;
• Suspend data flows;
• Order to satisfy demands for the exercise of the rights of data subjects, including under constraint;
• Impose an administrative fine (see hereafter).</td></tr>
<tr><td>For infringements such as:

• Unfair processing of personal data;
• Lack of information notice;
• Absence of consent from individuals;
• Non-compliance with individuals' rights of access etc.;
• Non-compliance with rules on transfers of personal data to third countries;
• Non-compliance with a DPA's injunction.</td><td>Data protection authorities are entitled to impose a sanction of up to:

• €20 million; or
• 4% of worldwide annual turnover, whichever is higher (article 83 GDPR).</td></tr>
<tr><td>For infringements such as failure to:

• Keep the data processing activities record;
• Notify data breaches;
• Ensure security of personal data,
• Implement Privacy by design,
• Conduct PIAs,
• Designate a DPO.</td><td>Data protection authorities are entitled to impose a sanction of up to:

• €10 million; or
• 2% of worldwide annual turnover, whichever is higher (article 83 GDPR).</td></tr>
</table>

In addition, please note that Article 80 of the GDPR provides for the representation of data subjects by any entity active in the field of personal data protection[8]. They may be represented by a third party body in order to defend their rights (ex: data protection association: *None of Your Business, Quadrature du net)*.

A GDPR sanction may consequently harm the image and reputation of the sanctioned entity.

There are several examples of French companies for which the CNIL issued a public sanction and that have suffered damage to their images:

- **Acadomia** is a French company specialised in personalised tutoring programs for kids and students. In 2010, the CNIL published a deliberation showing irregularities in the management of personal data by the company. Clients and tutors' files contained injurious or prejudicial messages. Acadomia subsequently received a public warning from the CNIL and its release in the press seriously harmed the company's image.

- **Boulanger** is a French company specialised in the sale of electronic devices and house appliances. In 2015, the CNIL discovered very prejudicial and heinous messages towards customers in the customer service application's comments area. The CNIL publicly summoned Boulanger to become compliant with the regulation within 3 months, and even published a tweet on its institutional Twitter account!

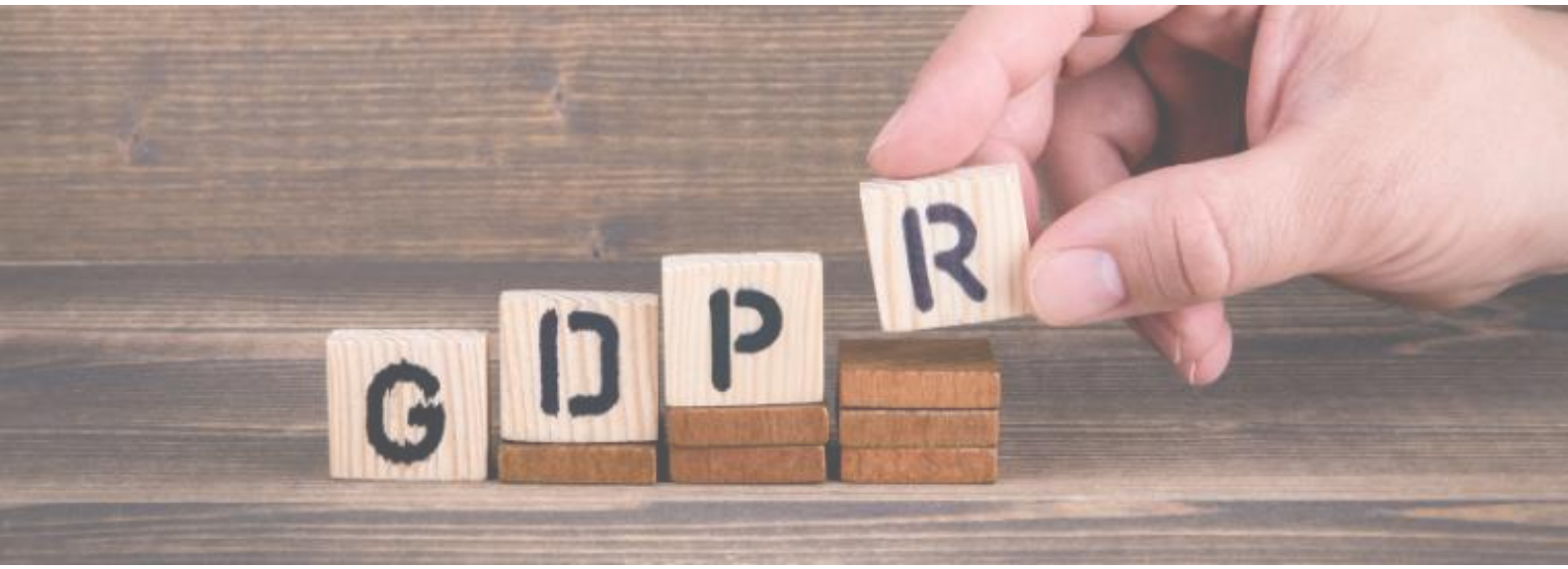
Practical example

Using the example of an application whose purpose would be to help contact emergency services in case of a major event and disaster management, the emergency service provider could face sanctions in cases of violations pertaining to:

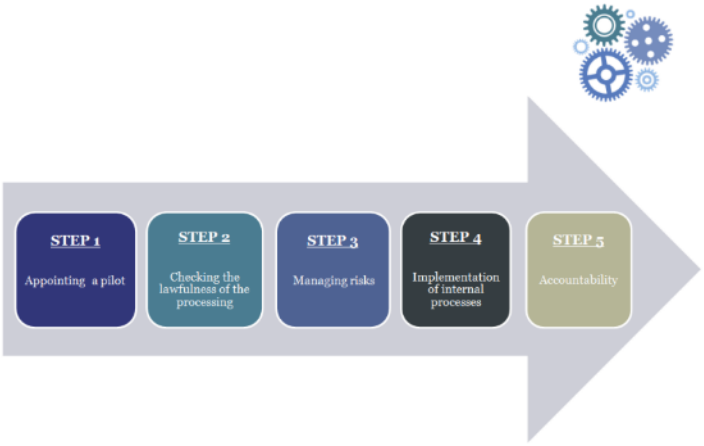
- The application security's vulnerability (that is, if the security measures put in place were to be ineffective or insufficient),
- Personal data breaches,
- A failure to notify personal data to the competent Data Protection Authority
- …

In such cases, sanctions could go **up to 2% of the worldwide annual turnover or €10 million.**

[8] "*The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf […]*"



6 | RECOMMENDATIONS FOR PUBLIC SAFETY ORGANISATIONS' COMPLIANCE WITH GDPR



The steps of compliance of the different organisations with the GDPR can be summarised in **5 steps** as follows:

1. Appointing a pilot/a data protection officer
2. Checking the lawfulness of the processing
3. Managing risks
4. Implementing internal processes
5. Applying the accountability principle

6.1 | APPOINTING A PILOT/DATA PROTECTION OFFICER (DPO)

What is a pilot/DPO?

A pilot means a person **responsible for the implementation of the compliance programme**.

He/she is in charge of implementing documentation, guidelines, processes, etc. to ensure optimal protection of personal data within the organisation collecting and processing personal data.

Most of the time, the pilot will be appointed as a **Data Protection Officer**.

The DPO can be **internal** or **external** to the organisation. However, he must be **easily reachable**/contactable and available through a generic address such as for instance.

Who is concerned by the appointment of a DPO?

According to article 37 of the GDPR, the following are concerned by the obligation to appoint a DPO:

- Both **public bodies** and **authorities**;
- **Private companies:**
    - When their **core activities** consist of **large-scale processing** operations requiring **regular and systematic monitoring of data subjects**;
    - When their **core activities** consist of **large-scale processing of sensitive data** or data relating to convictions and offences;

Whenever they are data **controllers** or data **processors**.

Please note that for companies that do not meet these criteria, the appointment of a DPO is still **strongly recommended** as it is an important indicator of compliance and an identified contact point for authorities and data subjects.

Practical example: Is the appointment of a DPO mandatory for emergency service providers?

An emergency service provider offering a software/application to be used to assist populations in the event of a major disaster would, in most cases, process personal data on a **large scale,** most likely **including sensitive data**. As it satisfies criteria of article 37 of the GDPR, the emergency service provider would need to appoint a DPO.

In any case, appointing a DPO helps ensure GDPR compliance (i.e respect of the accountability principle) and gain users, clients, providers and public bodies' trust.

What are the DPO's main missions?

The DPO will mainly **monitor** the GDPR compliance of the entity, for example by conducting audits to make sure that the GDPR requirements are satisfied, **informing and advising** the data controller or processor, for example by spotting unclear or vague purposes of processing, or advising that a PIA be carried out where necessary.

The DPO will also **be a contact point** for the supervisory authorities and needs to **cooperate** with the authority.

Who can be a DPO?

The DPO can be either a **member of the** data controller or processor's **staff** or a **person from outside** the organisation.

Thus, professional qualifications, a special knowledge of personal data and the ability to carry out the DPO's missions are the criteria to focus on while recruiting.

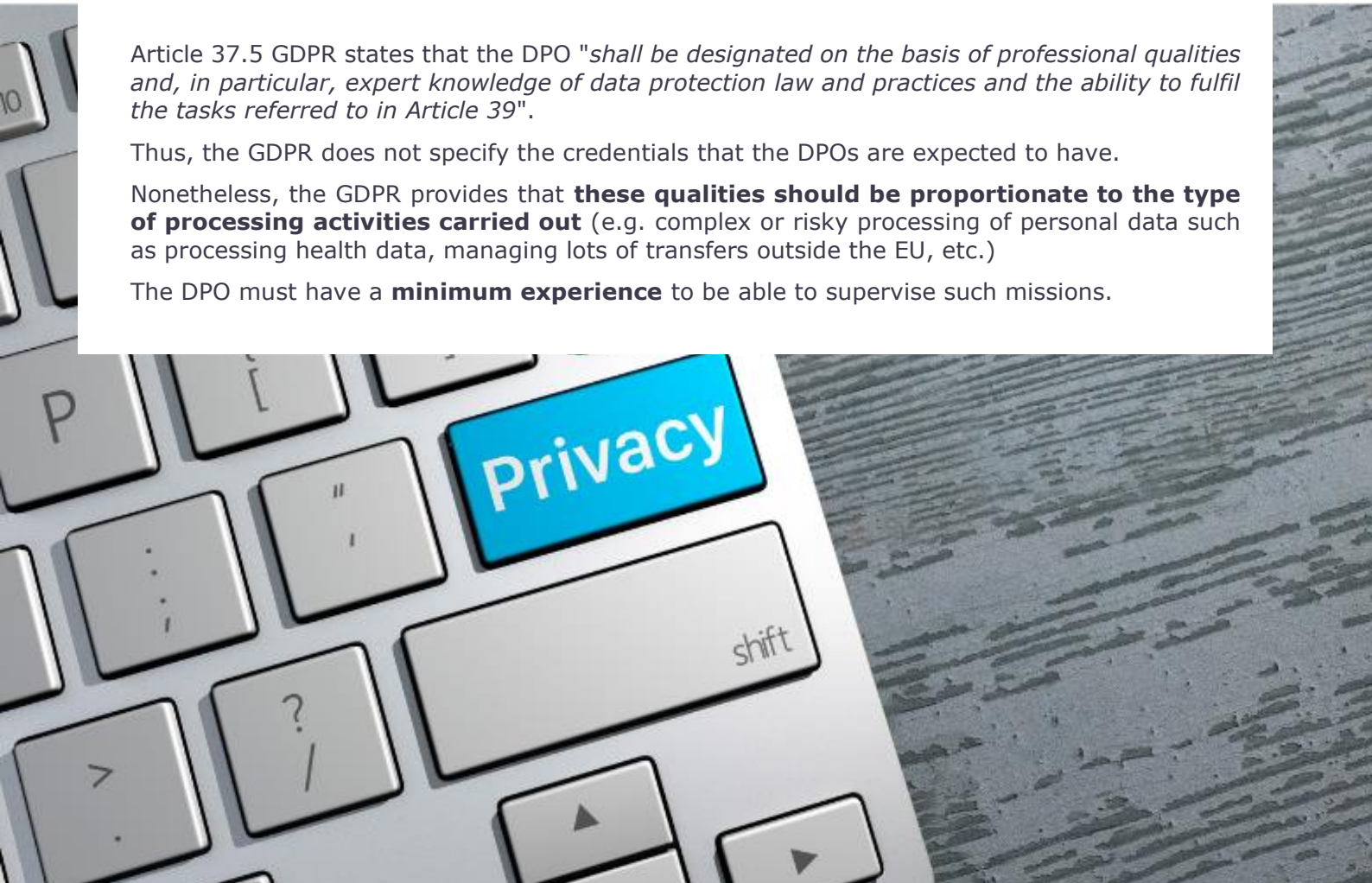
What shall be the DPO's qualifications?

Article 37.5 GDPR states that the DPO "*shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39*".

Thus, the GDPR does not specify the credentials that the DPOs are expected to have.

Nonetheless, the GDPR provides that **these qualities should be proportionate to the type of processing activities carried out** (e.g. complex or risky processing of personal data such as processing health data, managing lots of transfers outside the EU, etc.)

The DPO must have a **minimum experience** to be able to supervise such missions.



Absence of conflict of interest for the DPO

Article 38.6 of the GDPR states that "*the DPO may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests*".

According to the WP29[9], this provision means that the DPO **cannot perform any function leading to the determination of the purposes and means of the processing**. This will be avoided by deploying specific internal actions to anticipate conflicts of interest according to the business, size and structure of the entity in question.

Thereupon, on October 20, 2016, the Bavarian DPA (Bayerisches Landesamt für Datenschutzaufsicht) issued a non-public fine to a company that had appointed an IT manager as DPO. The find was issued for lack of independence of the DPO towards the purposes and means of processing.

From a practical point of view, it is frequent that DPOs are **attached to the Board or to the Compliance Department** in order to independently monitor the appropriate GDPR compliance measures.

DPO governance

The DPO governance is an ongoing and dynamic process.

Thus, the compliance governance must be **organised**: resources and internal organisation are required for it to function properly. Plus, the DPO needs to get feedback.

Awareness among top management and employees needs to be raised, by providing training sessions and ensuring that fundamental personal data protection principles are internally implemented.

Eventually, procedures must be implemented through the adoption of **internal rules** and through the **documentation** of any data protection steps and processes implemented.

The DPO must take into account the accountability obligation.

In order to fulfil the accountability principle in the long term, the DPO must be invited to:

- **Participate in important internal meetings related to decision-making** in terms of personal data protection;
- Be **involved in every matter** in relation to innovative projects, projects in progress or projects requiring a software change;
- **Support any personal data-related matter**, especially for a **PIA** (Privacy Impact Assessment);
- **Carry out and keep up to date a record of processing activities** reflecting the personal data processing operation.

7.1.1 What is the procedure for appointing a DPO?

[9] WP 243 rev.01 "Guidelines on Data Protection Officers (DPOs), adopted on 13 December 2016, as last revised and adopted on 5 avril 2017

What is the procedure for appointing a DPO?

When appointing a DPO, the public safety organisation should make sure that the candidate:

- Has sufficient **legal knowledge** (GDPR, local data protection laws, DPA's way of working, etc.),
- Can easily **handle training sessions, audits** and **implementation of documentation**,
- Is able to **provide advice** and **recommendations** regarding data protection (e.g. for a PIA),
- Is able to **act as a contact point** for the DPA and the data subjects,
- Will be **fully involved** in all data protection matters of the company.

Be careful! DPO appointing procedures are not equal between the different data protection authorities in Europe. Each authority has its own mechanism and form (online for most of them) to officially appoint DPOs.

Some examples:

Country	Mecanism	Practical information
France	Form to be filled out online on the CNIL website	**https://www.cnil.fr/fr/designation-dpo**
Luxembourg	Form to be filled in and sent to the CNPD by email	**declarationDPO@cnpd.lu**
Belgium	Form to be filled out and submitted via the APDInternet portal	**https://www.autoriteprotectiondonnees.be/formulaire-de-communication-des-coordonnees-du-delegue-a-la-protection-des-donnees**

6.2 | CHECKING THE LAWFULNESS OF THE PROCESSING

Legal basis

Before processing any personal data, the data controller must determine a legal basis for the processing. This must be carefully chosen and documented. Article 6 of the GDPR provides for **6 legal bases**. At least one of them must apply when processing personal data:

a) **Consent**: the data subject has given clear consent;

b) **Contract**: the processing of personal data is necessary to respect the contract concluded with the data subject;

c) **Legal obligation**: the processing of personal data is carried out to comply with legal obligations;

d) **Vital interests**: the processing is necessary to protect the data subject's vital interests;

e) **Public task**: the processing of personal data is necessary for the data controller to perform a task of public interest;

f) **Legitimate interest**: the processing is necessary for the data controller's legitimate interests or the legitimate interests of a third party.

If no lawful basis applies to the processing of personal data, the latter will be considered as unlawful. Consequently, data subjects will have the right to request the erasure of personal data, since it has been unlawfully processed.

In accordance with articles 13 and 14 of the GDPR, data subjects have the right to be informed about the legal processing of their personal data. This is why the lawful basis must be mentioned in the public safety organisation's privacy policy.

6.3 | FOCUS ON ONE SPECIFIC LEGAL BASIS: VITAL INTERESTS

This legal basis seems to be the most appropriate for the processing of personal data by public security organisations.

The notion of vital interests covers interests that are absolutely essential to data subjects' lives according to:

- **Article 6.1(d) GDPR**: "*processing is necessary in order to protect the vital interests of the data subject or of another natural person*".
- **Recital 46**

- **GDPR**: "*the processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis*".

Practical example: in an emergency situation

A phone call (and potential recorded images) in an emergency situation will result in the **processing of sensitive data based on the protection of vital interests of the data subject**. Indeed, the processing will enable the emergency call centre to react rapidly and take the necessary steps in rescuing the data subject.

Following the call, the transmission of the data subject's information results in the processing of sensitive data based on the same legal basis. It will be essential for the emergency call centre to use such data in order to transmit it to the emergency services so that they have accurate information about health status and location of the data subject.

6.4 | FOCUS ON SENSITIVE DATA PROCESSING ACTIVITIES

It is important to be extremely cautious in cases where **sensitive data** (such as health data or data relating to criminal convictions or offences) are being processed. **Additional caution will be required for processing such categories of data.**

In this respect, data concerning health means "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*"[10].

Examples of health data:

- Information collected for the purpose of receiving health care services;
- Information obtained when examining a part of the body (body substance, biological and genetic samples);
- Information about a disease.

[10] Article 4 of the GDPR

6.6 | GDPR KEY PRINCIPLES

Legal basis	An **appropriate legal basis** needs to be identified prior to any personal data processing activity. *Example: the legal basis could be the protection of the data subjects' vital interests.*
Fairness	Personal data should always be **processed in a fair manner,** that is to say in ways that it would reasonably be expected to be processed.
Transparency	Data subjects must always **receive proper and clear information** about the processing of their personal data: • The identified legal basis of such processing, • Its purposes, • Its conservation period, • The identity of the data controller and processor, • The identity of the DPO if applicable, • The transfers of personal data outside the EU along with the countries concerned by such transfers and the guarantees thereof… The data subject must fully understand the extent of their personal data processing.
Purpose limitation	Article 5.1(b) GDPR provides that "*personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". Prior to the processing of personal data, the data controller should answer 3 questions in order to determine whether he/she complies with the purpose limitation principle: • **Why** do such data need to be collected? • Are **transparency principles** fully respected? • Are **documentation obligations** properly fulfilled?
Data minimisation	Article 5.1(c) GDPR provides that "*personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)".* The data controller will have to make sure that: • Only personal data that are **truly necessary** for the purposes specified are collected; • All personal data that are not absolutely necessary are deleted;

	• Personal data in the database are periodically reviewed to ensure the data are still useful and necessary.
Accuracy	According to article 5.1(d) GDPR, "*personal data shall 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*". The data controller will have to verify, along periodic reviews of the database, that personal data are still **accurate** and **up to date**. If it is not the case, such data will have to be **deleted immediately**.
Storage limitation	According to article 5.1(e) GDPR, "*personal data shall 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".* An **identified or identifiable retention period** for personal data being processed is required. The GDPR does not provide any fixed data retention periods. The data controller will therefore be **in charge of setting retention periods**, which can be based on the purposes of the processing, legal or regulatory requirements, or relevant industry standards or guidelines. It is essential that a **proportionate approach** be used for the determination of the retention period so as to balance the impact of data retention and of the data subject's privacy. An **emergency service** (data controller) will have to answer two types of questions in order to set retention periods accordingly: • How long are personal data necessary to the management of emergency situations? • Is the data still needed after the emergency situation has been taken care of (for purposes of litigation or police investigation for example)?
Security	Article 5.1(f) GDPR provides that personal data shall be "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*". Plus, the GDPR requires that the processing has an **appropriate level of security** to prevent potential risks. *Technical and organisational security measures:*

- **Encryption** (article 32 GDPR)

Consists in encrypting data using cryptographic algorithm: only key holder will be able to decrypt them.

- **Pseudonymisation** (articles 4.5 and 32 GDPR)

Consists in replacing one or more attributes of a data set with random identifiers (e.g. replacing names with a number). The data remains personal data. However, pseudonymisation of such data will eliminate the need to notify in the event of a potential security breach.

- **Anonymisation** (recital 26 GDPR)

Personal data will be made anonymous by transforming them in such a way that "*the data subject is not or no longer identifiable*", according to recital 26 GDPR. Risks of re-identification will have to be prevented.

Ensure the security of data processing activities

Data controllers and processors will have to conduct **regular audits** to ensure that the procedures they have implemented are being respected. This will be an additional indication that the data controller is trying to protect personal data in the best way possible.

The audit may focus on:

- The **types of personal data** that are being processed and whether they are **processed electronically or on paper**;
- The **justification** that can be given to the **collection** of personal data;
- The **purposes** for which the data are being collected;
- **Who can access** personal data and whether these persons are authorised to have access to data;
- Whether personal data are **secure**.

MANAGING RISKS

In order to manage personal data protection risks, it is necessary to carry out a privacy impact assessment prior to the implementation of processing at risk.

What is a Privacy Impact Assessment (PIA)?

A Privacy Impact Assessment (hereafter, "**PIA**") is an essential tool for the accountability of data controllers. It not only helps them ensure that certain processing operations of personal data do not generate high risks for personal data, but it also demonstrates their compliance with the GDPR.

The establishment of a PIA is **mandatory** to be able to operate processing likely to generate high risks for the personal data of the data subjects. There are **3 steps** to follow:

- **Describing** the processing in order to analyse its inherent risks (description of the processing);
- **Identifying** security risks to evaluate their severity and potential impacts on the rights and freedoms of data subjects (security risks);
- **Addressing** the risks to determine if such risks are acceptable given the technical and organisational measures foreseen (legal assessment).

When is my PIA needed?

A PIA must be done prior to any type of processing that is "*likely to result in **a high risk** to the rights and freedoms of natural persons"* according to article 35.1 GDPR.

Further on, the article provides for non-exhaustive examples of situations in which data processing is likely to present high risks, in particular in cases of:

- **Systematic and extensive evaluation of personal aspects** relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- Processing on a **large scale** of **special categories** of data referred to in Article 9.1 or of personal data relating to criminal convictions and offences referred to in Article 10; *or*
- **Systematic monitoring** of a publicly accessible area on a large scale.

Article 35.1 and Recitals 90 and 93 of the GDPR specify that the PIA has to be carried out **prior** to processing personal data. It would be advisable that the PIA be carried out when designing the processing operation.

Some projects are so risky that the PIA will need to be continuous and will **require updates** as the project progresses.

Is my processing subject to a PIA?

Not all processing operations are automatically subject to an impact assessment. To determine whether the processing of personal data should be submitted, it is necessary to:

- ensure that the processing of personal data is not part of the processing operations for which a PIA is not required (a);

-then, look at the list of the supervisory authority concerning processing operations subject to mandatory impact assessment (b), and look at the criteria of the WP29 guidelines (c);

-finally, in case of doubt as to the need to conduct an impact assessment, it is appropriate in any case to carry out an impact assessment (d).

a) Article 35 GDPR provides for a list of processing for which a PIA is not required

It is not necessary to carry out a PIA when the processing is:

- Mandatory, for instance, when the processing of personal data is necessary to comply with a legal obligation to which the controller is subject
- Not likely to result in a high risk to the rights and freedoms of natural persons
- Necessary for the performance of a task in the public interest or subject to the public authority entrusted to it

- Already subject to a prior impact assessment
- Included on the optional list established by the supervisory authority of processing operations for which no PIA is required

b) List published by the Data Protection Authority for mandatory PIA

Data protection authorities may publish lists of processing operations for which a PIA will be optional or for which a PIA will be mandatory.

For instance, on November 6, 2018 the French Data Protection Authority (the CNIL) published guidelines and a non-exhaustive list of processing operations subject to the establishment of a PIA. The final list was adopted on October 11[11] after the European Data Protection Board (hereinafter: "EDPB") released an opinion. The CNIL gave examples of processing operations which would require a PIA such as whistleblowing systems, video surveillance systems, profiling processing, large scale processing of geolocation data, etc.

c) The WP 29 guidelines on Data Protection Impact Assessment[12]and example:

The WP 29 adopted guidelines on 4 April 2017 and revised them on 4 October 2017. They provide some criteria for conducting an impact assessment.

1. Evaluating scoring
2. Automated decision making with legal or similar significant effect
3. Systematic monitoring
4. Sensitive data
5. Data processed on large scale
6. Datasets that have been matched or combined
7. Data concerning vulnerable data subjects
8. Innovating use or applying new technological or organisational solutions
9. Data transfers across borders outside the European Union
10. Prevents data subjects from exercising a right or using a service or a contract

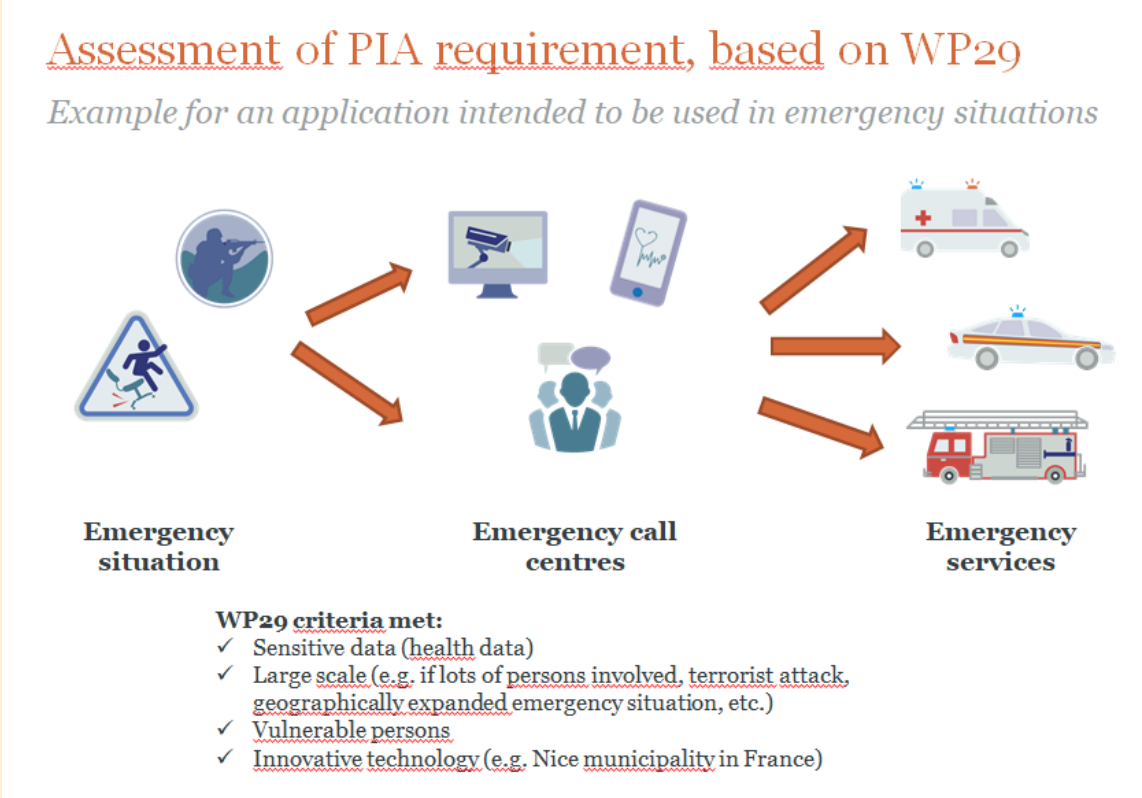
If only one criterion is met, a PIA is not mandatory, but it is still highly recommended. If more than one criterion is met, a PIA is mandatory.

[11] Déliberation n°2019-327 October 11 2018, adopting the list of types of processing operations for which a data protection impact assessment is required. In French: https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise-v2.pdf

[12] WP 248, « *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk*" for the purposes of Regulations 2016/679, 4 April 2017 as last revised and adopted on 4 October 2017

Practical example: assessment of a PIA requirement based on WP 29

Example for an application intended to be used in emergency situations



Practical example for a mobile application enabling contact with emergency services in emergency situations.

In case of an emergency situation, the application will serve as an intermediate with emergency call centres by processing people's personal data, which will then be transferred to emergency services so that they can provide appropriate assistance.

In this case scenario several WP29 criteria are met:

- There is processing of sensitive data (health data)
- Data are processed on a large scale: Indeed, if the emergency situation is a major one, such as a result of a terrorist attack or natural disaster, personal data of many people are likely to be processed.
- Vulnerable persons may be concerned by the emergency (underage or elderly people)
- Innovative technology may be used to process personal data (i.e. biometric data, facial recognition etc.)

How to carry out a PIA?

A PIA should be carried out according to the **following steps**:

1. **Identifying the necessity to carry out a PIA** by referring to different sources (GDPR, WP29 guidelines, DPAs lists, etc.);
2. **Describing the processing and determining** the purposes for which such processing are operated;
3. **Assessing the proportionality of the processing**;
4. **Identifying and assessing** the potential risks of such processing for the rights and freedoms of data subjects;
5. **Identifying technical and organisational** measures to mitigate risks and make them acceptable;
6. **Integrating outcomes** into an action plan to be able to predict a maximum of events;
7. **Involving the DPO,** able to provide guidance and monitor compliance;
8. **Assessing the necessity of the DPA's consultation**.

The CNIL put in place a **PIA software**[13], aiming at providing guidance to data controllers for demonstrating compliance with the GDPR.

PIA Software

This PIA Tool is designed around three parts:

- A didactic interface to carry out PIAs, which clearly unfolds the PIA methodology step by step and ensures a quick understanding of the risks involved with the data processing at stake;
- A legal and technical knowledge base, which enables legal points ensuring the lawfulness of the processing and the rights of the data subjects. The data are extracted from the GDPR, the PIA guides and the Security Guide from the CNIL. The contents displayed are adapted to the processing concerned;

A modular tool, which enables users to customise the contents to specific needs or business sectors. It is published under a free license as to make it possible to incorporate it into tools used by the organisation.

[13] Available into 18 languages - https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

FURTHER COMMENTS

Is the consultation of the supervisory authority required?

When conducting a PIA, it is not mandatory to consult the DPA. The latter should only be consulted if a high risk, which cannot be reduced by technical or organisational measures, is identified in the PIA.

The opportunity to consult the authority should be internally assessed and discussed.

Benefits of conducting a PIA

Carrying out a PIA can have many positive impacts and effects on the organisation as well as on data subjects:

- It helps reduce data protection risks;
- It is a way to ensure and demonstrate the organisation's compliance with the GDPR;
- It enables the organisation to respect the Privacy by design principle;
- It increases data subjects' trust in the organisation thanks to the improvement of communication on data protection issues.

Should the PIA be published?

The PIA does not need to be published. However, it is recommended to do so as it helps demonstrate accountability and transparency principles. This may also be particularly valuable to public authorities which intend on carrying out a PIA. There is no need to integrate the whole assessment in the published PIA, or to indicate all security measures and commercially sensitive information. A summary of the PIA is sufficient.

IMPLEMENTATION OF INTERNAL PROCEDURES WITHIN PUBLIC SAFETY ORGANISATION

Three internal procedures can be put in place, in order to comply with the GDPR namely:

1. Procedures relating to data breach;
2. Procedures for data transfers;
3. Procedure relating to the management of the data subject's rights.

Managing data breach

Article 4.12 of the GDPR defines a personal data breach as a "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*".

The data controller has the obligation to notify any personal data breach to the supervisory authority within 72 hours. If the notification is not made within 72 hours, the controller must give the reasons for the delay in the notification.

As for the data processor, he/she must notify the breach to the controller as soon as possible and "*without undue delay*" after having become aware of it, according to article 33 of the GDPR.

Where necessary, the controller must then inform the data subjects affected by the breach without undue delay. This will be necessary if the breach is likely to result in a high risk to the rights and freedoms of natural persons (article 34 GDPR).

The communication to the data subjects shall be made in clear and plain language and shall contain at least information about the probable consequences of the breach; a contact point where more information can be obtained (such as the DPO); *and* measures taken or proposed to be taken to address the personal breach. For example, the data subjects could be advised to change their account passwords.

Internal procedures need to be implemented in this regard.

There are a few precautions to take to be prepared for a potential personal data breach. Organisations need to make sure that they are able to recognise a data breach, but also to prepare a response in advance and an action plan in case a data breach actually occurs. Also, the staff must be trained and able to report security incidents to the appropriate person or team in the organisation.

In the event of a personal data breach, it will be very important to know which relevant supervisory authority should be notified, but also to have a proper process or procedure in place to respond to the breach.

Remember to make sure that as a data controller, an organisation should be able to notify the breach within 72 hours and there must be a process to inform data subjects when applicable.

In the case of a personal data breach within the emergency services, the emergency service provider (data processor) would have to notify the emergency service without undue delay after becoming aware of the breach to the data controller, in accordance with article 33 GDPR.

Emergency service provider (data processor)

Managing data transfers

Data transfers are strictly regulated under the GDPR. In principle, transferring personal data outside the EU (to third countries or international organisations) is prohibited under article 44 of the GDPR.

However, if the recipient country is recognised by the European Commission as ensuring an **adequate level of protection**, cross-border transfers outside the EU will be allowed. The European Commission has made a list of countries which have been recognised as having such a level of protection so far, including: *Andorra, Argentina, Canada, Isle of Man, Faro Islands, Israel, Japan, Jersey, New Zealand, Switzerland, and Uruguay*.

If this first exception is not met, it is still possible to proceed with such transfers outside the EU if appropriate safeguards are provided through **standard contractual clauses** (in the form of templates validated by the European Commission) or **binding corporate rules** (BCR which resemble codes of conduct and only apply to intra-group transfers).

Finally, if the second exception cannot be applied to the transfer at stake, there is an exhaustive list of **derogations** to the prohibition of data transfers outside the EU in article 49 of the GPPR, such as where:

- The data subject has **explicitly consented** to the proposed transfer, after having been informed of the **possible risks** or such transfers;
- The transfer is **necessary for the performance of a contract** between the data subject and the controller or the implementation of pre-contractual measures;
- The transfer **is necessary for the conclusion or performance of a contract concluded in the interest of the data subject** between the controller and another natural or legal person;
- The transfer is necessary for **important reasons of public interest**;
- The transfer is necessary for the establishment, **exercise or defence of legal claims**;
- The transfer is necessary in order to protect the **vital interests of the data subject;**
- The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which **is open to consultation** either by the public in general or by any person who can demonstrate a **legitimate interest.**

In any case, the data controller must **inform the data subject** that transfers of his/her personal data will take place (and give them information about which countries the data will be transferred to, as well as which types of guarantees the transfers are based on).

The controller must also mention such transfers in the **record of processing** activities in accordance with the accountability principle.

Practical example: cross-border processing operations

A cloud hosting personal data processed by an emergency centre or a service provider based outside the EU.

The data would therefore need to be transferred from the cloud (in the EU) to the service provider (outside the EU). Such a transfer would be lawful if it is made in compliance with the GDPR requirements in this matter.

In particular, personal data transfers relating to emergency services are likely to be lawful under the article 49.1(f) derogation.

Managing data subjects' rights

Article 13 and 14 of the GDPR contain the obligation for the data controller to provide clear and complete information to data subjects about the processing of their personal data, and especially about their rights towards the personal data that is being processed.

The privacy notice regarding a processing operation must contain the following indications:

- The identity of the controller and the DPO (where applicable);
- The purposes of the processing operation;
- Legitimate interests of the processing operation, if any;
- The mandatory or optional nature of answers to the privacy notice;
- The possible consequences of a failure to reply;
- The recipients or categories of recipients of the personal data;
- The right of the data subject: data subjects have a right of access to their personal data, along with the rights of rectification, opposition, and deletion. They also have rights to the portability of their data, to limitation of their data, and to give instructions on the fate of their data postmortem;
- Data transfers, if applicable, and the countries which will receive the personal data, as well as the appropriate guarantees which justify the data transfers outside the EU;
- Data retention periods or criteria enabling the determination of such period.

Focus on data subjects' rights

All data subjects' rights must be taken into account by controllers and processors.

Therefore, the GDPR provides the data subjects with numerous rights such as:

- The right to be forgotten, which is linked to the obligation of transparency of the data controller
- The right of access of the data subject to his or her collected personal data
- The right to rectification of such data if it were to be inaccurate (this can be linked to the principles of accuracy and purpose limitation)
- The right to erasure of data which may not be accurate, or which may be unlawfully collected or processed (this can be linked to the principles of purpose limitation, data minimisation and storage limitation)
- The right to restrict processing
- The right to object to a processing of personal data
- Rights related to automated decision-making and profiling: data subjects have the right not to be subject to a solely automated decision-making process and require human intervention.

ACCOUNTABILITY

Demonstrating compliance with the GDPR is ensured by the principle of Accountability. Indeed, demonstrating compliance requires updating contracts, drafting internal procedures, taking into account the principle of Privacy by Design from the beginning of each processing operation and raising awareness among operational staff.

Contracts

According to article 28 of the GDPR, personal data processing by a **processor** shall be governed by a contract or other binding legal act that sets out:

- 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.

According to article 26 of the GDPR, where two or more controllers jointly determine the purposes and means of processing, they shall be **joint controllers** and determine their respective responsibilities, especially when it comes to the exercising of the rights of the data subject and their respective duties to provide information by means of an arrangement between them.

For instance, a contract is necessary between the data controller and the data processor when an emergency service (data controller) uses an application from a service provider (data processor) used to help contact and send emergency services.

In order to be GDPR compliant, the data controller must ensure that a written agreement is entered into if they choose to resort to a data processor. Such an agreement must stipulate the liabilities and responsibilities of both parties and it must be ensured that both understand the extent of these provisions.

Article 26 and 28 set out mandatory elements to include in such contracts. For example, a joint controllers' arrangement shall duly reflect the respective roles and relationships of the controllers towards the data subjects and may designate a contact point for data subjects, who must be able to exercise their rights under the GDPR. The respective responsibilities and duties of the joint controllers with regards to the exercising of those rights shall be provided for.

In a processor/controller relationship, the contract shall include several elements relating to:

Documented instructions	The processor processes personal data on documented instructions from the controller, including with regards to transfers of personal data to a third country or an international organisation.
Confidentiality	The processor ensures that the persons authorised to process the data respect confidentiality, either because they agreed to confidentiality or because they are subject to a statutory obligation of confidentiality.
Security measures	The processor must take all technical and organisational measures needed pursuant to article 32 of the GDPR.
Rules for subcontracting	The processor must comply with the conditions set out for engaging another processor (this cannot be done without prior specific or general written authorisation of the controller).
Assistance to the data controller	The data processor shall assist the data controller in ensuring compliance with its obligations of: • Security of the processing; • Notification of data breaches to the supervisory authority and the data subjects where applicable, *and* • Carrying out a PIA and consulting the authority when applicable.
Audit provisions	The processor shall contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
Restitution/deletion of data	The processor shall delete or return all personal data to the controller after the end of the provision of services relating to processing, at the choice of the controller.

POLICIES AND PROCEDURES

The GDPR requires data controllers to provide the following documents:

- Information notices
- Privacy policy
- PIA, if applicable
- Security policy
- Procedure for handling complaints and exercises of their rights by the data subjects
- Procedure for handling data breaches
- Data retention policy
- Contracts
- Record of processing activities
- Procedure/checklist for "Privacy by design"

FOCUS ON RECORDS OF PROCESSING ACTIVITIES (ARTICLE 30 OF THE GDPR)

Both data controller and data processor shall keep up to date a record of processing activities:

Content of the record hold by a data controller	Content of the record hold by a data processor
Name and contact details of: • The organisation; • Joint controllers; • Representative; • Data protection officer, if applicable.	Name and contact details of: • The organisation; • Controller on behalf of which the processor acts; • Representative; • Data protection officer, if applicable.
Purposes of the processing	Categories of processing carried out on behalf of each controller
Description of the categories of individuals and categories of personal data	N/A
Categories of recipients of personal data	N/A
Details of data transfers to third countries including documenting the transfer mechanism safeguards in place	
Retention periods	N/A
A description of the technical and organisational security measures	

Privacy by design

The GDPR requires technical and organisational measures to be put in place to implement the data protection principles and safeguard individual rights.

In essence, this means the entity has to integrate or "bake in" data protection into the processing activities and business practices, from the design stage right through the lifecycle.

The Information Commissioner's Office (ICO), the UK's DPA, provides an example of a Privacy by design checklist:

- ✓ We consider data protection issues as part of the design and implementation of systems, services, products and business practices;
- ✓ We make data protection an essential component of the core functionality of our processing systems and services;
- ✓ We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals;
- ✓ We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes;
- ✓ We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy;
- ✓ We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.

Raising awareness

It is very important to raise awareness among teams. To keep teams informed of data protection issues, it is possible to:

- Organise conferences, training sessions, e-learning, Lunch&Learn (learn over a lunch debate) etc.;
- Communicate memos and recommendations internally

7 | CONCLUSION

As a conclusion and in order to assist public safety organisations in bringing their processing into compliance with the GDPR, the following (indicative) checklist should be respected:

STEP 1 - DESIGNATE A COMPLIANCE PILOT/DPO

It seems necessary to appoint a referent or DPO insofar as this is the contact point with the control authorities.

- ☐ Designate a pilot/DPO
- ☐ Choice of a DPO in charge of managing compliance with the GDPR (give reasons in the absence of appointment of the DPO)
- ☐ Internalise or outsource the function
- ☐ Definition of its reporting line

STEP 2- MAPPING DATA PROCESSING

This compliance step consists in creating an inventory of all the personal data processing operations of the organisation. In this inventory, a register should be established as an essential document to prove compliance with the competent control authority.

- Meet the processing entities
  - In order to identify all the actors involved in the data processing operations, it is necessary to produce an exhaustive inventory.
- List the data processing activities
  - Listing data processing operations by objectives and by the different categories of data provides an exhaustive overview and facilitates the identification of high-risk processing
- ☐ Identify all data processors
  - Identification makes it possible to guarantee a good traceability of data, particularly outside the EU
- ☐ Review processing procedures
  - Thus, it is necessary to know for each processing of data: the persons having access to the data, the storage place and the storage period.

STEP 3- PRIORITISE THE ACTIONS TO BE CARRIED OUT

The record of processing activities helps to identify the processing that presents the greatest risks for the protection of the data of the data subjects. Thus, each organisation can prioritise the actions it needs to take in order to comply with the GDPR.

- Implement the first measures to protect personal data
  - Collect only the data necessary for the purposes of the processing operations
  - Review information statements
  - Verify and review contract clauses with data processors
  - Provide for procedures for the exercise of the rights of the data subjects
  - Verify the current level of security of the processing operations implemented

- Identify high-risk processing activities

STEP 4 -IDENTIFY AND MINIMISE RISKS

When identifying a data processing operation that presents a significant risk to the privacy of the data subjects, a Privacy Impact Assessment (PIA) should be carried out. Privacy Impact Assessment is a tool that will help to minimise future risks and prevent data breaches in advance.

- Identify high-risk processing
  - By listing all data processing operations, distinguish between high-risk operations in order to carry out a PIA

- Carry out a PIA
  - For each processing operation that presents a risk to the privacy of individuals, carry out PIA in order to take measures to ensure the highest level of data protection

STEP 5 – ORGANISE OR REORGANISE INTERNAL PROCEDURES

Compliance with the GDPR requires a necessary reorganisation of internal procedures and practices.

- Raise awareness and train staff members
  - Any employee who may handle personal data must be familiar with the practices to ensure confidentiality is protected.

- Create new internal procedures
  - Organisations must establish procedures for managing security breaches, responding to the rights of data subjects, etc.

STEP 6 – PROPERLY DOCUMENT ITS COMPLIANCE

The organisation must demonstrate its compliance with the GDPR and produce various documents to be updated regularly.

- Write and update compliance documents.
- In the event of an audit by the competent supervisory authority, the organisation must have the necessary documents to demonstrate its compliance with the GDPR.
  - Record of processing activities completed
  - PIAs conducted on all high-risk treatments
  - Reviewed information statements
  - Procedures for obtaining consent and exercising rights
  - Contract clause with reviewed processors

APPENDIX : 1 YEAR OF GDPR – TABLE OF SANCTIONS IN THE EUROPEAN UNION

DÉCISIONS GDPR / COUNTRY	AMOUNT OF THE SANCTION	BREACH
GERMANY		
N26 – 2018	**50.000 €**	**Legal basis for processing -** Unauthorised processing of personal data of all previous customers of an online bank for the purpose of maintaining a blacklist
Knuddels.de – november 2018	**20.000 €**	**Security obligation** - Loss of nearly 800,000 email addresses and more than 1.8 million IDs and passwords
AUSTRIA		
Sports betting establishment - September 2018	**5.280 €**	**Principle of purpose limitation, obligation of information and principle of accountability -** Illegal video surveillance (no adequate purpose of processing, no history of video surveillance processing, no appropriate information on the presence of cameras)
BELGIUM		
A mayor - May 28, 2019	**2.000 €**	**Purpose limitation principle -** The day before the municipal elections in October 2018, the mayor sent an election message to all clients of an architect who had contacted him as part of a subdivision modification (clients copied in the email). This data could not be reused for personal purposes.
DENMARK		
Taxa 4X35 – April 2019	**160.000 €**	**Data minimisation principle** - Storage of personal data beyond the limit for such data and ineffective attempt to anonymize data (taxi company)

	SPAIN	
LaLiga – 12th June 2019	**280.000 €**	**Data processing in a lawful, fair and transparent manner** - Registration of users of a mobile football application (inadequate level of information)
	FRANCE	
Google – January 21, 2019	**50 million €** equivalent to 0.05% of Google's annual income	**Transparency and information obligations and legal basis for processing (Article 6 of the GDPR) -** Personalisation of advertising (highest penalty to date)
Sergic – June 6, 2019	**400.000 €**	**Data security (Article 32 of the GDPR) and the principle of data minimisation -** Documents of applicants for rental freely accessible without prior authorisation and kept without interruption beyond the period necessary for the allocation of housing (real estate sector)
Uniontrad Company – June 13, 2019	**20.000 €**	**Obligation to inform the data subjects and safety obligation -** Constant video surveillance of employees
	HUNGARY	
Unknown – February 2019	**3.000 €**	**Right of access to their personal data of the persons concerned -** the applicant had asked the company to view and obtain a copy of a recording of a security camera filming him at reception, and not to delete the recording for 5 years, arguing that he needed it for various unrelated legal disputes, which the company had refused to do

LITHUANIA		
MisterTango UAB – May 21th 2019	**61.500 €**	**Inadequate processing and failure to notify a breach of personal data -** Processing of more data than was indicated as necessary for the execution of payments: a list of payments was visible for more than two days, and unauthorised persons had access to it, without the company reporting this breach of personal data
NORWAY		
Ville de Bergen – May 8, 2019	**170.000 €**	**Security obligation -** File containing the login credentials of 35,000 students and employees found in a public storage space (lack of appropriate security measures in the computer file system)
POLAND		
Bisnode – March 26 2019	**230.000 €**	**Transparency -** The company had not informed more than 6 million people of the processing of their personal data
PORTUGAL		
Centro Médico Barreiro – November 2018	**400.000 € -** 1st GDPR sanction	**Obligation of confidentiality and principle of limiting access to data -** Too much authorisation to access files and weakness in the management of user accounts

This EENA document was written by Bird & Bird.