Data Protection

TRILATERAL RESEARCH
Ethical AI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 958264

OPTIMAI

Contents

General Data Protection Regulation

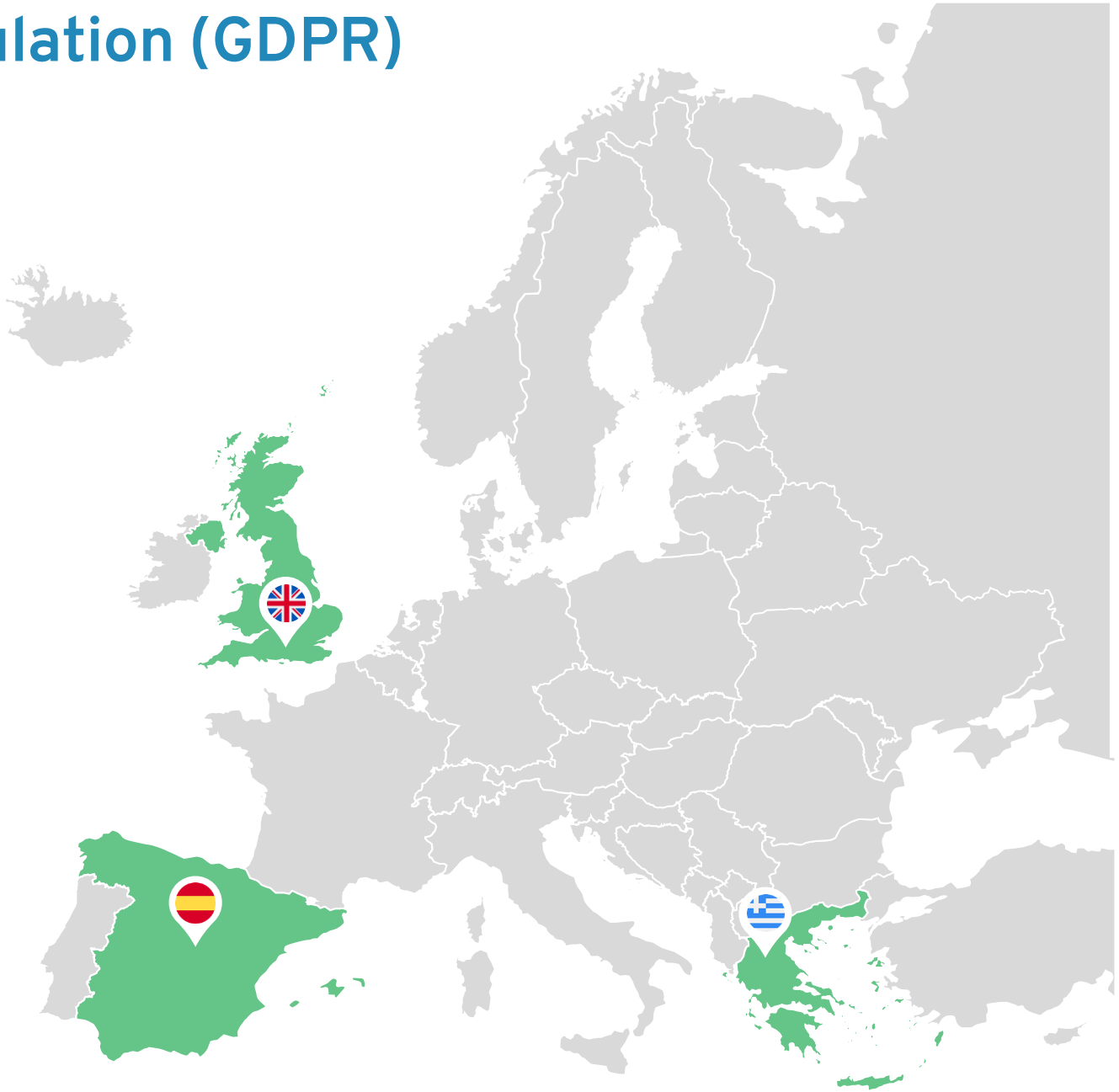
1

General Data Protection Regulation (GDPR)

The **General Data Protection Regulation (GDPR)** came into force in the European Union on May 25, 2018. The regulation has been transposed into law and is applicable in the countries of OPTIMAI's pilot sites: Greece, Spain, and the United Kingdom.

The GDPR enshrines **important obligations for data controllers with regards to the handling of personal data.**

25 May, 2018



Personal Data

- In the GDPR, **personal data** is defined as:

  any information relating to an identified or identifiable natural person ('data subject').

- An identifiable natural person is **one who can be identified, directly or indirectly, by reference to an identifier** such as a name, an identification number, location data, or an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- In OPTIMAI, all partners may have various uses for personal data, including names and contact details or may handle data containing identifiers of persons including audio and visual data from factory floors.

Consent & Legitimate Interest

Consent

When OPTIMAI partners are processing personal data, they should make sure they do so with an appropriate lawful basis. In some cases, **consent** will be an appropriate basis for processing such data.

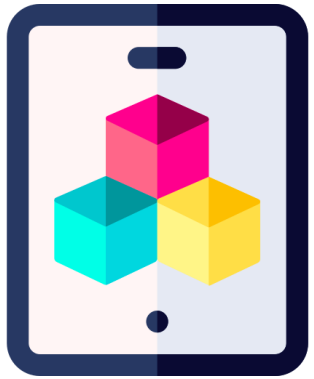
- Consent should be:
  - Freely given
  - Informed
  - Specific to the data processing activity
  - Given by the data subject with clear agreement
  - Revokable

- If you are planning to publish images of identifiable employees on a website or social media, for example, you should **ask for the employee's permission** to take and share the image, ensuring that **they are informed of where it will be published and why**, and how they can later **have it removed** if they withdraw their consent.

Consent

During OPTIMAI Pilot activities, many employees participating in the research cannot be fairly said to be able to consent to all data processing operations by end-users or other partner.

The **vulnerable position of an employee relative to their employer often militates against consent as a lawful basis for processing their data**, particularly if it cannot be demonstrated that an employee freely chose without any pressure.



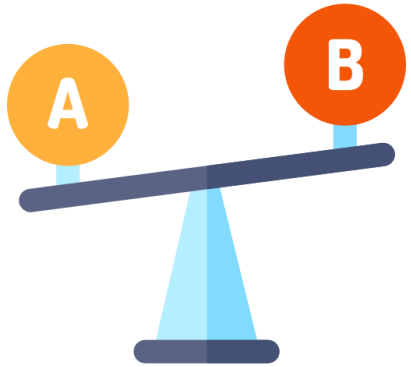
- For matters including the use of new tools that that may form an intrinsic element of the employee's role and require personal information for log ins, for example, they may not be in a position to freely refuse processing of their personal data **without compromising their ability to perform their job.**

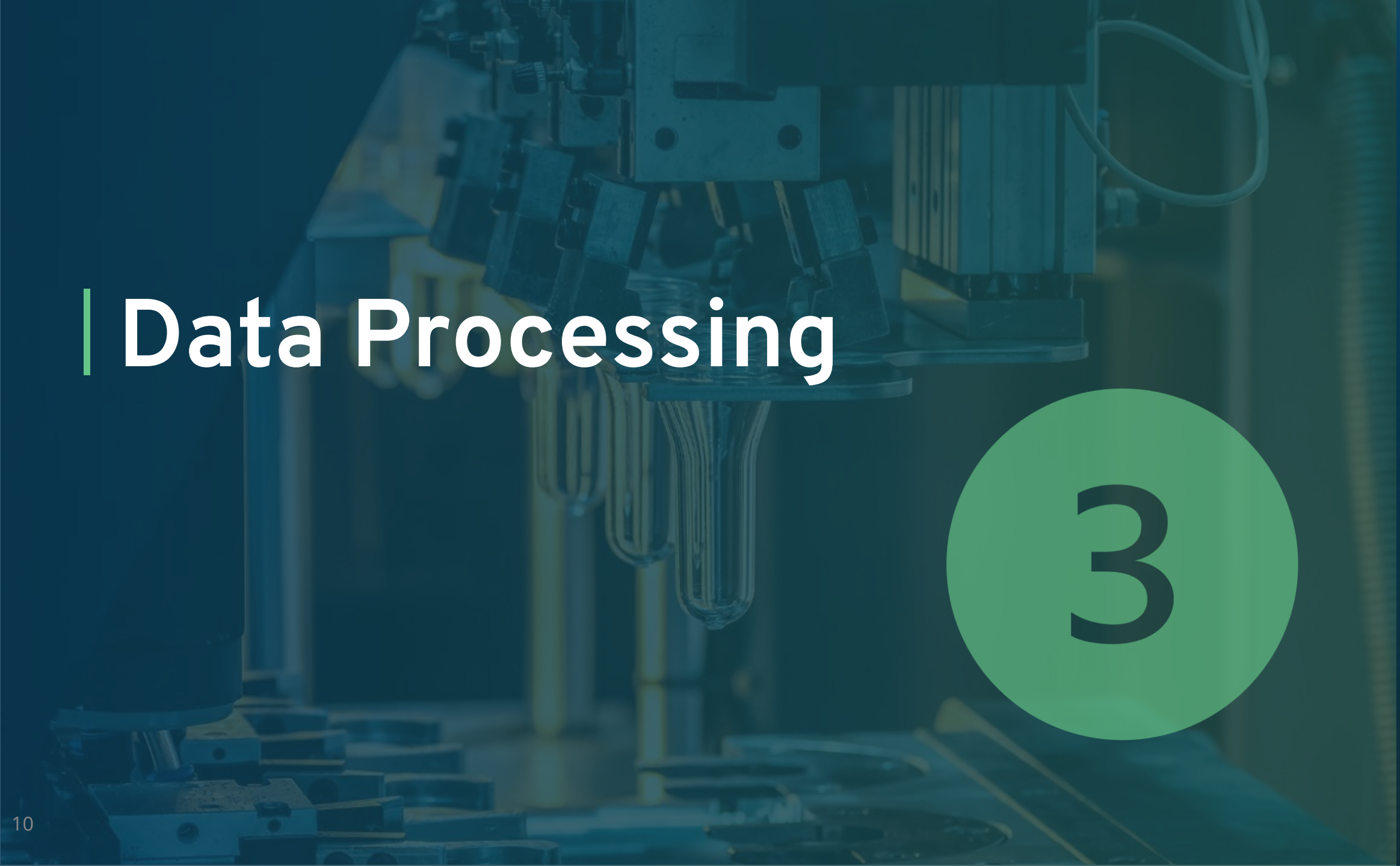
Legitimate Interest

In this case, the data controller may rely on another lawful basis, including **legitimate interest**.

- A relevant legitimate interest to specific instances of data processing may exist between end-users and employees, for example, based on a **“relevant and appropriate relationship”** and where data subjects can **“reasonably expect”** the data processing operations at the time and in their context of taking place.

- For this lawful basis, a **balancing test** should be performed and documented with the assistance of a legitimate interest assessment as provided by ethics and legal partners.





Data Processing

3

Data Processing Operation

The processing operation should be **transparent**, and pilot site employees should be clearly and fully-informed about them including the purposes of the data processing.

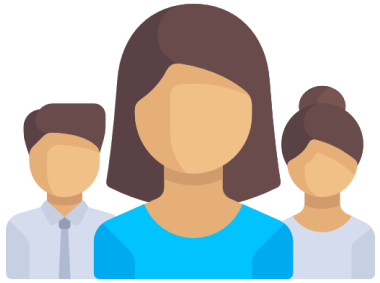
The data controller must communicate all relevant information to the data subject in a concise, transparent, intelligible, and easily accessible form.

- This means **no technical jargon** or via **unusual formats**.

- Data controllers, and especially end-user partners, should make sure that employees are aware of all data processing activities, and **what kinds of information** are being processed and to **whom they are being sent** and **why**.

Changes to Processes & Processing Activities

It is good practice for employees to be **consulted about changes** to workplace processes and data processing activities.



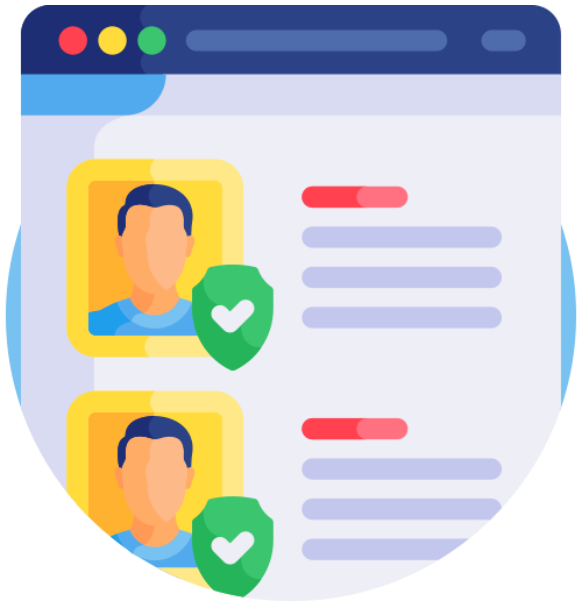
- Any new changes with regards to the installation of new devices in the workplace environment should be brought to employees ahead of time, for example, and some **time should be granted for input and feedback**.

- This can **help avoid data processing operations that employees could not reasonably expect**, which could invalidate a lawful basis for the processing such as legitimate interest.

OPTIMAI

Data Minimization

Data controllers should ensure that they only process data that they need in order to achieve their legitimate goals, so it should be **adequate, relevant** and **limited** to the purposes of the processing operation. This is in line with the principle of **data minimization**.



- Adequate
- Relevant
- Limited to the purposes of the processing operation

Data Minimization

Data Security

Data controllers must ensure that the tools they use to process data are **adequately secured** and that organizational policy around data processing and who has access to what information protect the fundamental rights of data subjects.

Hardware

Software

Anonymization

Data Protection & Cyber Security

Data Security

Hardware

Hardware used for data processing operations should be secured with suitable access control and authentication, for example, and only persons with duties relevant to the data and its processing should have access. Access to personal data should also be logged in order to support accountability and ensure no intrusions have occurred.

Software

Appropriate software should also be in place on systems that process personal data, including anti-malware solutions, and all necessary security dependencies should be kept up-to-date.

Data Security

Anonymization

Where it does not compromise the capacity of OPTIMAI researcher to achieve legitimate research purposes and goals, all personal data should be anonymized or pseudonymized.

Data Protection & Cyber Security

All data controllers should make sure that their organization has and implements effective data protection and cyber-security policies.

Rights of Data Subjects

4

Rights of Data Subjects

Data controllers need to consider the specific rights of data subjects, many of whom might be pilot site employees. These include the right to:

1. *Information*
2. *Access*
3. *Rectification*
4. *Erasure*
5. *Restriction of Processing*
6. *Data Portability*
7. *Object*
8. *Avoid Automated Decision Making*

Rights of Data Subjects

In brief, this means that:

1. The data controller is to communicate all relevant information to the data subject in a **concise, transparent, intelligible and easily accessible form**, and must be aware that duties apply **even where personal data was not collected by the data controller.**

2. The data subject must be **notified about data processing activities** and **be given access to any data held about them** and related information including about **their rights**. The data controller shall implement means to **verify the identity** of any persons making subject access requests.

3. The data subject has the right to have **incorrect information about them corrected** and have **incomplete information corrected** including by supplementary.

Rights of Data Subjects

4 The data subject has the right for their data to be **erased** where it is **no longer necessary**; **consent is withdrawn**; they **object to processing**; the data has been **unlawfully processed**; among other potential reasons

5 The data subject has the right to have **data processing restricted** where the personal data's **accuracy is contested**; processing is unlawful and the subject **requests restriction** rather than erasure; the controller **no longer has use for the data, but the data subject does** (e.g., for a legal claim); or the data subject has **objected pending verification** of whether the grounds of the controller override the subject's interest

6 The data subject has the right to receive their personal data “in a structured, commonly used and machine-readable format and have the right to **transmit** those data to another controller **without hindrance** from the controller to which the personal data have been provided,” where the processing is based on consent or is carried out by automated means.

Rights of Data Subjects

7

The data subject has the right to **object to processing** of their personal data and the controller shall no longer process the personal data **unless** the controller demonstrates **compelling legitimate grounds** for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

8

The data subject has the right **not to be subject to automated decision-making** including profiling with legal (or similar) effects. Exceptions arise based on performance of contract, authorisation by law, and where explicit consent is obtained from the data subject.

For more information…

All partners and research participants can learn more in:

Project Deliverable 7.3:

Ethics Recommendations and Regulatory Framework

which is publicly available on the OPTIMAI website.

OPTIMAI

Thank you

TRILATERAL RESEARCH
Ethical AI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 958264