



**UNDERSTANDING  
THE GDPR:  
TEN CONCEPTS  
IT DEVELOPERS  
SHOULD CONSIDER**

# contents

—• Introduction **1 – 3**

—• Key terms **4 – 7**

**01.** Protection of data **8 – 10**

**02.** What is personal data? **11 – 15**

**03.** Anonymised or pseudonymised data? **16 – 17**

**04.** Geolocation **18 – 19**

**05.** What is personal data processing? **20 – 22**

**06.** What are the conditions for processing personal data? **23 – 27**

**07.** Do I have a specific purpose? **28 – 29**

**08.** Rights of the data subject **30 – 37**

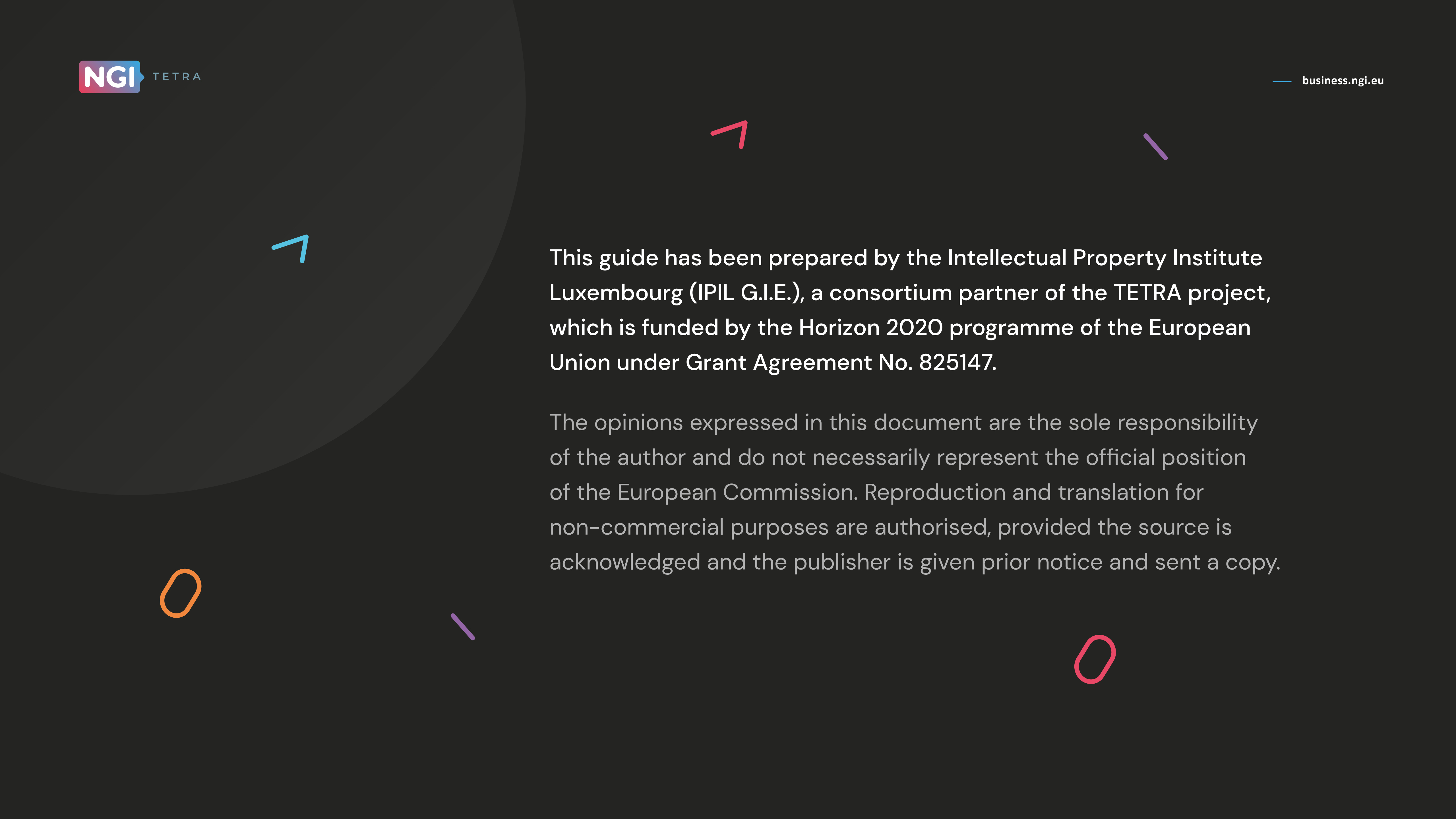
**09.** Liability and compliance **38 – 43**

**10.** Global data management and documentation **44 – 47**

—• Resources **48 – 50**



This guide aims to provide practical answers to data management questions frequently asked by IT developers. It does not aim to be a comprehensive training material for the IT sector, which would not be possible within such a short publication. We hope that this material will contribute to raising awareness of data management issues in general within the IT sector, and especially of personal data management, which presents a convergence of reasoning with Intellectual Property (IP) rights management. The information provided in this document only concerns European specificities on data management with a focus on the regulation of personal data.



This guide has been prepared by the Intellectual Property Institute Luxembourg (IPIIL G.I.E.), a consortium partner of the TETRA project, which is funded by the Horizon 2020 programme of the European Union under Grant Agreement No. 825147.

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Commission. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the publisher is given prior notice and sent a copy.

# Introduction

As developers, you create and develop IT tools to meet identified needs. These tools need data as input and generally produce new data as a result. **The aim of this guide is to enable you to acquire good practices to increase compliance with data protection requirements, and especially with personal data under the EU General Data Protection Regulation (GDPR).<sup>1</sup>**

The GDPR provides a framework to protect European citizens from the processing of personal data and gives them maximum control over their digital information. The GDPR does not hinder the processing of personal data, but aims to ensure compliance with certain conditions.

<sup>1</sup>. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation – GDPR). Can be accessed [here](#).

# Introduction

The GDPR applies to any organisation, public or private, that processes personal data on its own behalf or on behalf of another entity, as long as it is established on the territory of the European Union, or if its activities directly target EU residents.

Unlawful data processing can have serious implications for the lives and rights of the individuals whose data is processed. For this reason, the principle of accountability, which involves demonstrating data protection compliance, must be at the core of every data processing activity.

If you are processing personal data, you are responsible for this processing, the reasons why you do it and the way you do it. **This means you need to make sure not only that you comply with data protection laws, but that you can demonstrate this compliance.**



# Introduction

One way to demonstrate compliance is to document all processing operations that you undertake. Depending on the level of risk this processing entails for individuals, you may be subject to additional documentation requirements.

The purpose of this guide is to help you integrate these core principles into your IT development work, in the smoothest and most practical way possible.

Its focus is on personal data as an individual element influencing IT development and how to manage this type of data, especially in the context of EU-funded projects.

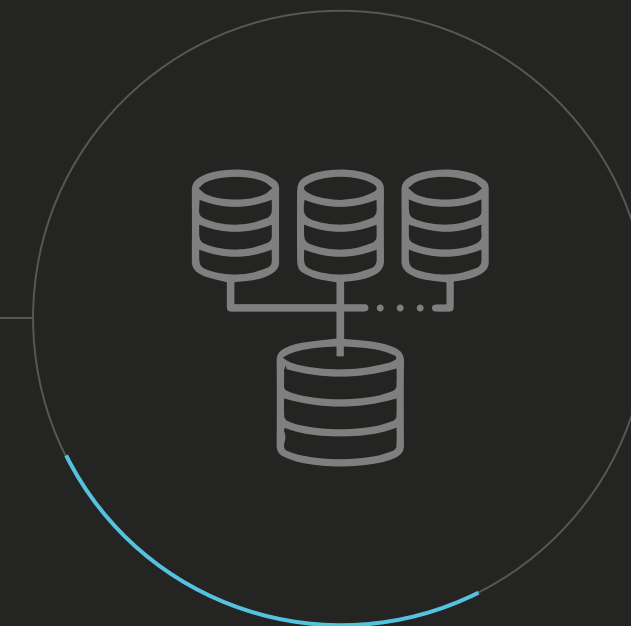
Below is a list of key terms<sup>2</sup> used in the GDPR terminology and in this guide.

# Key terms



## Data

Information in an electronic form that can be stored and used by a computer. In computing, data is the representation of information in a program.



## Dataset

Collection of separate sets of information that is treated as a single unit by a computer.



## Database

Structured set of data held in a computer, especially one that is accessible in various ways.



<sup>2</sup>. Definitions are taken from the Cambridge Dictionary, the Oxford Language Dictionary and Regulation (EU) 2016/679.

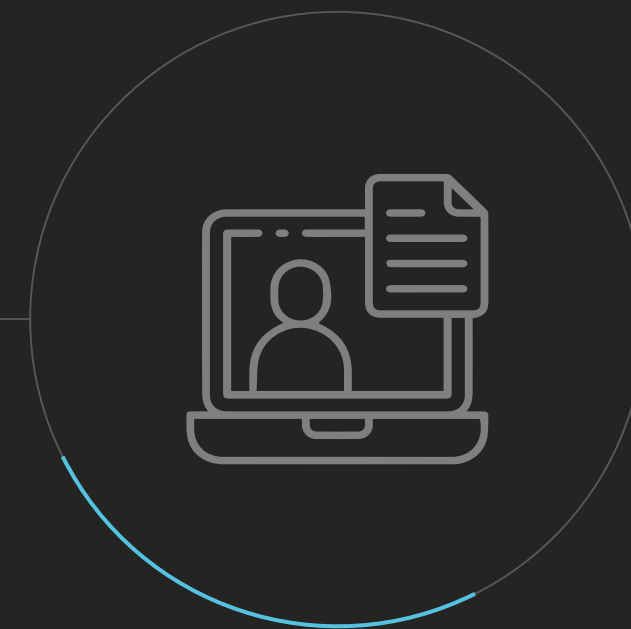


# Key terms



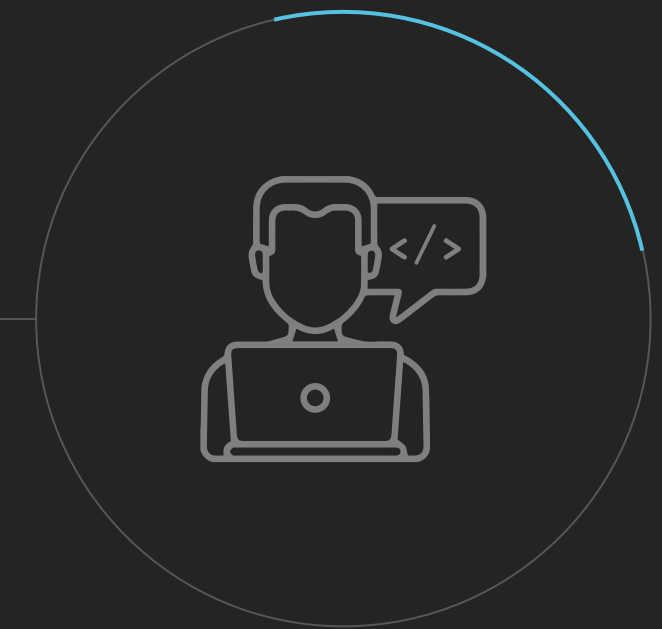
## Personal data

Under the GDPR, personal data is any information relating to an identified or identifiable natural person, directly or indirectly.



## Data subject

Natural person identified or identifiable by personal data.



## Processing

Any operation or set of operations which may or may not be carried out by automatic means.



# Key terms



## Data controller

Person or entity that determines the purposes and means of the processing of personal data.



## Data processor

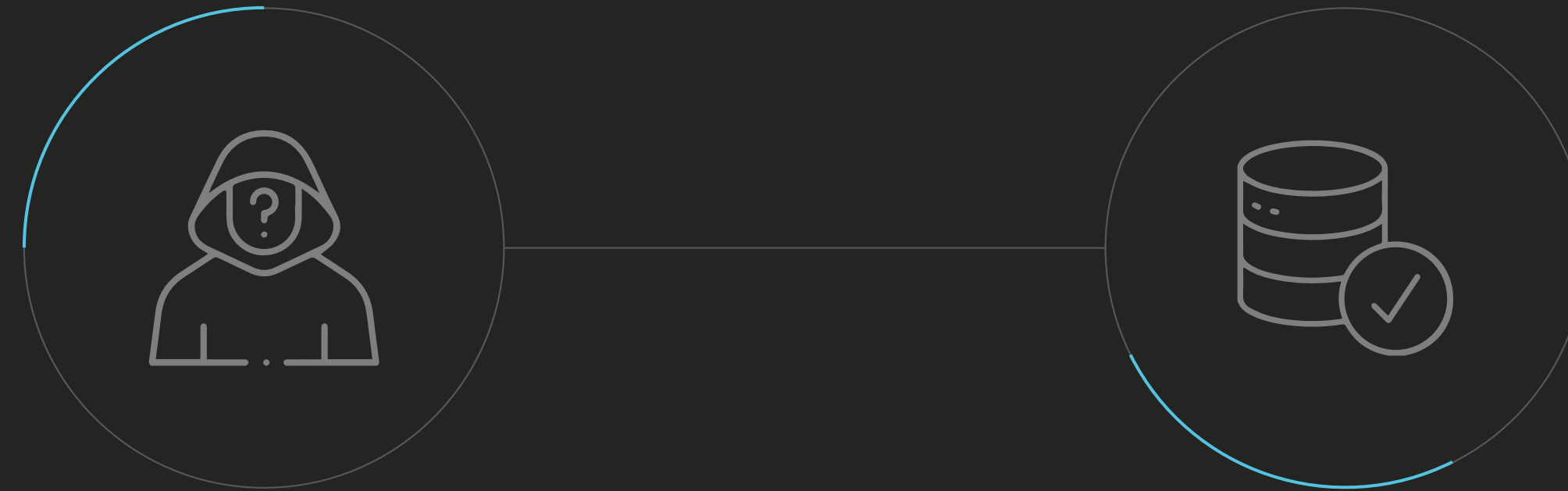
Person or entity that processes personal data on behalf of the controller. The data processor can be a controller at the same time.



## Pseudonymisation

Processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

# Key terms



## Anonymous data

Information that does not relate to an identified or identifiable natural person, or personal data that has been rendered anonymous in such a way that the data subject is not or no longer identifiable.

## Consent of the data subject

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data.



# 01.

## Protection of data

We generally hear about legal protection, i.e. protection through legal means. However, there is no law that protects everything, and everything cannot always be protected.

Protection is not only about protecting a product as a whole. It is also about protecting each of its components. You are free to choose whether you want to protect your own creations or not. However, you must respect third-party rights, especially when you reuse third-party elements.

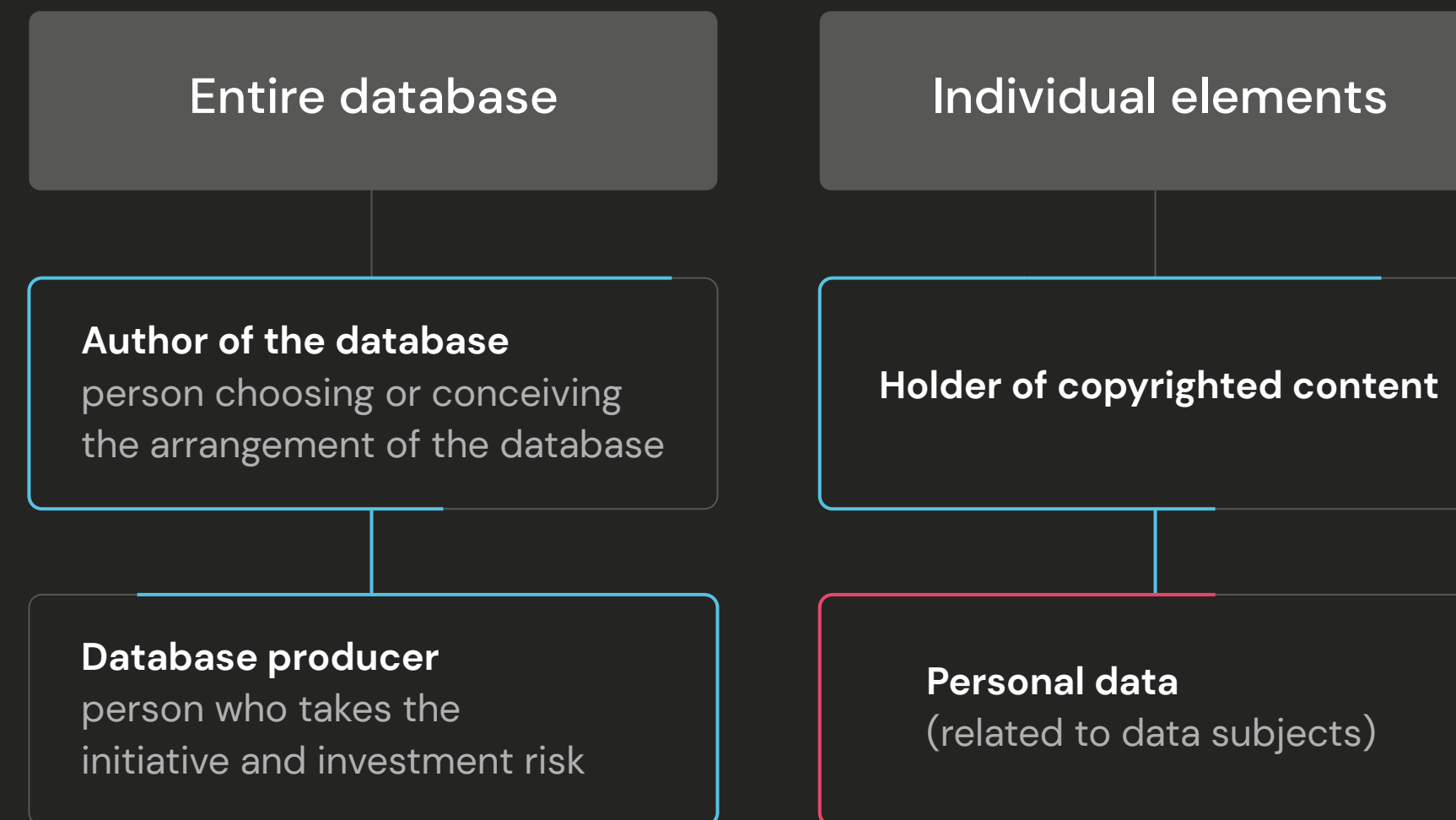
A work might be subject to several protected rights belonging to different right holders. For instance, in the case of databases, there might be rights related to the entire database structure belonging to one right holder, and separate rights related to the content of the database belonging to other right holders. As a result, the different rights need to be reconciled.

# 01.

## Protection of data

### Privacy and Intellectual property

It is important to not confuse Intellectual Property (IP) rights that apply to data with personal data protection. Although both types of rights may apply to a same object, each has a different purpose: IP protects the creation and the creator, while personal data protects physical persons.



**Note:** The items in blue concern "intellectual property", the item in red concerns "personal data regulation".

Figure. IP vs. personal data, example of a database

# 01.

## Protection of data

In order to determine the protection and obligations that might apply, **it is necessary to identify the applicable right(s) through an element-by-element approach for each part of the project.**

This requires an **analytical effort to identify the different elements that can be protected and valued.** One way to do this is to implement agile development methods.

It is necessary to separate all the elements of the project: the product, the process, the business model, the communication elements, the IT tools (programs, databases, etc.) and, regarding the GDPR, to adopt a project management approach that makes the person concerned (data subject), as the client (or user), the main driver of the development team.



# 02.

## What is personal data?

The notion of "personal data" is to be understood in a very broad way.

Any information directly or indirectly related to an identified or identifiable natural person is personal data.

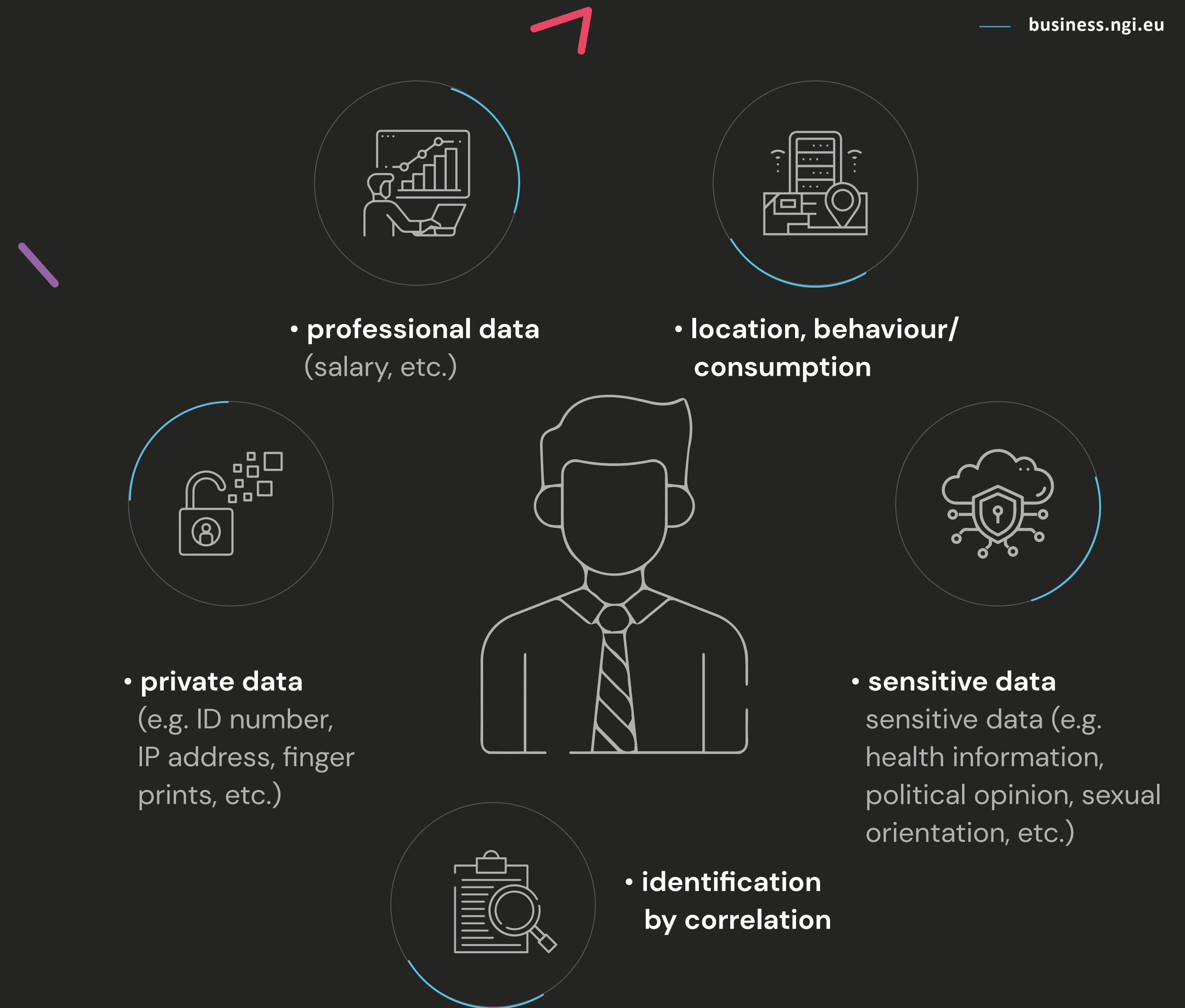


Figure: Personal data surrounds us (data examples are not exhaustive)

# 02.

## What is personal data?

### Examples of personal data:

- the name of a person together with their telephone details or information about their working conditions or hobbies
- a list of participants (first and last names) in a meeting
- an address
- workers' holidays, breaks or rest periods

- income from work or another source
- personal assets
- IP address – be it static or dynamic
- an academic examination paper, etc.



# 02.

## What is personal data?

Personal data is not only digital data: it can be hand-written information, an image, a voice – as long as it allows a person to be identified.

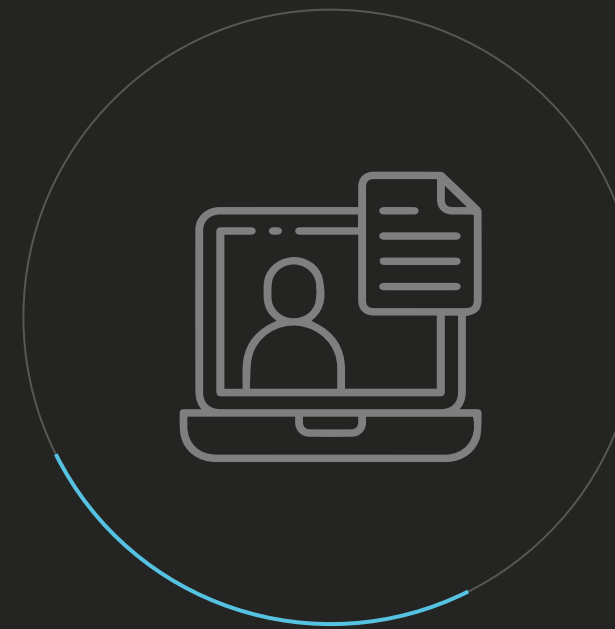
Among personal data, some is considered to be particularly “sensitive” and subject to specific processing conditions (consent, security, etc.):

- data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs,
- trade union membership,
- genetic data, biometric data processed solely to identify a human being,
- health-related data,
- data concerning a person’s personal life or sexual orientation.



# 02.

## What is personal data?



Identification is direct when it is directly and precisely linked to a person (e.g. surname, first name).

Identification is indirect when the information does not make it possible to identify the person concerned, but the identification can be achieved by combining this data with other data.

# 02.

## What is personal data?

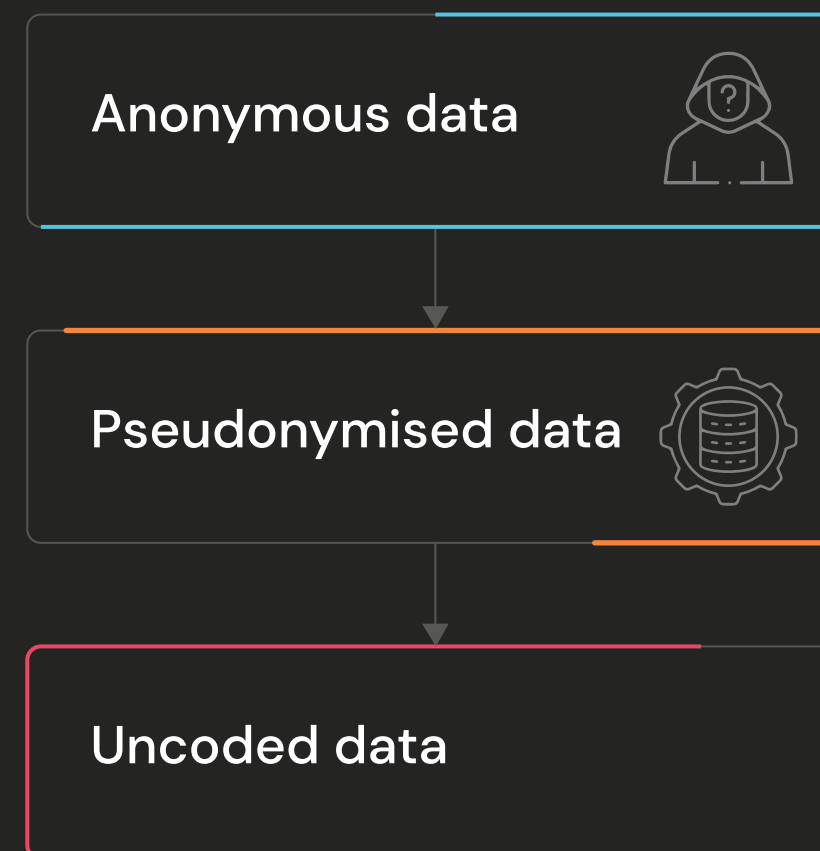
### Example

In order to identify the person who consulted a web site, the dynamic IP address must be combined with the date and time of connection or with additional information held by the network access provider. In this case, the information used to identify the person can be qualified as personal data. It does not matter whether or not all the information facilitating the identification of the data subject is in the hands of one entity. It is sufficient that this indirect identification is possible, including with the support of additional information or an identification technique held by a third party.

This might lead in practice to the presumption that any data is personal data or likely to become so.

# 03.

## Anonymised or pseudonymised data?



Data is considered to be anonymous when it cannot be (re-)identified. Anonymous data is not considered to be personal data.

The processing of anonymous data therefore does not have to comply with the GDPR.

In practice, several techniques exist to anonymise data, some of which may have shortcomings. For this reason, data controllers implementing anonymisation techniques should regularly analyse the inherent risk of re-identification by assessing the severity and likelihood of this risk on a case-by-case basis.



# 03.

## Anonymised or pseudonymised data?

Pseudonymised data is personal data. Pseudonymisation is a security measure that controllers can use so that personal data can no longer be attributed to a specific data subject without using additional information that is separately stored and protected.

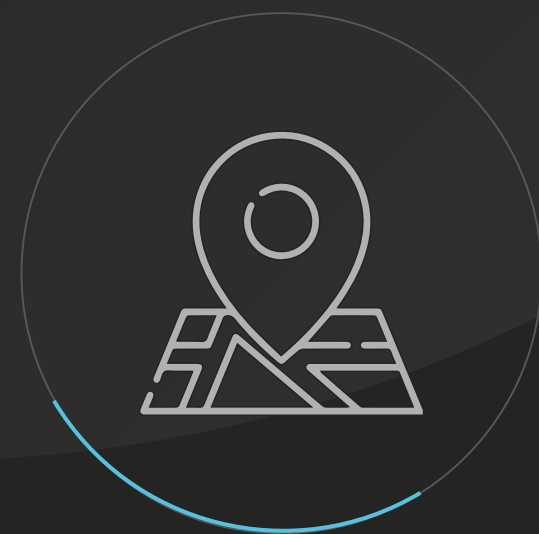
Encryption or hashing of personal data, for instance, are considered to be pseudonymisation, not anonymisation.

The use of pseudonymised data reduces the risk for data subjects and contributes to compliance with the GDPR.

Note that pseudonymisation operations amount to personal data processing.

# 04.

## Geolocation



***If I use an external service provider to neutralise the last bytes of the IP addresses, am I processing anonymous or pseudonymised data?***

Geolocation data is considered to be personal data if it directly or indirectly allows the identification of a person. Because of this, an IP address – be it static or dynamic – is considered to be personal data.

A location at the level of a city, region or country without using the IP address in its entirety is considered to be pseudonymised personal data.

When neutralising the last bytes of an IP address (e.g. the last 2 bytes), it cannot be said that anonymous data is produced. However, it can be said that the processing of personal data is minimised (1) if we do not intend to re-identify individuals; and (2) if we take the necessary measures to limit the risk of re-identification by third parties who might gain access to this data, either legally (partnerships, contracts, etc.) or illegally (data leakage, hacking, etc.).

# 04.

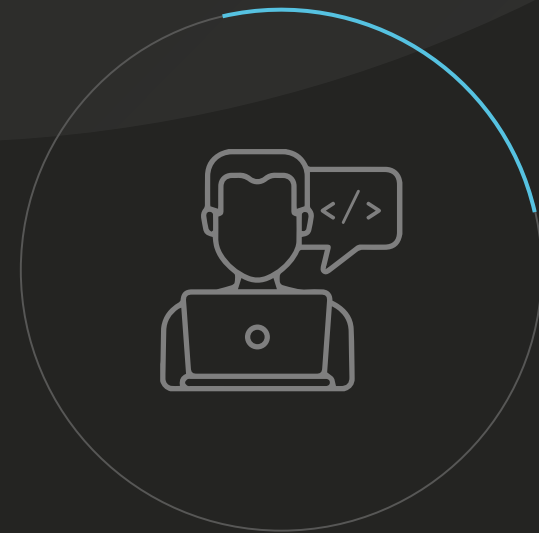
## Geolocation

If you intend to subcontract the processing (e.g. collection) and/or pseudonymisation of IP addresses, it is necessary that the subcontractor contractually commit to complying with the GDPR.

It is the responsibility of the ordering party to provide clear indications to the subcontractor justifying the purpose of the data processing.

# 05.

## What is personal data processing?



“Processing of personal data” is an operation, or set of operations, applied to personal data, regardless of the process used (collection, recording, organisation, storage, adaptation, modification, retrieval, consultation, use, communication by transmission, dissemination or any other form of making available, matching).

### Example

Keeping a file of customers, collecting contact details of prospective customers via a questionnaire, updating a file of suppliers, etc. are considered to be processing of personal data.

# 05.

## What is personal data processing?

With respect to the data life cycle, each stage is also deemed to be processing of personal data.

Note that personal data processing does not necessarily have to be computerised: paper files must also be treated and protected under the same conditions.

# 05.

## What is personal data processing?

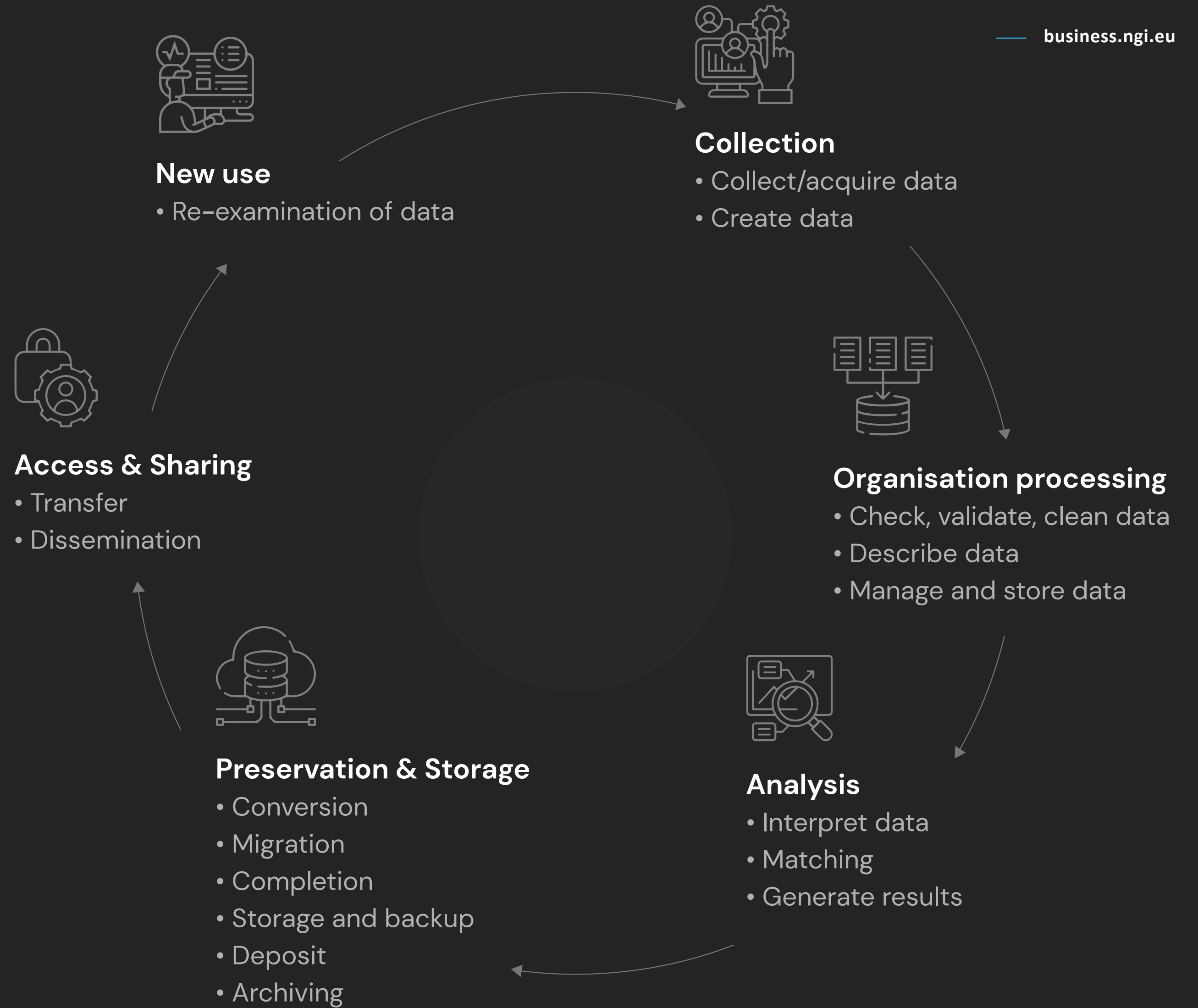


Figure: An illustration for "personal data life cycle management"



# 06.

What are the conditions for processing personal data?

Any processing of personal data must be lawful, fair and transparent. These principles start with an obligation to provide to the data subject information on the existence and conditions of the processing of personal data, and are closely linked to the data controller's specific purpose for personal data processing. The data must be accurate, proportional and relevant.<sup>3</sup>

<sup>3</sup>. For more information about the data protection rules, you can also refer to the EU website [here](#).

# 06.

What are the conditions for processing personal data?



Figure: Conditions to process personal data

# 06.

What are the conditions for processing personal data?

## Processing personal data in a lawful, fair and transparent manner

In order to comply with GDPR, personal data must be collected, stored, used and transferred in good faith and in a manner that is transparent to the data subject.

Direct collection without the consent of the person concerned is prohibited beyond the specific purpose clearly notified to the data subject.<sup>4</sup> For example, where consent to the collection of Wi-Fi network identifiers (SSIDs), MAC addresses of Wi-Fi routers and Wi-Fi connection data is obtained for the stated purpose of “optimising geolocation services offered by a company to its customers”, this consent does not mean that the data can be used for other purposes, such as, for example, “obtaining information on the content of messages”.

<sup>4</sup>. See section 7. “Do I have a specific purpose?”

# 06.

What are the conditions for processing personal data?

In addition to the fact that personal data processing must be done in a fair and clear manner, that processing must also have a legal basis and the data subject must be informed about that legal basis.

For example, if there is a legal obligation for the police to collect address data to send traffic fines, the data subject cannot oppose this collection however the police must inform the data subject that such data collection is required by law.

# 06.

What are the conditions for processing personal data?

## Collection of personal data with a clear purpose

Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way that is incompatible with those purposes.

## Applying the data minimisation principle

It is important to collect as little personal data as possible and to only process the data that is necessary to fulfil the purposes you have identified.

## Ensure that data is accurate and kept up-to-date

Incorrect data should be corrected or deleted without delay, and must be kept for the minimum amount of time necessary for the purpose of the processing.

# 07.

Do I have  
a specific  
purpose?

The description of the purpose of the data processing is a key step, as it is the basis for the compliance of the processing.

Why is personal data being processed? For what purposes?

A data processing operation must have an objective, a purpose!

- The GDPR does not allow personal data to be collected or processed for an unlimited period. A defined period must be provided for those operations.
- Each data processing operation must have a purpose, which must be lawful and legitimate in relation to the project and to the stage of the data life cycle.
- The purpose must be specified, explicit, legitimate and be determined in advance.



# 07.

Do I have  
a specific  
purpose?

Therefore, the data controller must find a basis for the processing:<sup>5</sup>

- based on the consent of the data subject,
- necessary for the performance of a contract to which the data subject is party,
- necessary for compliance with a legal obligation to which the controller is subject,
- necessary to protect the vital interests of the data subject or of another natural person,
- necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

## Example

Collection of customer information to make a delivery, issue an invoice or offer a loyalty card constitutes processing of personal data for customer management purposes.

<sup>5</sup>. Necessary for the purposes of the legitimate interests pursued by the controller, unless the interests, freedoms or fundamental rights of the data subject prevail.

# 08.

## Rights of the data subject

### Definitions

Below is a list of the rights of the data subject and their definition.<sup>6</sup>



01.

02.

03.

#### Right to information

The right to obtain transparent and fair information throughout the life cycle of the processing of one's personal data, including the provision of information in response to requests to exercise other rights.

#### Right of access

The right to be informed of the personal data processed by the controller, to be given access to the data or to receive a copy of the data.

#### Right to rectification

Right to correct inaccurate data about the person (e.g. wrong age or address) or to complete data (address without flat number) in connection with the purpose of the processing.

<sup>6</sup>. The definitions are extracted from [1], [8], [9], [10], [11], [12], [13], [14].

# 08.

## Rights of the data subject

### 04.

#### Right to erasure ("right to be forgotten")

The right of any person to obtain the deletion, as soon as possible, of personal data concerning him/her.

### 05.

#### Right to limitation of processing

Right to obtain that his/her data is no longer processed beyond their lawful/consented conservation period or without the consent of the data subject.

### 06.

#### Right to data portability

The right of any data subject to recover personal data relating to him or her, which he or she has provided to the controller, in a structured, commonly used and machine-readable format, or to have such data transmitted directly to another controller (e.g. customer file history, patient's file, customer history).

# 08.

## Rights of the data subject

# 07.

### Right to object

Right to object to the use of his/her data by the controller for a specific purpose, provided valid reasons are given relating to his or her particular situation (except in the case of commercial prospecting, where no reason is required).

# 08.

### Right not to be subject to a decision based exclusively on automated processing

Right to be informed in advance of the existence of algorithmic decision-making and to be able to know the logic of the processing or even in some cases to obtain human intervention by the controller. Right of user to express his/her point of view and to contest the decision taken in his or her regard.

# 08.

## Rights of the data subject

It is not only a question of providing information to the data subject, but also of improving the quality of the content of his/her information, in accordance with the principle of transparency and fairness. **The information must be accessible, understandable and up-to-date.**

If there is any amendment on personal data (e.g. rectification in his/her "shopping interests" or deletion of his/her data on "car ownership"), this change must be reflected in the collected data, and the data subject must be informed about these updates to his/her information accordingly. The data controller must ensure that the data subject can access, modify, delete etc. his/her personal data.

The appropriate time for transmitting the information and the form in which the information is provided must be assessed on a case-by-case basis, considering the life cycle of the personal data, the type of services or products offered, and even the characteristics of the data subjects, taken as a group.



# 08.

## Rights of the data subject

### Information on data processing

The main principles governing the provision of information on personal data processing are that the following must be provided:

- Information to the data subject at the time of data collection (e.g. informing the data subject when filling in an online questionnaire with contact details).
- Information on data obtained from other sources within a reasonable time (maximum one month).
- Prior information in case of onward transfer for a purpose different from the initial purpose.
  - Such additional processing must be subject to specific prior information to the data subject, collectively and individually. This prior information obligation applies whether or not the data is collected from the data subject or not. The reasonable time limit must be assessed in light of the context, and in particular the risks to the rights and freedoms of the data subject associated with the transfer. The higher the risks, the longer the period should be.
- Prior information in case of future updates.



# 08.

## Rights of the data subject

The information to be provided must be clear and concise, while being precise and adapted to the target audience, particularly children.

The data controller is encouraged to provide this information through several channels that can be complementary, such as SMS, emails, QR codes referring to dedicated pages, etc.

Access to the information must be free of charge except in case of abuse on the part of the data subject (e.g. constantly requesting data access, etc.).



# 08.

## Rights of the data subject

### Specific derogations in cases where data is not collected from the data subject

In cases where the controller is unable to provide the above information to the data subject, or where doing so would require disproportionate efforts which would seriously compromise the achievement of the objectives of the processing, it is up to the controller to show either that it is absolutely impossible to provide the information or that the effort required would be disproportionate.

- e.g. processing for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

### Example

Processing for historical purposes of data concerning 20,000 persons, collected 50 years ago, which other researchers would like to continue to use.

# 08.

## Rights of the data subject

### Deletion obligations

There are some obligations regarding the conservation of personal data. Such data must not be kept for an unlimited time and must be deleted<sup>7</sup> in the following situations:

- data is no longer necessary for the purposes of the processing,
- withdrawal of consent and lack of any other legal basis for processing,
- exercise of the right to object and lack of compelling legitimate grounds for further processing,
- unlawful processing of data,
- compliance with a legal obligation,
- data collected online from minors.

<sup>7</sup>. Note that data deletion is considered to be data processing.

# 09.

## Liability and compliance

The principle of accountability is a cornerstone of European data protection law. This principle sets out two main categories of obligations for actors (data processor, data controller, data subject, etc.), which are then broken down into a series of general obligations applicable to all, and specific obligations that actors must fulfil in certain situations.

The principle of accountability requires that actors establish a method to effectively ensure the adoption of compliance measures.

# 09.

## Liability and compliance

### Data flow documentation

The data controller has to have an overview of the data processing flow and the data flow has to be documented.<sup>8</sup>

The following table presents the different steps in data flow documentation, with the different actions to be performed.

<sup>8</sup>. Some data flow diagram examples can be consulted [here](#) or [here](#).

# 09.

## Liability and compliance

### Steps to follow according to the GDPR

### Example measures to undertake

Developing and maintaining a record of activities

Record of processing activities that leads to the creation of an inventory of the data processing and provides an overview of what is done with the personal data.

Format:

- Written or electronic
- Constant updating
- Data retention: limited periods (recommendation: 5 years)

Conducting risk analysis

Where data processing is likely to result in a **high risk to the rights and freedoms of natural persons**, the controller should carry out a privacy impact assessment (PIA).

Description of operations  
Necessity and proportionality  
Technical and organisational measures

A PIA can also be useful to assess the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations.

In cases where it is not clear whether a PIA is required, it is recommended that a PIA is carried out nonetheless as it is a useful tool to help controllers comply with the GDPR.



# 09.

## Liability and compliance

### Protecting data by design

The data controller should take data protection into account at the early stages of planning a new way of processing personal data. In accordance with this principle, a data controller must take all necessary technical and organisational steps to implement the data protection principles and protect the rights of individuals. These steps could include, for example, using pseudonymisation.

### Protecting data by default

The data controller should always make the most privacy-friendly setting the default setting. For example, if two privacy settings are possible and one of the settings prevents personal data from being accessed by others, this should be used as the default setting.

### Duty to inform (fairness principle)

Duty of the controller to pro-actively inform the data subject, in a concise, understandable and easily accessible manner. Such information should be in writing or by other means, including electronic means.

### Ensuring data quality

The data should be readable and kept updated.

# 09.

## Liability and compliance

### Taking security measures

#### Objectives:

- Authenticity, integrity and confidentiality of data
- Avoid loss, destruction, accidental damage

Definition of security measures according to risk, nature and volume of data.

Consider the state of the art and costs.

Use technical operations such as encryption and pseudonymisation.

### Protecting data when working with third parties (e.g. subcontracting, in partnerships, auditing, etc.)

Requirement for an agreement between joint controllers:  
This agreement must specify the respective responsibilities of each of the joint controllers.

**Requirement for a binding act specifying the relationship between controllers and processors. This act must define** “[...] the purpose and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, and the obligations and rights of the controller”.

Obligation to cooperate with supervisory authorities: The controller and the processor must respond to requests from the authorities. Failure to do so is penalised through sanctions.

# 09.

## Liability and compliance

### Appointing a data protection officer (DPO)

Mandatory for public bodies and certain private bodies whose core business involves large-scale processing of sensitive data or data allowing regular and systematic monitoring of individuals (this type of processing is determined by law or on a case-by-case basis).

The DPO can be internal or external (e.g. lawyer). The DPO must be able to act autonomously (hierarchically, technically, financially, etc.), and must be exempt from conflicts of interest.

#### Missions

- Advise the company on data protection and training
- Cooperate with the supervisory authority
- Constitute a contact point for data subjects

# 10.

## Global data management and documentation

The questions and methodology presented in this guide should be considered at each stage of the project, in the context of the data life cycle.

**The notion of global data management is very important:** it provides for a comprehensive approach while also specifying precise information for each element of the project. In this context, a data management plan, completed and linked to specific documentation for each element (register of activities, PIA, register of licence agreements, etc.), makes it possible to establish a connection between the developers and the lawyers working on the project.

# 10.

## Global data management and documentation



Figure: A general illustration of a data life cycle



# 10.

## Global data management and documentation

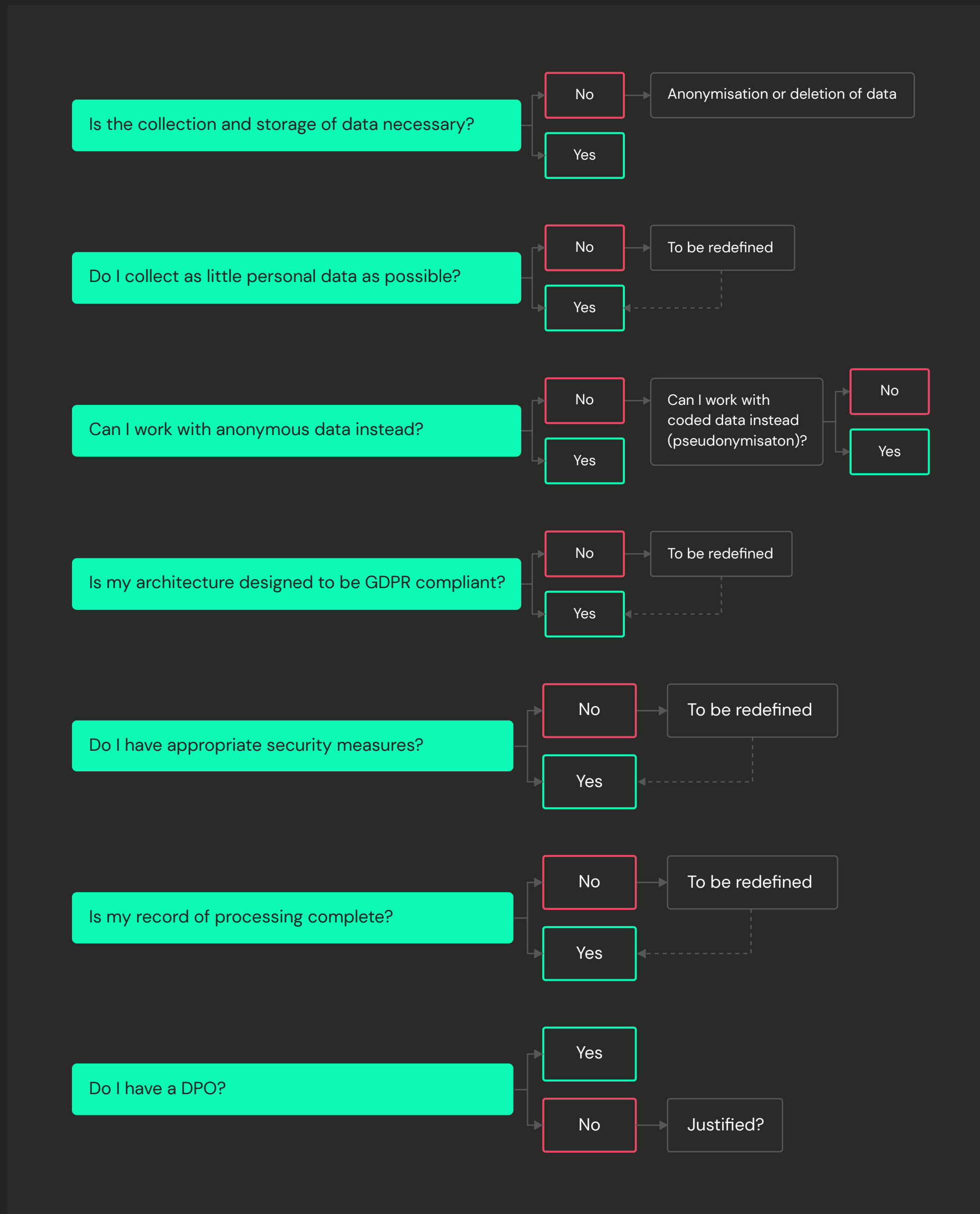
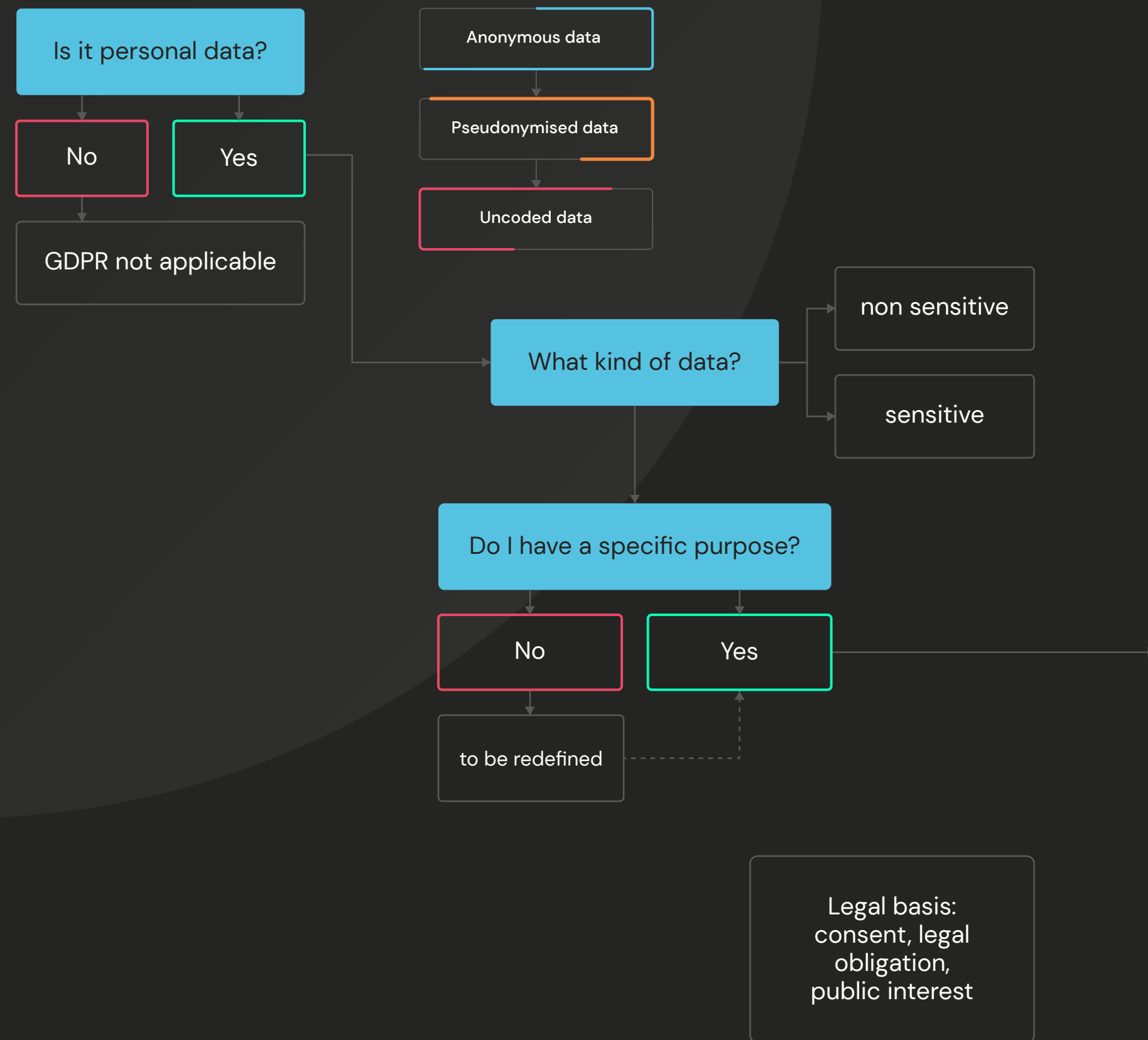
### Particulars of access & sharing in European projects

European projects are generally subject to an obligation to share results under an open licence. One point requiring attention is to check the type of licence and whether the open licence concerns the intellectual property developed and/or used in the project (background and results), or whether it affects the processing of the data.

In the framework of such projects, the use of tools such as a data management plan makes it possible to coordinate and reconcile the simultaneous application of various legislations, which can be complex.<sup>9</sup>

<sup>9</sup>. You can find further information on how to manage data protection and open licences in European projects [here](#).





### Decision tree on personal data protection management

The data protection management rules and measures set out in this guide are summarised in this diagram:

# Resources

01. "Regulation (EU) 2016/679 of the European Parliament and 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)", EUR-Lex.  
<https://eur-lex.europa.eu/eli/reg/2016/679/oj> (Last consulted: 15.06.2022)
02. "Reform of EU data protection rules", European Commission.  
[https://ec.europa.eu/info/law/law-topic/data-protection/reform\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform_en) (Last consulted: 15.06.2022)
03. Information on the "Digital single market", EUR-Lex.  
[https://eur-lex.europa.eu/summary/chapter/31.html?expand=3108#arrow\\_3108](https://eur-lex.europa.eu/summary/chapter/31.html?expand=3108#arrow_3108) (Last consulted: 15.06.2022)
04. "Infographic - Data protection regulation", European Council.  
<https://www.consilium.europa.eu/en/infographics/data-protection-regulation-infographics/> (Last consulted: 15.06.2022)
05. Website of the European Data Protection Supervisor.  
[https://edps.europa.eu/\\_en](https://edps.europa.eu/_en) (Last consulted: 15.06.2022)
06. "GDPR Developer's Guide", Commission Nationale de l'Informatique et des Libertés (CNIL).  
<https://www.cnil.fr/en/gdpr-developers-guide> (Last consulted: 15.06.2022)

# Resources

07. "The open source PIA software helps to carry out data protection impact assessment", Commission Nationale de l'Informatique et des Libertés (CNIL).  
<https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>  
(Last consulted: 15.06.2022)
08. "Handbook on European data protection law – 2018 edition", European Union Agency for Fundamental Rights (FRA).  
<https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>  
(Last consulted: 15.06.2022)
09. "Manuel de droit européen de la protection des données à caractère personnel", Olivia Tambou.  
<https://www.larcier.com/fr/manuel-de-droit-europeen-de-la-protection-des-donnees-a-caractere-personnel-2020-9782802764328.html> (Last consulted: 15.06.2022)
10. "Le Data Protection Officer", Virginie Bensoussan-Brulé et al.  
<https://www.larcier.com/fr/le-data-protection-officer-2020-9782802763451.html> (Last consulted: 15.06.2022)
11. "Droit des applications connectées", David Lefranc.  
<https://www.larcier.com/fr/droit-des-applications-connectees-2017-9782804471712.html> (Last consulted: 15.06.2022)
12. "Guide pratique des plateformes", Axel Beelen et al.  
<https://www.larcier.com/fr/guide-pratique-des-plateformes-2021-9782807920583.html> (Last consulted: 15.06.2022)

# Resources

- 
13. "Le Contract Manager", Alain Bensoussan, Eric Le Quellenec.  
<https://www.larcier.com/fr/le-contract-manager-2019-9782802763130.html> (Last consulted: 15.06.2022)
- 
14. "Article 29 Working Party".  
[https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party\\_en](https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en) (Last consulted: 15.06.2022)
- 
15. "GDPR Compliance Process", Compliance Junction.  
<https://i.pinimg.com/originals/d8/9e/52/d89e5278d3944674718070c09c80f6fa.png> (Last consulted: 15.06.2022)
- 
16. "Analytical Report 3: Open Data and Privacy", European Commission.  
[https://data.europa.eu/sites/default/files/open\\_data\\_and\\_privacy\\_v1\\_final\\_clean.pdf](https://data.europa.eu/sites/default/files/open_data_and_privacy_v1_final_clean.pdf) (Last consulted: 15.06.2022)
-



@NGI4EU #TETRA  
#Business4NGI

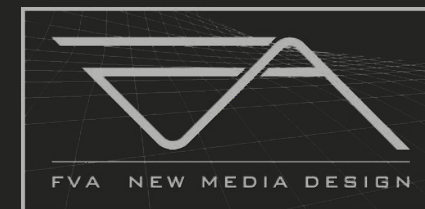
## Partners



CIVITTA



Startup Division



LOBA CUSTOMER EXPERIENCE DESIGN



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 825147



[info@tetraproject.eu](mailto:info@tetraproject.eu)