Project title: European Federation for Cancer Images
Project acronym: EUCAIM
Grant Agreement: 101100633
Call identifier: DIGITAL-2022-CLOUD-AI-02

D*3.1*: [Report on the technical and organizational measures to safeguard the rights and freedoms of data subjects]

Partner(s): [KUL, UV]
Author(s): [Janos Meszaros, Ricard Martinez, Francisco R. Soriano, Isabelle Huys]
Date of delivery: [31\12\2023]
Version: **1.2**

Contents

Executive summary

In response to the growing importance of secondary use of health data within the European Union (EU), this report provides a comprehensive overview of the technical and organizational measures employed to safeguard the rights and freedoms of data subjects, as mandated by the General Data Protection Regulation (GDPR). The EUCAIM is dedicated to the responsible and transparent sharing of health data, underscoring the imperative to strike a delicate balance between innovation and the protection of individuals' privacy.

This deliverable delves into the intricacies of GDPR compliance, outlining the key principles and provisions that guide the lawful processing of health data. Robust technical safeguards, such as state-of-the-art encryption and anonymization techniques, are highlighted to ensure the confidentiality and integrity of the shared information. Furthermore, the organizational measures implemented are discussed, emphasizing the adoption of privacy-by-design principles and the establishment of clear governance structures.

In addition, the report addresses the role of Data Protection Impact Assessments (DPIAs) in identifying and mitigating privacy risks associated with the processing of health data. It illustrates how the project partners diligently assess the necessity and proportionality of data processing activities, striving to minimize the impact on data subjects while achieving the overarching goals of the project.

By examining these technical and organizational measures in detail, the report aims to serve as a valuable resource for project partners. It articulates a commitment to compliance with GDPR and the ethical imperative of safeguarding the rights and freedoms of individuals contributing their health data to the project, thereby contributing to the responsible advancement of healthcare innovation within the EU.

Acronyms and Abbreviations

AI Artificial Intelligence

CJEU Court of Justice of the European Union

DGA Data Governance Act

DoA Description of Actions

EDPB European Data Protection Board

EDPS European Data Protection Supervisor

EHDS Proposal for a Regulation of the European Health Data Space

ENISA European Union Agency for Cybersecurity

EU European Union

GDPR General Data Protection Regulation

HLEG AI High-Level Expert Group on Artificial Intelligence

NIS Network and Information Security

WP Work Package

WP29 Article 29 Working Party

Disclaimer

The opinions stated in this report reflect the opinions of the authors and not the opinion of the European Commission.

All intellectual property rights are owned by the consortium of EUCAIM under terms stated in their Consortium Agreement and are protected by the applicable laws. Reproduction is not authorized without prior written agreement. The commercial use of any information contained in this document may require a license from the owner of the information.

I. Introduction

1) The EUCAIM Project

The EUCAIM Project proposes to deploy a pan-European digital federated infrastructure of FAIR cancer-related anonymized images from Real-World. The infrastructure is designed to preserve the data sovereignty of providers and provide a platform, including an Atlas of Cancer Images, for the development and benchmarking of AI tools towards Precision Medicine. EUCAIM will address the fragmentation of existing cancer image repositories by building on repositories of the AI4HI initiative, European Research Infrastructures and national/ regional repositories and include clinical images, pathology, molecular and laboratory data.

In order to achieve its main aims the EUCAIM project has defined the following Specific Objectives (SO):
SO1. Set up the **Ethical, Legal and Security framework** of EUCAIM, which will define the data access and transfer agreements, the de-identification and anonymisation procedures, and the legal bounds of the project.
SO2. Set up a **Coordinating Entity** that will host the services of the Central Hub and will define the legal model, the rules for participation (for data and service providers and consumers), the recognition models and the operative procedures.
SO3. Integrate and implement the Central Services that will provide a platf**orm for data discovery, data querying and access** to deidentified high-quality data on the federated nodes.
SO4. Follow a data protection and **privacy-by-design and by-default approach** (as established in article 25 of GDPR) to define an Authentication and Authorisation Infrastructure (AAI) and to implement the privacy-preserving technologies needed to fulfil the security agreements.
SO5. Define the **common data models**, interoperability guidelines, best practices, FAIR metrics, tools and standards for the integration of federated data and metadata.
SO6. **Integrate a set of key data providers** of cancer images coming from existing repositories, hospital coalitions, Research Infrastructures, networks and other data providers in the consortium.
SO7. Integrate a **distributed processing environment** including appropriate processing tools, federated learning and computing intensive frameworks with a seamless access to the data resources to implement the on- demand processing by the research users.
SO8. **Monitor data provisioning, data access, data processing**, users, data accesses and other key metrics of the repository for reporting, evaluating and assessing the functionality of the platform.
SO9. Define and **implement the operating bodies** of EUCAIM, which will be in charge of the access, scientific guidance, technical support, training and monitoring of the EUCAIM infrastructure.
SO10. Create an environment for supporting a **collaborative network across already existing Research Infrastructures** such as EATRIS, ELIXIR, BBMRI and Euro-BioImaging.
SO11. Define a **sustainability plan** and implement the necessary structures to be able to operate the repository as a Research Infrastructure beyond the end of the project.

This set of general aims and specific objectives is framed within the broader framework provided by the European Strategy for Data and particularly by the Digital Decade Policy Programme 2030 and the European Health Data Space (EHDS). In this context, guaranteeing the fundamental rights of all actors concerned, and particularly the rights of patients, will be a core principle that has a particular bearing on the design of this deliverable. The EUCAIM Data Repository will process personal data in a GDPR-compliant manner. In addition, the provisions of the Data Governance Act (DGA) must be taken into account[1].

[1] See Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868

The **personal data is anonymised or de-identified** in accordance with GDPR and minimized to protect personal and non-personal data not only at rest but also while in use. The **ethical principles** applicable to artificial intelligence as defined by the European Commission's High-Level Expert Group will be added to those of Biomedical Research and inspire the Project. In addition, the Project will have to adapt the Regulation of the European Parliament and of the Council on the European Health Data Space[2] (EHDS-R), which will have a decisive impact on aspects such as security, interoperability or the processes for generating datasets and the conditions that will facilitate access to them.

The achievement of these main purposes and Specific Objectives necessarily entails the design of a data governance strategy that must reach all possible levels, including technological governance, the definition of an ethical and legal governance model, and governance in management and decision-making processes.

2) Compliance

Within the dynamic landscape of health data utilization, the EUCAIM Project undertakes a focused examination of the technical and organizational measures implemented to ensure **compliance with the General Data Protection Regulation (GDPR), European Health Data Space (EHDS), Data Governance Act (DGA), and the Artificial Intelligence Act (AI Act).** This deliverable provides a systematic overview of the strategies employed to safeguard data subjects' rights and freedoms while facilitating the responsible secondary use of health data.

As we delve into the intricacies of legal frameworks, the subsequent sections outline the **technical measures** deployed and those planned for implementation. This includes a comprehensive range of security measures, encryption protocols, access management strategies, and disaster recovery planning, aimed at upholding the confidentiality, integrity, and availability of health data.

The **organizational measures**, equally pivotal, are presented in detail. From awareness initiatives to data access governance, risk mitigation strategies, and adherence to data protection impact assessments, each aspect is objectively analyzed to showcase the concerted efforts to fortify the project's data security framework.

The **intersection of AI and security, along with an in-depth exploration of Data Protection Impact Assessment**, adds granularity to our commitment to transparency and ethical data processing. By systematically addressing risk evaluation, necessity and proportionality assessments, and the identification of mitigating measures, this deliverable offers a pragmatic guide to our approach.

In providing this comprehensive overview, the **EUCAIM Project** seeks to transparently communicate its commitment to **legal compliance, technological rigour, and organizational resilience**.

[2] See Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0197

II. Legal Background for technical and organizational measures

In the ever-evolving landscape of data-driven innovation, the responsible handling of personal data, especially within the health data domain, is paramount. **This chapter introduces the most important regulations** that contour our approach to safeguarding the rights and freedoms of data subjects. With a primary focus on the GDPR, the unique challenges posed by the health data space, and the emerging regulatory landscape marked by the AI Act. Nevertheless, variations in national regulations within the EU underscore the need for partners and their Data Protection Officers (DPOs) to stay informed and comply with these diverse measures.

1) General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a comprehensive data protection and privacy regulation implemented by the European Union (EU) in 2018. It establishes **a framework for the collection, processing, and storage of personal data of EU citizens**, granting them greater control over their information. The GDPR imposes strict requirements on organizations handling such data, including the need for clear consent, the right to access and rectify personal information, and the obligation to implement robust security measures to safeguard data. Non-compliance with GDPR can result in significant fines, making it a crucial legal framework for protecting individuals' privacy rights.

Information security plays an instrumental role in guaranteeing fundamental rights. Therefore, the **GDPR defines it as one of its fundamental principles** in Article 5, as an essential objective, and as an obligation for controllers and processors. Under the 'risk-based approach', the controller must take appropriate measures in accordance with the state of the art.

GDPR Recital 78
Personal data should be processed in a manner that ensures **appropriate security and confidentiality** of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.[3]

GDPR Article 32
Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the **controller and the processor shall implement appropriate technical and organisational measures** to ensure a level of security appropriate to the risk, including inter alia as appropriate:
(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

[3] GDPR Recital 39

The European Data Protection Board highlighted the important of data protection by design and provided a non-exhaustive list of the most important requirements in the **guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020**[4]

"85. Key design and default integrity and confidentiality elements may include:

· **Information security management system (ISMS)** – Have an operative means of managing policies and procedures for information security.

· **Risk analysis** – Assess the risks against the security of personal data by considering the impact on individuals' rights and counter identified risks. For use in risk assessment; develop and maintain a comprehensive, systematic and realistic "threat modelling" and an attack surface analysis of the designed software to reduce attack vectors and opportunities to exploit weak points and vulnerabilities.

· **Security by design** – Consider security requirements as early as possible in the system design and development and continuously integrate and perform relevant tests.

· **Maintenance** – Regular review and test software, hardware, systems and services, etc. to uncover vulnerabilities of the systems supporting the processing.

· **Access control management** – Only the authorized personnel should have access to the personal data necessary for their processing tasks, and the controller should differentiate between access privileges of authorized personnel.

o **Access limitation (agents)** – Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly.

o **Access limitation (content)** – In the context of each processing operation, limit access to only those attributes per data set that are needed to perform that operation. Moreover, limit access to data pertaining to those data subjects who are in the remit of the respective employee.

o **Access segregation** – Shape the data processing in a way that no individual needs comprehensive access to all data collected about a data subject, much less all personal data of a particular category of data subjects.

· **Secure transfers** – Transfers shall be secured against unauthorized and accidental access and changes.

· **Secure storage** – Data storage shall be secure from unauthorized access and changes. There should be procedures to assess the risk of centralized or decentralized storage, and what categories of personal data this applies to. Some data may need additional security measures than others or isolation from others.

· **Pseudonymization** – Personal data and back-ups/logs should be pseudonymized as a security measure to minimise risks of potential data breaches, for example using hashing or encryption.

· **Backups/logs** – Keep back-ups and logs to the extent necessary for information security, use audit trails and event monitoring as a routine security control. These shall be protected from unauthorised and accidental access and change and reviewed regularly and incidents should be handled promptly.

· **Disaster recovery/ business continuity** – Address information system disaster recovery and business continuity requirements to restore the availability of personal data following up major incidents.

· **Protection according to risk** – All categories of personal data should be protected with measures adequate with respect to the risk of a security breach. Data presenting special risks should, when possible, be kept separated from the rest of the personal data.

· **Security incident response management** – Have in place routines, procedures and resources to detect, contain, handle, report and learn from data breaches.

[4] • EDPB, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default" Version 2.0. Adopted on 20 October 2020, <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article- 25-data-protection-design-and_en>.

· **Incident management** – Controller should have processes in place to handle breaches and incidents, in order to make the processing system more robust. This includes notification procedures, such as management of notification (to the supervisory authority) and information (to data subjects)

2) The European Health Data Space (EHDS)

Since EUCAIM aims to provide a **secure processing environment (SPE),** aligned with the European Health Data Space, it is crucial to align with the EDHS proposal.[5] The European data strategy of February 2020 announced the creation of data spaces in 10 strategic fields.[6] The first legislative proposal to emerge in a specific area was for a European Health Data Space (EHDS).[7] The proposed EHDS' main objectives are three-fold, namely to: 1) **increase control for natural persons** over their electronic health data, 2) create a legal framework consisting of **trusted governance mechanisms** and a secure processing environment, and 3) contribute to a genuine **single market for digital health products and services**.[8]
The EHDS builds upon legislation such as the GDPR, the medical devices and cybersecurity legal frameworks,[9] the proposed Data Act and AI Act. The EHDS proposal establishes rules for the primary and secondary use of data. Primary use is defined as "the processing of personal electronic health data for the provision of health services",[10] whereas secondary use encompasses the use of electronic health data for broader needs, such as health research or public policy.[11]

EHDS Proposal Recital 54.
The health data access body or the data holder providing this service should remain at all time in **control of the access to the electronic health data** with access granted to the data users determined by the conditions of the issued data permit. Only non-personal electronic health data which do not contain any electronic health data should be extracted by the data users from such secure processing environment. Thus, it is an essential safeguard to preserve the rights and freedoms of natural persons in relation to the processing of their electronic health data for secondary use.

EHDS Proposal Article 50
Secure processing environment
1.The health data access bodies shall provide access to electronic health data only through a secure processing environment, **with technical and organisational measures and security and interoperability** requirements. In particular, they shall take the following security measures:
(a)**restrict access** to the secure processing environment to authorised persons listed in the respective data permit;
(b)minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art technological means;

[5] See Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0197

[6] https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[7] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space COM/2022/197 final.

[8] Explanatory memorandum accompanying the EHDS proposal and EHDS proposal Recital 1

[9] Regulation (EU) 2017/745 on medical devices, Regulation (EU) 2017/746 on in vitro diagnostic medical devices, Directive 2016/1148 on security of network and information systems

[10] EHDS proposal Article 2(2)(d)

[11] EHDS proposal Article 2(2)(e) and Chapter IV; Marcus et al. The European Health Data Space. Study requested by the ITRE committee, December 2022.

(c)limit the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals;
(d)ensure that data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;
(e)keep **identifiable logs of access** to the secure processing environment for the period of time necessary to verify and audit all processing operations in that environment;
(f) ensure **compliance and monitor** the security measures referred to in this Article to mitigate potential security threats.

2.The health data access bodies shall ensure that electronic health data can be uploaded by data holders and can be accessed by the data user in a secure processing environment. The data users shall only be able to download non-personal electronic health data from the secure processing environment.
3.The health data access bodies shall ensure **regular audits** of the secure processing environments.
4.The **Commission shall, by means of implementing acts, provide for the technical, information security and interoperability requirements for the secure processing environments**. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).

3) Data Governance Act

The Data Governance Act (DGA) is seeking to establish a framework for the responsible and sustainable use of data within the European Union. It aims to **increase data availability by facilitating data sharing, promote trust and security in data handling**, and foster innovation and competitiveness. The DGA introduces guidelines for data intermediaries, implements a data access obligation, and proposes a data quality framework to achieve these objectives.[12]

DGA Article 2
(20) '**secure processing environment'** means the physical or virtual environment and organisational means to ensure compliance with Union law, such as Regulation (EU) 2016/679, in particular with regard to data subjects' rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, as well as with applicable national law, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms;

4) Artificial Intelligence Act (AI Act)

At the time of writing this Deliverable, the final text of AI was still not reachable, therefore, the authors refer to the **proposal**. [13]

[12] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)

[13] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach, <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>.

(45a) The **right to privacy and to protection of personal data** must be guaranteed throughout the entire lifecycle of the AI system. In this regard, the principles of data minimisation and data protection by design and by default, as set out in Union data protection law, are essential when the processing of data involves significant risks to the fundamental rights of individuals. Providers and users of AI systems should implement state-of-the-art technical and organisational measures in order to protect those rights. Such measures should include not only anonymisation and encryption, but also the use of increasingly available technology that permits algorithms to be brought to the data and allows valuable insights to be derived without the transmission between parties or unnecessary copying of the raw or structured data themselves.

(50) The **technical robustness** is a key requirement for high-risk AI systems. They should be resilient against risks connected to the limitations of the system (e.g. errors, faults, inconsistencies, unexpected situations) as well as against malicious actions that may compromise the security of the AI system and result in harmful or otherwise undesirable behaviour. Failure to protect against these risks could lead to safety impacts or negatively affect the fundamental rights, for example due to erroneous decisions or wrong or biased outputs generated by the AI system. Users of the AI system should take steps to ensure that the possible trade-off between robustness and accuracy does not lead to discriminatory or negative outcomes for minority subgroups.

(51) **Cybersecurity** plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. Cyberattacks against AI systems can leverage AI specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial attacks or confidentiality attacks), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. To ensure a level of cybersecurity appropriate to the risks, suitable measures should therefore be taken by the providers of high-risk AI systems, as well as the notified bodies, competent national authorities and market surveillance authorities, also taking into account as appropriate the underlying ICT infrastructure. High-risk AI should be accompanied by security solutions and patches for the lifetime of the product, or in case of the absence of dependence on a specific product, for a time that needs to be stated by the manufacturer.

II. Technical measures implemented, and to be implemented

In this part, we will describe in detail which technical measures are already in place and those that are planned to be implemented during the development, testing, and application of the services in the EUCAIM Project. **This is not an exhaustive list of measures. The listed measures and additional ones need to be continuously reassessed according to the risks and state-of the art technology.** The status of current implementation or future ambition are indicated for each single measure:

1) Secure Processing Environment

EUCAIM provides a secure processing environment while providing flexible requirements to fit a wide range of use cases. Although security requirements will be further refined throughout the project, the basis will be the following:

- Users of the platform will be properly identified and will need to register to the platform to access the services of EUCAIM. **Only registered users** will be able to submit access data access request proposals.
- **Access to restricted data** will be made through either Virtual Research Environments, with on-site access to data, restricting downloading the data out of the platform and providing users with tools and resources to process the data; or blind distributed processing in which users will be able to run processing pipelines without being able to display the data.
- Actions performed in the platform will be registered in a non-repudiable form, and system administrators will be able to browse these **logs** when requested.
- The platform will go through a Privacy Assessment and Cyber security analysis.
- All communications will be performed under **secure protocols and encrypted channels**.
- Data in rest will be stored unencrypted, but access to the physical resources will be **restricted** to the system administrators and developers of the platform.
- **Applications will be audited** prior to be registered in the platform and will follow strict guidelines in terms of security and vulnerabilities.

These points are described in more detail in the following subsections.

2) Pseudonymization or anonymization of personal data

Data Providers send or make their data available in pseudonymized or anonymized form, according to their local requirements.

Pseudonymization (art. 4 (5) GDPR) is a data management and de-identification procedure that increases privacy by replacing the identifying fields of individuals by using one or more artificial identifiers, or pseudonyms, that cannot be linked directly to their corresponding nominative identities. Pseudonymized data is usually still regarded to be personal data and remains under the scope of the GDPR in the EU Member States.

As regards anonymization, Recital 26 of the GDPR states that the principles of data protection do not apply to anonymous information (more on this concept in D5.1 and the pseudonymization strategy). It should be ensured that anonymization is engineered appropriately in order to place the processing and storage of data declared as anonymous outside the scope of GDPR.

However, there is a recent relevant regulatory development concerning the April 2023 ruling of the **European General Court on the case Single Resolution Board vs the European Data Protection Supervisor.** With respect to this development, **potential implications for EUCAIM could be significant, depending on the outcomes.** This is because the case concerns the fundamental question of how the key concepts “personal data” and “anonymous data” should be interpreted under the GDPR. The ruling by the General Court favors the so-called “**contextual**” interpretation of the concepts, which is concerned with whether data can be related to an identifiable natural person by a particular party; if the party cannot link the data to an identifiable individual by employing means reasonably likely to be used in the context of re-identifiability, the data should be deemed anonymous from this party's perspective. This, however, differs from the **"absolute" interpretation** of the concepts, which holds that a piece of information must be considered personal data if it is possible (through means reasonably likely to be used) to attribute it to a natural person by any party. The absolute view on the concepts of personal data and anonymity is based on the literal interpretation of Recital 26 GDPR and has been embraced by most EU data protection authorities. Consequently, the ruling of the General Court has been challenged in the Court of Justice of the European Union with outcome pending.

EUCAIM will provide tools to perform the anonymization or pseudonymization of the data for those providers which don't have their own method to do so. Regarding metadata in imaging studies, based on the strategies followed in the AI4HI projects, the EUCAIM tools will de-identify the data based on a de-identification profile for each cancer type. This profile specifies how to process the DICOM tags, removing those that contain Personal Identifiable Information such as the Institution Name and Address, and the Patient's Name. In addition, it will replace other tags with values of similar meaning that can still be of interest to the final user without compromising the identification of the patient.

Concerning **clinical data**, EUCAIM will define a set of variables to be provided by cancer type. However, the information provided will be analyzed and the variables with personal information will be removed or replaced.

Moreover, a **wizard tool** will be developed under the scope of EUCAIM. This tool will support the identification of risks and propose ways to mitigate them. In addition, it will raise awareness on weak points of each process, foster a secure-by-desing anonymization planning and facilitate compliance to EUCAIM requirements and accountability obligations.

3) Encryption

Encryption is the procedure that converts clear text and original information or data into a code using a key, where the outgoing information only becomes readable again by using the correct key.
Encryption may be used in various systems, such as:

- Hard drive (hardware) (not visible for user)
- Storage platform system (not visible for user)
- Operating system level encryption (IT administrators' driven), e.g., directory or storage partition specific
- File or application specific encryption (user or middleware/application driven).

Encrypted contents are basically unreadable for third parties who do not have the key. Encryption is the best way to protect data during transfer and also a manner to secure stored personal data. It also reduces the risk of abuse within a company, as access is limited to authorized people with the right key (https://gdpr-info.eu/issues/encryption/).

4) Access control management

Access control management – Only the authorized personnel should have access to the personal data necessary for their processing tasks, and the controller should differentiate between access privileges of authorized personnel.

o **Access limitation (agents)** – Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly.
o **Access limitation (content)** – In the context of each processing operation, limit access to only those attributes per data set that are needed to perform that operation. Moreover, limit access to data pertaining to those data subjects who are in the remit of the respective employee.
o **Access segregation** – Shape the data processing in a way that no individual needs comprehensive access to all data collected about a data subject, much less all personal data of a particular category of data subjects.

In order to avoid fraudulent access or misuse of data during the development and application of EUCAIM, logging access and measures to manage incidents need to be adopted. Each data request and access will be logged in the Platform.

Details are provided in the following sections.

5) User registration and Passwords

In order to access the platform, **users have to register**. **An internal document describing the process is available in the URL** https://docs.google.com/document/d/12fJwhPLqk1x6NIm9glGLd-kSCjA80maLIicT8AdLBBE/edit?usp=sharing. Users must create a Life Sciences AAI account, preferably using their own institutional Identity Providers. This will permit users to be identified, but it will not grant access to EUCAIM's data or services. In order to have access to the services, users will need to request membership to the EUCAIM group. This process is supervised by a human who checks the validity of the request prior to accepting the membership. Being a member of the EUCAIM group only grant access to the catalogue, explorer, helpdesk and negotiator services. Access to data will require the submission of an access request proposal and the approval of the Access Committee.

User's password restrictions are set in their Identity providers (e.g. university or hospital) and EUCAIM does not have access to the password or know the content of local policies and procedures, which indeed may vary from different providers and services. However, EUCAIM Platform will provide guidelines and best practices. Moreover, multi-factor authentication will be evaluated.

6) Protecting internal network

The services of EUCAIM run in a **Kubernetes cluster** and are connected through an overlay network supported by Cillium (https://cilium.io/). External access is provided through a Kubernetes ingress proxy to the Dashboard, Catalogue, Negotiator and Explorer services. Those services can only be accessed through the 443. Critical services, such as the Kubernetes console, are only accessible through the institutional network (either physically or through a VPN). Databases are only accessible in the internal overlay network. Only platform administrators have access to the internal network.
Developers can access a separate test deployment which runs under similar conditions, but using a separate overlay network.

7) Securing servers

EUCAIM applies a protocol of **role separation in all the services**, minimising the risk of a malicious user accessing some user's credentials. **In this way, we separate three levels: Physical servers, virtual servers and platform services.**

Since general terms, servers must be well protected against incidents with several measures, such as:

a. Allowing only qualified individuals to access the tools and administration interfaces;
b. Defining a specific, more secure password policy for server administrators;
c. Installing updates and carrying out backups and system configuration regularly;
d. Implementing protocols ensuring encryption and authentication, as a minimum for any online data exchange and verify its proper implementation via the appropriate tools;
e. Server administration operations should be carried out via a dedicated and isolated network, accessible only with strong authentication and enhanced traceability.

To avoid fraudulent incidents on the developer's and systems administrators' side, firewall and separated admin and user accounts are necessary. There are various teams handling different system components such as storage, network, physical servers, operating systems, cloud middleware, container platforms, storage middleware, software development, software administration, log and monitoring systems etc. User authentication and authorization processes are carefully reviewed. Malware detection software are installed and monitored. Providers, users and administrators have the legal obligation to inform the consortium whether and when data breaches or leakages occur. Moreover, users are also encouraged to protect their laptop or local servers with antivirus software and be aware of possible scam sites or emails. Each user institution is encouraged to adopt procedures and policies for preventing fraudulent access, data breaches and leakages.

The **EUCAIM platform comprises a set of central services and the services of the federation**. The central hub services run on a cloud infrastructure managed at the UPV. The cloud infrastructure is physically installed in an access-restricted room, secured with an electronic key. The administrator credentials of the cloud infrastructure are managed by the UPV system administrator team. EUCAIM platform developers do not have this privileged access. EUCAIM platform system administrators hold the administrator-privileged credentials of the virtual servers. EUCAIM platform developers hold managing credentials only at the level of the Kubernentes namespace where their service runs.

8) Regular backups

Appropriate backup process for the case that the systems suffer a physical or technical incident are adopted. There is data mirroring between the two data repositories. Platform configurations are stored in back-ups form where the system can be recovered (e.g. in the case of server breaks, or if a database is corrupted).

The platform images are backuped in a separate server, stored in the same institution but not directly mounted in the platform to avoid the propagation of ransomware. Periodic backups of the database are also performed.

9) Archiving and destroying personal data

The data which is no longer necessary for the purpose for which it was collected should be archived or removed. Data contributed to EUCAIM usually remains stored for the lifetime of the project, but it might be stored beyond the project's lifetime. The retention time for the Personal Data of Users and Providers having accessed the EUCAIM is still to be determined, but it will remain as long as required for security considerations and scientific reasons. The data retention policy is detailed in the Data Management Plan.

10) Maintenance of systems

All computer hardware has a limited lifecycle, thus servicing and maintaining them is crucial. However, third parties responsible for repairing them might pose risks, thus deleting data from the devices is crucial before sending them out to third parties.

The **project has selected a long-term support version of the operating system** (ubuntu 22.04) for both the virtual servers and the Kubernetes containers. EUCAIM servers have been deployed following an Infrastructure as Code (IaC) procedure. This approach facilitates the reproducibility of the platform and the upgrading of the services. Upgrades of software packages and platform services will be tested in the test environment.

11) Securing transmission of data with other organizations

In EUCAIM, data transfer protocols adopt security measures and ensure that transmissions only take place in a secure manner by applying encryption in upload and transfer services. External access is only available to secured endpoints and through encrypted communication protocols, as described before. Data access is provided through a **VNC desktop client** (in the case of the sites providing in-situ processing) or the distributed processing interface. Therefore, data is not transferred out of the boundaries of the federated platform. In both cases, **encrypted network protocols** are used.

II. Organizational measures implemented, and to be implemented

Similar to technical measures, we will illustrate hereafter the organizational measures that are already adopted and those that are planned to be implemented by the EUCAIM partners and the Platform.

1) Constant awareness on data security

Building awareness on data security can be achieved by assigning some responsible people for this area and providing them with resources and real power to enforce these tasks.
Data centers are already implemented:

a) co-ordination between key people in the organization (e.g., between the IT and security manager(s))
b) a proper monitoring and protecting the access to premises or equipment of the Platform.

The EUCAIM Platform system administrators ensure that the systems are being well maintained and patched against known security vulnerabilities. They also systematically check that the security measures remain appropriate and up to date.

2) Security and Confidentiality Agreements with third parties

Third-party operators, e.g., for hardware maintenance, need to sign necessary security and confidentiality contracts with subcontractors and are subject to adequate supervision by each data center. Each data center has its own policy in this regard.

3) Data access and data processing only by authorised people

With regard to personal and non-personal data, access controls will be implemented to prevent unauthorized persons from gaining access to data processing systems.
In EUCAIM, appropriate authentication methods will be used, and specific policies on the control of access rights will be defined.
The Users' access rights will be withdrawn as soon as they are no longer authorized to access an IT resource, as well as at the end of their contract and a regular review of the access rights will be carried out.
As described in the previous section, **three levels of access are implemented**:

- **Anonymous access**. Limited to the public section of the Dashboard and the Catalogue.
- **Users identified by LS AAI and registered in the EUCAIM VO group**. They can access the full information in the Catalogue, the Federated Search and the Negotiator.
- **Users who have access granted to data**. Users who went through the access request negotiation procedure and have access granted. They can access the data and/or the distributed processing, depending on the conditions of the dataset and the hosting site.

4) Measures to mitigate the risks of data security

EUCAIM requires all Users to adopt specific and appropriate technical and organizational measures to protect the Data, and the legal commitment to such adoption can occur through legally binding instruments regarding transfer and access to data, such as Data Transfer Agreements (DTA), Data Access Agreements (DAA), or other contracts, as appropriate on the basis of the further determination of the roles of the User Organizations.

5) Data processors and subcontractors

In case of processors or sub-processors, Data Processing Agreements with each of the third parties who process personal data need to be signed before the start of the processing. The agreement details the parties, rights and duties, and adequate safeguards of the processing and fulfils other requirements of GDPR (see Art. 32 (4) and 28 (3) GDPR).

For sub-processing, each Subcontractor is bound to the same obligations as the Data Processor, and the latter has to be transparent about the identity of the Subcontractor towards the Data Controller(s) by communicating the Subcontractor's identity in the Data Processing Agreement itself or – if Data Processing Agreements contains a general authorization for engagement of sub-processors - by informing the Data Controller(s) in writing about the identity and contact details of the proposed Sub-processor, any replacement thereof, in advance thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object. Subcontractors always need to provide guarantees that they are reliable and that they possess the required knowledge and resources.

Due Diligence for Processor Selection

The EUCAIM Project employs a rigorous due diligence procedure to select processors, ensuring adherence to data protection standards. The process involves:

1. **Initial Assessment:** Clearly defining processing needs and mapping data flows.
2. **Pre-screening:** Checking legal compliance and evaluating security measures.
3. **Request for Information:** Reviewing documentation, seeking references, and evaluating past performance.
4. **Data Protection Impact Assessment (DPIA):** Identifying and mitigating risks associated with processing activities.
5. **Legal Contractual Framework:** Defining clear contractual terms, including data processing agreements.
6. **Ongoing Monitoring:** Conducting regular audits and incident response planning.
7. **Continuous Improvement:** Establishing feedback mechanisms and adapting to regulatory changes.

This meticulous procedure aims to build a network of trusted entities, ensuring transparency, accountability, and compliance throughout the project lifecycle.

6) Raising staff awareness and ensuring security practices

Human error is a leading cause of breaches in security. This can be caused by simply sending an email to the incorrect recipient or opening an email attachment containing malware and clicking on a corrupted link. Both at the level of the hosting data centers and of the Data Contributors, the staff needs to be trained to recognise these threats, such as phishing emails and other malware. It is crucial that EUCAIM partners, data providers and users raise awareness of privacy among the staff by informing and educating them about the measures implemented to deal with the risks and the potential consequences. This can be conducted by organising awareness-raising sessions, regularly sending updates on the relevant procedures for the individuals' roles and sending them reminders via e-mail. Each organisation is responsible for its staff training. However, on the consortium level, WP2 and WP3 both provide training, related to privacy and security in a limited extent.

7) Data protection impact assessments

It is crucial to assess high-risk data processing activities and developing mitigating solutions to prevent or reduce risks. A Data Protection Impact Assessment (DPIA) is required under the GDPR (art. 35) when processing is likely to involve "a high risk" to the rights and freedoms of natural persons.
In the case of EUCAIM, special categories of data (such as health data or biometric data) are being processed and being there a high risk for rights and freedoms, a DPIA is therefore required. **The primary responsibility for the DPIA lies with the individual Controllers, in particular the Data Contributors**.

8) Agreements between the Data Providers and with the technical partners of the EUCAIM Consortium

It is important to draft and sign agreements between Data Providers and with the technical partners building the Platform. Such agreements depend on the actual roles and responsibilities, which are currently discussed in the consortium.

9) Data Access Agreements

For future data usage, a **Data Access Agreement template** will be drafted. This template will ensure that the usage of the data will be limited to the scope approved by the Data Access Committee and\or Data Providers.

10) Information security policies and procedures

The Platform will adopt information security policies and procedures that concern specific areas such as remote access and asset management.

11) Disaster Recovery Plan

EUCAIM will draft a Disaster Recovery Plan: this document will review the risks for a major incident and the actions to recover the services.

12) Reviews and Audits

After indicating all the policies, controls and measures in place or expected, it is important to check whether they are effective.
The Platform services shall be audited against standards, which proves that the hosting organizations can control, manage and continuously improve information security in their services and operations. Regular security scanning and penetrations tests will also be done.

13) Vulnerability Management and Penetration Testing

As regards to 'Vulnerability Management' (VM), which is an ongoing process to identify critical vulnerabilities, the platform operators do continuous vulnerability monitoring and security updates for various software.
As regards to 'Penetration Testing' (PT), which is a periodic audit checking if there are vulnerabilities, to judge whether their company data is adequately protected, precisely through penetration tests.

These tests will be performed by the cybersecurity experts in the consortium (S2-Grupo) after the M18 release.

14) Security architecture

EUCAIM will follow a hybrid federated-centralised model, preserving the independence of Research Infrastructures and existing thematic, national or institutional repositories and providing centralised governance corresponding to a higher coordination layer that provides a cohesive and coherent structure in the access to the data. EUCAIM will also support observational studies and will provide long-term preservation and sustainability for the data collected in these studies. This architecture is implemented through the following main types of services:

- A **public catalogue** that gathers the collections from the different providers with the collections' metadata and enables the user to browse and explore the existing data.
- A **federation layer** comprising services that make the data compliant with FAIR principles, connecting the different repositories to the EUCAIM core services' layer using a Federated Query service and a Hyperontology that will facilitate querying the data stored in the federated providers platforms regardless of the data models that they have adopted.
- A set of core services providing a coherent and seamlessly connected **Authentication and Authorisation Infrastructure (based on Life Sciences AAI),** a monitoring service to improve operation, a traceability service to log all the data-related interactions of users and services to support the recognition models and to monitor the fulfilment of the Terms of Usage, a federated processing service, and a third-party data transfer service for temporary copies of datasets on High-Performance Computing sites.
- A set of **organisational services such as a helpdesk system** to support users and manage incidences and a security incident response service.
- A **Dashboard** that integrates all the functionality in a coherent environment, enabling users to browse and search datasets, request access to them, access data in the federation according to each repository's access conditions, and browse tools and pipelines to run them on a containerised environment at the provider's side.
-

Figure 1 shows the architecture of the EUCAIM repository. Users will register on the **EUCAIM platform**, which will entitle them to **browse and search the datasets available** in the federation. The user will be provided with **aggregated information and metadata** from the dataset matching their criteria, indicating the provenance, the access conditions and the processing services available at the provider side. Users will be able to **request access to the actual data, which will be selectively granted**. Subject to the Access Conditions of the providers, **granted users will be able to explore, process the data on-site and/or through federated processing services**, using containerised applications from the federation marketplace. In the case of intensive data processing, data could be temporarily transferred to a High-Performance Computing service. **The central storage of EUCAIM will be integrated as any other node** in the federation.

Providers will commit to a given service level, which will define the expected availability of services, the quality and quantity of the data and the access conditions. EUCAIM will provide them with tools, interoperability plugins and services to facilitate the integration into the federation, and will provide recognition by publishing aggregated data on the usage of the data of each provider. Providers will also benefit from networking opportunities, the creation of communities and the participation in projects by being members of EUCAIM.

The **federated central hub will create the governance of the EUCAIM infrastructure to regulate the onboarding of data and tools providers and data users**. The onboarding procedure will define the Service Level Agreement, the technical interoperability, data quality metrics, compliance to FAIR principles and data standards so datasets from providers can be findable in the central hub Dashboard. The Dashboard will provide the first step for the data access process, collecting the necessary information and forwarding the access request to the provider for the final decision.

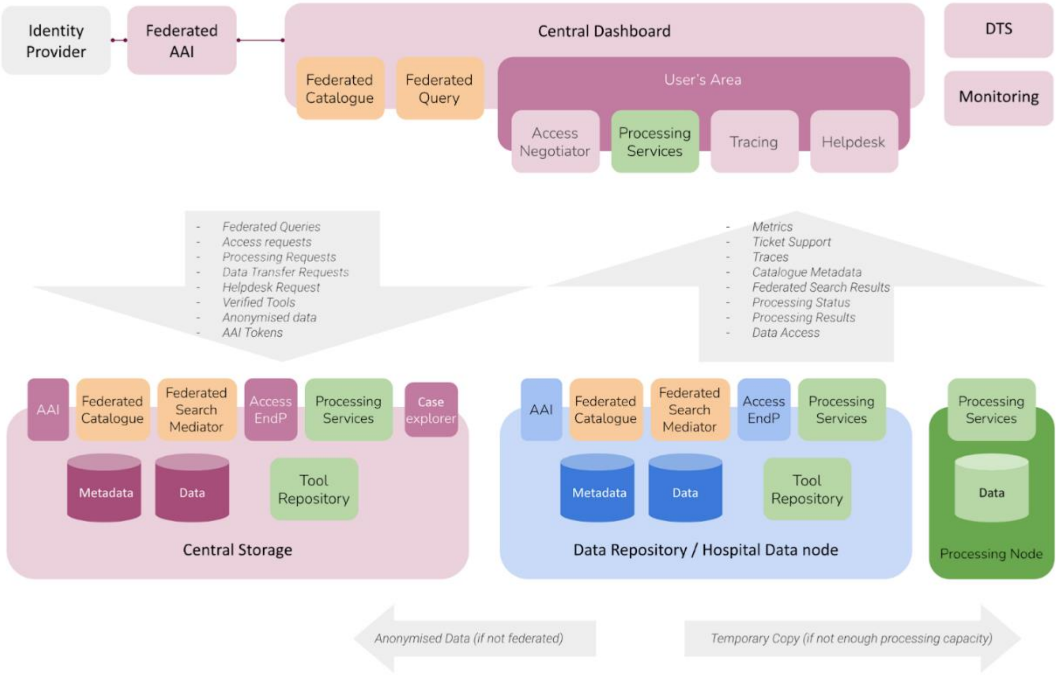


Figure 1. High-level architectural view of EUCAIM.

The **Authentication and Authorisation Infrastructure (AAI) architecture** relies in the Life Science AAI (LS AAI). The services of the central hub will directly rely on the LS AAI for Authentication and Authorisation, which will use external institutional IdPs for authentication. The architecture should be interoperable with external federated providers which should trust on the LS AAI for authentication, but could manage their own AAI instances. This way, a user registered in the LS AAI could browse and explore the dataset's metadata available in the central hub, whose services will trust on the LS AAI tokens and will use the group entitlements as authorisation information. The use of GA4GH token sets will also be considered.

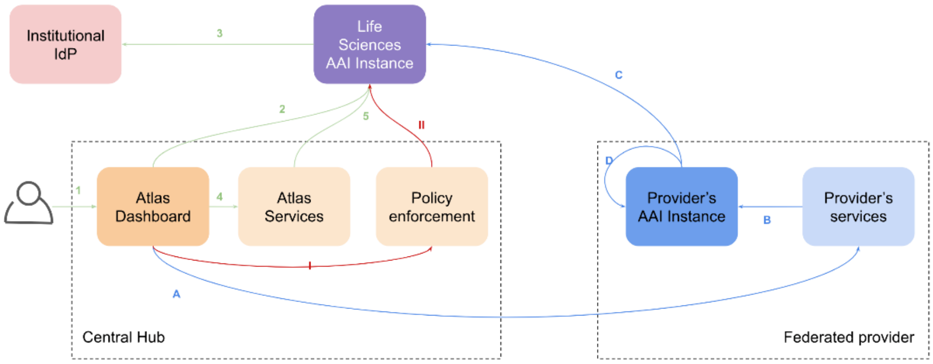


Figure 2: Architecture Diagram for the AAI services

Figure 2 shows the interactions among the main components. A user will access the Dashboard (1) and get authenticated through the LS AAI (2), which will trust on the Institutional IdP (3), providing a token back to the atlas. Other services of the Atlas (4) can verify the token in the LS AAI for verifying the identity.

When a user gets the authorization to access a specific provider (I), the policy enforcement component of the Atlas could trigger the inclusion of the user in a specific group (II) (this process could be human-based). This will allow the user accessing the dashboard to access the provider services. The Atlas Dashboard will directly forward to the provider services (A), which will request the login through the provider's AAI (B). If the user is registered with LS AAI as IdP, the authentication (C) will be automatic. Then, if the user is the first time it logs in, the Provider's AAI instance can create the user automatically if the proper group in LS AAI is given (D). However, this process could be more restrictive if the provider does not accept this approach (e.g. by requesting a full registration in the system). This approach will only request that the Federated Providers trust LS AAI as IdP and the configuration of the AAI provider's instance to create users automatically (e.g. Keycloak can do it).

This approach will require:

- Creation of an EUCAIM group with different roles for fine-grain differentiation of access rights.
- Implement the dashboard with the LS AAI as major AAI, including registration.
- Support the LS AAI from the provider's side, potentially supporting the management of groups/roles for the authorisation.

The **AAI should manage different groups/roles so the permissions can be defined**. Depending on the granularity, we could aim for individual group permissions for providers or a coarse level. An example of roles could be:

- EUCAIM General role. This is the minimum role given to the registered users, and allows a user to browse the catalogue and search for aggregated metadata. It will be granted automatically when a user registers the platform.
- EUCAIM Federation Requester. This is a catch-all role given to all the users that have access granted. Providers can decide to authorise this role for a coarse-grain access permission.
- EUCAIM Provider X Requester. To implement fine-grained access to a provider by a user, we could create a separate group/role per provider. In this way, a user may be authorised to selectively access the providers. Providers can simply implement the authorisation rules for their own group.
- EUCAIM Provider. Providers will need this role to access the provider's page and link their services to the federation.

15) Physical security

Physical security underscores the imperative of **safeguarding data integrity and ensuring the resilience of organizational infrastructure.** Priority is assigned to **fire security**, with the implementation of advanced fire detection and suppression systems deployed across facilities. Regular assessments and drills can validate the effectiveness of these measures, enabling swift responses to potential threats and minimizing the impact on data integrity.

Furthermore, physical premises need to incorporate **rigorous access controls**, such as biometric authentication systems, surveillance cameras, and secure card access mechanisms. These measures function to regulate entry and exit points, bolstering the security of physical infrastructure against unauthorized access and contributing to the protection of data. Additionally, the **distribution of backup facilities across diverse physical locations** mitigates the risk of data loss due to unforeseen events, enhancing redundancy and resilience in our data storage infrastructure. This comprehensive approach to physical security underscores the commitment to maintaining the confidentiality and operational continuity of data management systems.

16) Data breach

According to the GDPR “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.” Given its importance, the table below highlights the obligation to notify the supervisory authority and the data subject affected by the breach:

Notification to the supervisory authority, GDPR Article 33	Communication to the data subject, GDPR Article 34
• When a personal data breach occurs, the controller must notify the personal data breach to the supervisory authority competent in accordance with Article 55 GDPR. • The notification should take place without undue delay and not take longer than 72 hours after having become aware of it. Notifications that were not made within 72hours shall be accompanied by the reasons for the delay. • Data processors who are on notice of a data break must notify the responsible controller without undue delay after becoming aware of the breach. • The notification shall contain a description at least of the information referred to in Article 33(3)(a-d) GDPR.	• If a data breach is likely to result in a high risk to the rights and freedoms of the data subject, the controller must communicate said breach to the data subject. • The communication to the data subject shall take place without undue delay. • The communication must inform the data subject in a clear and plain language. • The communication shall contain a description of the nature of the data break and contain at least theinformation and measures referred to in Article 33(3)(lit. b, c, and d) GDPR.

III) AI Security

The security of AI-driven systems is not explicitly introduced in the EU's Cybersecurity Strategy for the Digital Decade.[14] However, it is crucial not to overlook its significance. The European Union Agency for Cybersecurity (ENISA) has released multiple reports about cybersecurity and algorithms.[15] Given EUCAIM's focus on medical images, it is worth highlighting the ENISA report that explores cybersecurity and privacy concerns in AI applications related to medical imaging diagnosis.[16] It identifies multiple aspects relevant in this context, namely the assets, actors and their roles, relevant processes, AI algorithms and the requirements related to cybersecurity and privacy.[17]

Both cybersecurity and privacy are crucial aspects. However, achieving a balance between the two can be challenging and may lead to trade-offs, such as compromises in accuracy.[18] In September 2022, the European Commission introduced a directive proposal known as the AI Liability Directive,[19] aiming to adjust non-contractual civil liability rules concerning AI. The primary objective is to safeguard individuals impacted by harm resulting from the engagement of AI systems. Notably, the draft directive does not prescribe specific cybersecurity requirements. Instead, it acknowledges cybersecurity as a pertinent factor in the proposal for particular categories of AI systems. This mention serves to underscore the significance of addressing cyber vulnerabilities in order to raise awareness.[20]

Moreover, the **High-level expert group on artificial intelligence (HLEG AI) ethical principles** will now be a binding legal standard by the AI Act.

Article 4

General principles applicable to all AI systems

1. All operators falling under this Regulation shall make their best efforts to develop and use AI systems or foundation models in accordance with the following general principles establishing a high-level framework that promotes a coherent human-centric European approach to ethical and trustworthy Artificial Intelligence, which is fully in line with the Charter as well as the values on which the Union is founded:

a) '**human agency and oversight'** means that AI systems shall be developed and used as a tool that serves people, respects human dignity and personal autonomy, and that is functioning in a way that can be appropriately controlled and overseen by humans;

b) '**technical robustness and safety'** means that AI systems shall be developed and used in a way to minimize unintended and unexpected harm as well as being robust in case of unintended problems and being resilient against attempts to alter the use or performance of the AI system so as to allow unlawful use by malicious third parties;

c) '**privacy and data governance'** means that AI systems shall be developed and used in compliance with existing privacy and data protection rules, while processing data that meets high standards in terms of quality and integrity;

d) '**transparency'** means that AI systems shall be developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an

[14] Joint Communication To The European Parliament And The Council, The EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018>.

[15] See ENISA, "Cybersecurity Challenges of Artificial Intelligence", <https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>; also: ENISA, "Securing Machine Learning Algorithms", <https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms>

[16] ENISA, "Cybersecurity and privacy in AI - Medical imaging diagnosis", 7 June 2023, <https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis>.

[17] ENISA (2023), ibid., p. 5.

[18] ENISA (2023), ibid., p. 20.

[19] European Commission, "Liability Rules for Artificial Intelligence", <https://commission.europa.eu/business- economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en>.

[20] See, for instance, explanatory memorandum at page 3, or Article 4(2)(d) AI Liability Directive referring to the AI Act.

AI system as well as duly informing users of the capabilities and limitations of that AI system and affected persons about their rights;.
e) ‘**diversity, non-discrimination and fairness**’ means that AI systems shall be developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law;
f) ‘**social and environmental well-being’** means that AI systems shall be developed and used in a sustainable and environmentally friendly manner as well as in a way to benefit all human beings, while monitoring and assessing the long-term impacts on the individual, society and democracy.

IV. Data Protection Impact Assessment

The GDPR requires controllers to implement appropriate measures to ensure and be able to demonstrate compliance with the GDPR, taking into account among others "the risks of varying likelihood and severity for the rights and freedoms of natural persons" (article 24 (1)).

1) Risk

DPIA is a risk management tool that was introduced in data protection law with GDPR. Article 35 of GDPR states that it is necessary to conduct an impact assessment if the processing is 'likely to result in a high risk to the rights and freedoms of natural persons'. Article 25 of the GDPR data protection-by design obligation requires to take into account the 'risks of varying likelihood and severity for rights and freedoms of natural persons'. Therefore, the determination of risks is central to the performance of key data protection obligations.

Risk is an abstract and vague concept which can be interpreted in different ways.[21] The GDPR does not provide a definition of risk, nor does it specify a risk model. Instead, it generally states that the risk assessment should be an objective one. It also states that the likelihood and severity of the risk should be determined by keeping the nature, scope, context and purposes of the processing in mind.[22]

The ordinary meaning of the term risk refers to a 'possibility of something bad happening'.[23] A definition can be found in risk management standards. ISO defines risk as an either positive or negative 'effect of uncertainty on objectives'.[24] The concept also finds its place in the field of cybersecurity. NIS (2) Directive defines risk as 'the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident'. In the data protection context, Article 29 Working Party defines risk as "a scenario describing an event and its consequences, estimated in terms of severity and likelihood".[25]

Hence, risk has (i) a various degree of possibility of occurrence, (ii) has a various degree of magnitude or severity, (iii) has various consequences, which can be positive or negative, and which carry a various degree of severity and likelihood.[26]

2) DPIA

The GDPR does not formally define the concept of a DPIA as such, but - its minimal content is specified by Article 35(7) as follows:

"(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned"

[21] Raphaël Gellert, The Risk-Based Approach to Data Protection (Oxford University Press, 2020) 27-28.

[22] Recital 76, GDPR

[23] Cambridge Dictionary available at https://dictionary.cambridge.org/

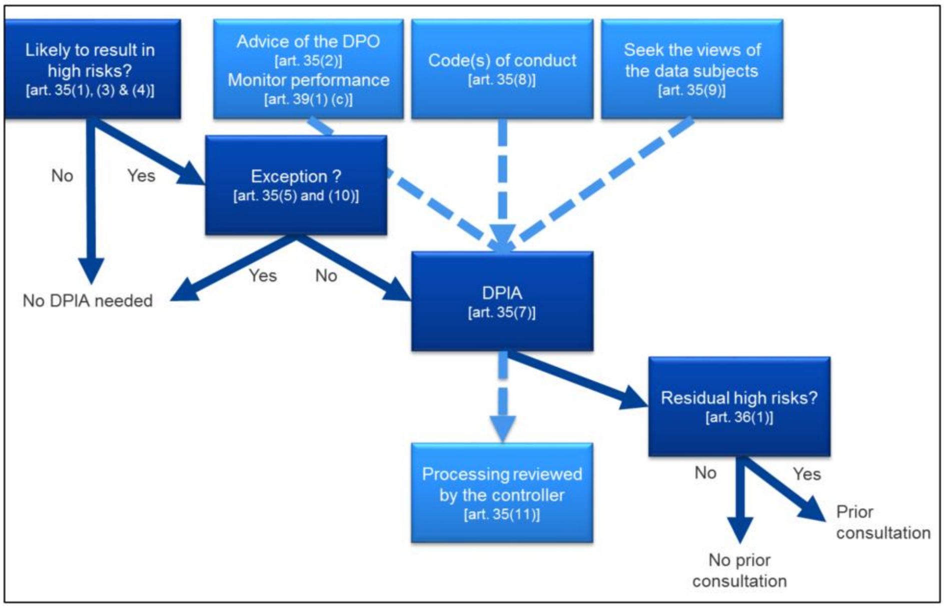
[24] ISO 31000 Risk management, See https://www.iso.org/iso-31000-risk-management.html/

[25] Article 29 Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679" (2017) 6.

[26] Raphaël Gellert, The Risk-Based Approach to Data Protection (Oxford University Press, 2020) 27-28.

The meaning and role of DPIA is clarified by GDPR recital 84 as follows: “In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk”

Figure 3: The necessity of DPIA[27]


Likely to result in high risks? [art. 35(1), (3) & (4)]
Advice of the DPO [art. 35(2)] Monitor performance [art. 39(1) (c)]
Code(s) of conduct [art. 35(8)]
Seek the views of the data subjects [art. 35(9)]
No
Yes
Exception ? [art. 35(5) and (10)]
No DPIA needed
Yes
No
DPIA [art. 35(7)]
Residual high risks? [art. 36(1)]
Processing reviewed by the controller [art. 35(11)]
No
Yes
Prior consultation
No prior consultation

What does a DPIA address? A single processing operation or a set of similar processing operations?

A **single DPIA could be used to assess multiple processing operations** that are similar in terms of nature, scope, context, purpose, and risks. Indeed, DPIAs aim at systematically studying new situations that could lead to high risks on the rights and freedoms of natural persons, and there is no need to carry out a DPIA in cases (i.e. processing operations performed in a specific context and for a specific purpose) that have already been studied. This might be the case where similar technology is used to collect the same sort of data for the same purposes.

Which processing operations are subject to a DPIA? Apart from exceptions, where they are “likely to result in a high risk”?

As reproduced above, Article 35 of the GDPR sets out a framework of criteria that includes:
- “(a) **a 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 person12;
- (b) **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 1013; or
- (c) a systematic monitoring of a publicly accessible area on a large scale”.

[27] Article 29 Working Party, “Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is ‘Likely to Result in a High Risk’ for the Purposes of Regulation 2016/679” (2017) 7.

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, taking into account the particular elements of Articles 35(1) and 35(3)(a) to (c), each National Data Protection Authotity could adopt and publish a list of additional criteria. The lists published and submitted for the consideration of the European Data Protection Committee contain a set of criteria applicable to the processing operations that could potentially be carried out in EUCAIM.

Country	DPA	Criteria
FRANCE	CNIL	Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médico- sociaux pour la prise en charge des personne
GERMANY	Datenschutkonference	Anonymisation of personal data pursuant Article 9 of the GDPR, not only in individual cases (in relation to the number of data subjects and the information per data subject) for the purpose of transmission to third parties
GERMANY	Datenschutkonference	Processing of personal data in accordance with Art. 9 para. 1 and Art. 10 GDPR - even if it is not to be regarded as "large scale" within the meaning of Art. 35 para. 3 lit. b) - provided that non-recurring data collection takes place by means of the innovative use of sensors or mobile applications and these data are received and processed by a central office.
ITALY	Garante Privacy	Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
		Trattamenti di categorie particolari di dati ai sensi dell’art. 9 oppure di dati relativi a condanne penali e a reati di cui all’art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
PORTUGAL	CNPD	Processing activities that have a scientific, historical research purpose or a statistical purpose as required in Article 65 of the law of August 1st, 2018 (Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016) ;
SPAIN	AEPD	Processing that involves the use of special categories of data as referred to in article 9.1 of the GDPR; data concerning criminal convictions and offences as referred to in article 10 of the GDPR, or data that allow the financial situation or solvency to be determined, or that allow personal information in relation to special categories of data to be determined or deduced.
SPAIN	AEPD	Processing that involves the use of data on a large scale. In order to determine whether processing can be considered to be on a large scale, the criteria laid down in guide WP243, ‘Guidelines on Data Protection Officers (DPOs)’ of the Article 29 Working Party shall be taken into account.
SPAIN	AEPD	Data processing regarding vulnerable subjects or those who are at risk of social exclusion, including the data of persons aged under 14, older people with any kind of disability, the disabled, persons who access social services, and

		the victims of gender-related violence, as well as their descendants and persons who are in their guardianship or custody.
SPAIN	AEPD	Processing that involves the use of new technologies or an innovative use of consolidated technologies, including the use of technologies on a new scale, for a new purpose, or in combination with others, in a manner that entails new forms of data collection and usage that represents a risk to people's rights and freedoms.

As a consequence, the deployment of the DPIA in EUCAIM will have particular conditions as it will be mandatory:
1.-Deploy a DPIA of the specific information system environment that integrates all EUCAIM operations.
2.-Require evidence of DPIAS performed by data holders according to national lists in the following cases:
- Federated data processing processes in the local premises of the data holders.
- Sharing of data sets at EUCAIM premises when the generation and/or sharing of the data set so requires.
3.-Cooperate with the DPIAs of the data access applicants when these are required of them.

3) Guidance for conducting DPIA

EUCAIM will preferably use the Guidance and Methodologies proposed by the EDPB, the AEPD and the CNIL. However, it shall accept documents that comply with the national Guidance, examples of which are included below.

Country	Guidance
FRANCE	https://www.cnil.fr/en/privacy-impact-assessment-pia
Germany	A short paper on the DPIA is available (in German) at: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf An example of how to do a DPIA is published (in German): https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf
Italy	https://www.garanteprivacy.it/regolamentoue/DPIA
Spain	https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-nueva-guia-gestionar-riesgos-y-evaluciones-impacto
Portugal	https://cnpd.public.lu/en/professionnels/obligations/AIPD.html

Legal framework

- Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108 (**Convention 108**).

- Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5 (**ECHR**).

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194 (**NIS Directive**).

- Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) PE/28/2019/REV/1, OJ L 172 (**Open Data Directive**).

- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, PE/32/2022/REV/2, OJ L 333 (**NIS 2 Directive**).

- Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995 (**Data Protection Directive**).

- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (**AI Liability Directive**) COM/2022/496 final.

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (**Data Act**) COM/2022/68 final.

- Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (**Artificial Intelligence Act**) and amending certain Union legislative acts - General approach, <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>.

- Proposal for a Regulation Of The European Parliament And Of The Council on the European Health Data Space COM/2022/197 final (**EHDS**).

- Proposal for a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, COM/2021/206 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>.

- Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No. 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC 2017, OJ L 117/1 (**MDR**).

- Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, OJ L 117 (**IVDR**).

- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions,

bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, PE/31/2018/REV/1, OJ L 295.

- Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, PE/53/2018/REV/1, OJ L 303 (**FFNPDR**).

- Regulation (EU) 2021/2282 of the European Parliament and of the Council of 15 December 2021 on health technology assessment and amending Directive 2011/24/EU (2021) OJ 458/

- Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (**Data Governance Act**) PE/85/2021/REV/1, OJ L 152.

- Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJ L 158 27.5.2014, p. 1 (**Clinical Trial Regulation**).

Official Documents

- Article 29 Working Party, “Annex to Letter from the WP29 to the European Commission”, DG CONNECT on mHealth, <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf>.

- Article 29 Working Party, “Opinion 01/2012 on the data protection reform proposals”, Adopted on 23 March 2021, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf>.

- Article 29 Working Party, „Opinion 05/2014 on Anonymisation Techniques”, Adopted on 10 April 2014, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

- Article 29 Working Party, “Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is ‘Likely to Result in a High Risk’ for the Purposes of Regulation 2016/679” (2017)

- Communication From The Commission To The European Parliament And The Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM/2019/250 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN>.

- Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A European strategy for data COM/2020/66 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>.

- Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - Fostering a European approach to Artificial Intelligence COM/2021/205 final, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A205%3AFIN>.

- Council of Europe, “Guidelines to respect, protect and fulfil the rights of the child in the digital environment”, Recommendation CM/Rec(2018)7 of the Committee of Ministers, <https://rm.coe.int/guidelines-to-respect- protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>.

- EDPB, “Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))”, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf>.

- EDPB, “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”, Version 2.0, Adopted on 18 June 2021, <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020- measures-supplement-transfer_en>.

- EDPB, Guidelines 05/202 on consent under Regulation 2016/679, Version 1.1, Adopted on 4 May 2020, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.

- EDPB-EDPS (2022) Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Adopted on 4 May 2022, <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion- 22022-proposal-european_en>.

- ENISA, “Cybersecurity and privacy in AI - Medical imaging diagnosis”, 07.06.2023, <https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis>.
- ENISA, “Cybersecurity Challenges of Artificial Intelligence”, 15.12.2020, <https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>.
- ENISA, “Data Pseudonymisation: Advanced Techniques and Use Cases”, 28.01.2021, <https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases>.
- ENISA, “Securing Machine Learning Algorithms”, 14.12.2021, <https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms>.

- EDPB, “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default” Version 2.0. Adopted on 20October 2020, <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article- 25-data-protection-design-and_en>.

- European Commission, “Coordinated Plan on Artificial Intelligence”, <https://digital-strategy.ec.europa.eu/en/policies/plan-ai#:~:text=The%20key%20aims%20of%20the,AI%20policy%20to%20avoid%20fragmentation.&text=The%20C oordinated%20Plan%20on%20Artificial%20Intelligence%202021%20Review%20is%20the,global%20l eadershi p%20in%20trustworthy%20AI.>.

- European Commission, "The EU's Cybersecurity Strategy for the Digital Decade", <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>.

- European Commission, ANNEXES to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence COM(2021) 205 final, ANNEX, <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>.

- European Commission, Directorate-General for Research and Innovation, Eechoud, M., Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research, Publications Office of the European Union, 2022, <https://data.europa.eu/doi/10.2777/71619>.

- European Parliament, "DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts", Version 1.1, 16/05/2023, <https://www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf>.

- High-Level Expert Group on Artificial Intelligence (HLEG), "Assessment List for Trustworthy AI (ALTAI) for self assessment", 17 July 2022, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy- artificial-intelligence-altai-self-assessment>.

- High-Level Expert Group on Artificial Intelligence, "A Definition of AI: Main capabilities and disciplines", 8 April 2019, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

- High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI", 8 April 2019, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

- Joint Communication To The European Parliament And The Council, The EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018>.

- Medical Device Coordination Group (MDCG) 2019-11 Guidance on Qualification and Classification of Softwarein Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, October 2019, <https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf>.

- Medical Device Coordination Group (MDCG) 2019-16 Rev.1 Guidance on Cybersecurity for medical devices,December 2019, July 2020 rev.1, <https://ec.europa.eu/docsroom/documents/41863>.

- UNCRC, The United Nations Convention on the Rights of the Child, <https://www.unicef.org.uk/wp-content/uploads/2016/08/unicef-convention-rights-child-uncrc.pdf>.
- WHO, Ethics and governance of artificial intelligence for health, <https://www.who.int/publications/i/item/9789240029200>.

- WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects, 6 September 2022, <https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for- medical-research-involving-human-subjects/>.

- WMA Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks, 4 June 2020, <https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health- databases-and-biobanks/>.

- WMA, Declaration of Taipei – Research on Health Databases, Big Data and Biobanks, <https://www.wma.net/what-we-do/medical-ethics/declaration-of-taipei/>.

- ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion n. 5/2014 on Anonymisation Techniques, WP216 (10.04.2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, 0829/14/EN WP216

- Cyber Essentials by the UK National Security Centre, https://www.cyberessentials.ncsc.gov.uk/

- The CNIL`s Guides (2018) Guidance on the Security of Personal Data

- The ICO Guide on data security, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

- The ICO guidelines on the safe disposal of IT devices, https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

- UKRI Engineering and Physical Sciences Research Council, EPSRC Policy Framework on Research Data
- ICO (2012) Bring your own device (BYOD) guidance, https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

- ICO (2016) A practical guide to IT security – Ideal for the small business p. 13., https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

- ICO draft guidance, Chapter 1: introduction to anonymisation - Chapter 2: How do we ensure anonymisation is effective? - Chapter 3: pseudonymisation - Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance, February 2022, https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/

Opinions of the European Data Protection Board (EDPB) Regarding Data Protection Impact Assessments (DPIA)

- Opinion 7/2020 on the draft list of the competent supervisory authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR). Date: 22 April 2020. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). EDPB France.
- Opinion 13/2019 on the draft list of the competent supervisory authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR). Date: 12 July 2019. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). EDPB France.

- Opinion 12/2019 on the draft list of the competent supervisory authority of Spain regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR). Date: 12 July 2019. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). EDPB Spain.
- Opinion 11/2019 on the draft list of the competent supervisory authority of the Czech Republic regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR). Date: 12 July 2019. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). EDPB Czech Republic.
- Opinion 10/2019 on the draft list of the competent supervisory authority of Cyprus regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35(4) GDPR). Date: 12 July 2019. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). EDPB Cyprus.
- Opinion 7/2019 on the draft list of the competent supervisory authority of Iceland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 12 March 2019. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Iceland EDPB.
- Opinion 6/2019 on the draft list of the competent supervisory authority of Spain regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 12 March 2019. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). EDPB Spain.
- Opinion 2/2019 on the draft list of the competent supervisory authority of Norway regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 23 January 2019. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). EDPB Norway.
- Opinion 01/2019 on the draft list of the competent supervisory authority of the Principality of Liechtenstein regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 23 January 2019. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). EDPB Liechtenstein.
- Opinion 27/2018 on the draft list of the competent supervisory authority of Slovenia regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 4 December 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Slovenia.
- Opinion 26/2018 on the draft list of the competent supervisory authority of Luxembourg regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 4 December 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Luxembourg.
- Opinion 25/2018 on the draft list of the competent supervisory authority of Croatia regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 4 December 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Croatia.
- Opinion 24/2018 on the draft list of the competent supervisory authority of Denmark regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 4 December 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Denmark.
- Dictamen 25/2018 sobre el proyecto de lista de la autoridad de control competente de Croacia en relación con las operaciones de tratamiento que requieren una evaluación de impacto relativa a la protección de datos (artículo 35, apartado 4, del RGPD). Date: 4 December 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Croatia.
- Dictamen 24/2018 sobre el proyecto de lista de la autoridad de control competente de Dinamarca en relación con las operaciones de tratamiento que requieren una evaluación de impacto relativa a la protección de datos (artículo 35, apartado 4, del RGPD). Date: 4 December 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Denmark.

- Opinion 9/2018 on the draft list of the competent supervisory authority of France regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). France.
- Opinion 8/2018 on the draft list of the competent supervisory authority of Finland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Finland.
- Opinion 7/2018 on the draft list of the competent supervisory authority of Greece regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Greece.
- Opinion 6/2018 on the draft list of the competent supervisory authority of Estonia regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Estonia.
- Opinion 5/2018 on the draft list of the competent supervisory authorities of Germany regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Germany.
- Opinion 4/2018 on the draft list of the competent supervisory authority of Czech Republic regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Czech Republic.
- Opinion 3/2018 on the draft list of the competent supervisory authority of Bulgaria regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Bulgaria.
- Opinion 22/2018 on the draft list of the competent supervisory authority of the United Kingdom regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). United Kingdom.
- Opinion 21/2018 on the draft list of the competent supervisory authority of Slovakia regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Slovakia.
- Opinion 20/2018 on the draft list of the competent supervisory authority of Sweden regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Sweden.
- Opinion 2/2018 on the draft list of the competent supervisory authority of Belgium regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Belgium.
- Opinion 19/2018 on the draft list of the competent supervisory authority of Romania regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Romania.
- Opinion 18/2018 on the draft list of the competent supervisory authority of Portugal regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Portugal.

- Opinion 17/2018 on the draft list of the competent supervisory authority of Poland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Poland.
- Opinion 16/2018 on the draft list of the competent supervisory authority of the Netherlands regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Netherlands.
- Opinion 15/2018 on the draft list of the competent supervisory authority of Malta regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Malta.
- Opinion 14/2018 on the draft list of the competent supervisory authority of Latvia regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Latvia.
- Opinion 13/2018 on the draft list of the competent supervisory authority of Lithuania regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Lithuania.
- Opinion 12/2018 on the draft list of the competent supervisory authority of Italy regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Italy.
- Opinion 11/2018 on the draft list of the competent supervisory authority of Ireland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Ireland.
- Opinion 10/2018 on the draft list of the competent supervisory authority of Hungary regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Hungary.
- Opinion 1/2018 on the draft list of the competent supervisory authority of Austria regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Austria.
- Dictamen 22/2018 sobre el proyecto de lista de la autoridad de control competente del Reino Unido en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos. Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). United Kingdom.
- Dictamen 21/2018 sobre el proyecto de lista de la autoridad de control competente de Eslovaquia en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos. Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Slovakia.
- Dictamen 20/2018 sobre el proyecto de lista de la autoridad de control competente de Suecia en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos (artículo 35, apartado 4, del RGPD). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Sweden.
- Dictamen 2/2018 sobre el proyecto de lista de la autoridad de control competente de Bélgica en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos (artículo 35, apartado 4, del RGPD). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Belgium.

- Dictamen 19/2018 sobre el proyecto de lista de la autoridad de control competente de Rumanía en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos (artículo 35, apartado 4, del RGPD). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Romania.
- Dictamen 18/2018 sobre el proyecto de lista de la autoridad de control competente de Portugal en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos (artículo 35, apartado 4, del RGPD). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Portugal.
- Dictamen 17/2018 sobre el proyecto de lista de la autoridad de control competente de Polonia en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos (artículo 35, apartado 4, del RGPD). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Poland.
- Dictamen 16/2018 sobre el proyecto de lista de la autoridad de control competente de los Países Bajos en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos. Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Netherlands.
- Dictamen 15/2018 sobre el proyecto de lista de la autoridad de control competente de Malta en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos (artículo 35, apartado 4, del RGPD). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Malta.
- Dictamen 14/2018 sobre el proyecto de lista de la autoridad de control competente de Letonia en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos (artículo 35, apartado 4, del RGPD). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Latvia.
- Dictamen 13/2018 sobre el proyecto de lista de la autoridad de control competente de Lituania en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos (artículo 35, apartado 4, del RGPD). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Lithuania.
- Dictamen 12/2018 sobre el proyecto de lista de la autoridad de control competente de Italia en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos. Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Italy.
- Dictamen 10/2018 sobre el proyecto de lista de la autoridad de control competente de Hungría en lo que respecta a las operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos (artículo 35, apartado 4, del RGPD). Date: 3 October 2018. Opinion of the Board (Art. 64). Data Protection Impact Assessment (DPIA). Hungary.