EUCAIM
CANCER IMAGE EUROPE

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

D3.4: [D3.4 – AI Impact Assessment Report]

Partner(s)	KUL, UV
Author(s):	Janos Meszaros, Ricard Martinez, Francisco R. Soriano, Alma Virtu, Isabelle Huys, Carles Hernandez-Ferrer
Date of delivery:	30\12\2024
Version:	1.5

Contents

Executive summary

The EUCAIM project leverages artificial intelligence (AI) technologies to transform cancer imaging and research. In the internal and open calls, AI tool developers have applied to use the EUCAIM platform. Given the ethical, legal, and technical challenges inherent in deploying AI in healthcare, compliance with European Union (EU) regulations is paramount. This deliverable, in its current form, outlines the baseline legal and ethical standards that EUCAIM expects AI tool developers to meet.

As of the delivery date of this report (December 2024), the legal and technical evaluation of internal and external AI tool developers is still in progress. An updated version of this deliverable will be issued after the evaluation of the applicants' legal and ethical compliance is complete.

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

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**.

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 explores **the implications of the EU AI Act and the European Health Data Space Regulation, ensuring that development and benchmarking of AI tools are lawful, ethical, and robust**. Furthermore, it leverages the Assessment List for Trustworthy Artificial Intelligence (ALTAI) to evaluate AI systems' alignment with principles of fairness, transparency, and accountability.

All the AI Tool Developers and testers in EUCAIM need to do AI Impact Assessment and provide a DPO (Data Protection Officer) statement. Some of them also need to provide ethical review and DPIA (Data Protection Impact Assessment), according to their national regulations.

As of the delivery date of this report (December 2024), the legal and technical evaluation of internal and external applicants is still in progress. While some applicants have submitted all the required documents, others have provided only partial documentation, and some have not submitted any. This is due to ongoing efforts by the applicants to obtain the necessary legal and ethical documents and required information.

This deliverable, in its current form, outlines the legal and ethical requirements that EUCAIM expects from AI tool developers. Once the majority (or all) of the applicants have submitted the required documents and WP3 has completed their evaluation, the deliverable will be finalized**. An updated version of this deliverable will be issued after the evaluation of the applicants' legal and ethical compliance is complete.**

II. Quick Checklist of key items for AI Tool developers

This checklist offers a quick starting point for AI tool developers to ensure compliance with the AI Act, EHDS, and MDR. While not exhaustive, it highlights key considerations like risk assessment, prohibited practices, and trustworthy AI principles. Developers must ensure thorough due diligence to meet all applicable regulatory and ethical requirements.

I. Prohibitions

First, AI tool developers need to make sure that their tool is not prohibited.

a) Prohibited uses in the AI Act

The European Union's Artificial Intelligence Act (AI Act, Article 5) identifies specific AI practices that are prohibited due to their potential to cause significant harm or infringe upon fundamental rights. These prohibited practices include:

1) Subliminal Manipulation: AI systems that deploy subliminal techniques beyond a person's consciousness to materially distort behavior, impairing the ability to make informed decisions and causing significant harm.

2) Exploitation of Vulnerabilities: AI systems that exploit vulnerabilities of individuals or specific groups based on age, disability, or socio-economic status, leading to behavior distortion and significant harm.

3) Social Scoring: AI systems used for evaluating or classifying individuals or groups over time based on social behavior or personal characteristics, resulting in unjustified or disproportionate detrimental treatment.

4) Predictive Policing: AI systems that assess or predict the risk of individuals committing criminal offenses based solely on profiling or assessing personality traits, without objective and verifiable facts directly linked to criminal activity.

5) Untargeted Facial Recognition Data Collection: AI systems that create or expand facial recognition databases through untargeted scraping of facial images from the internet or CCTV footage.

6) Emotion Recognition in Sensitive Areas: AI systems used to infer emotions of individuals in workplaces and educational institutions, except when intended for medical or safety reasons.

7) Biometric Categorization: AI systems that categorize individuals based on biometric data to deduce or infer sensitive attributes such as race, political opinions, religious beliefs, or sexual orientation.

8) Real-Time Remote Biometric Identification: The use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes, with specific exceptions for serious threats or criminal investigations.

b) Prohibited uses in the European Health Data Space

In the latest version of the forthcoming European Health Data Space (EHDS) Regulation, specific prohibitions are outlined to ensure the ethical use of health data (EHDS, Article 35).

1) Detrimental Decision-Making: Using health data to make decisions that could harm individuals or groups, such as developing harmful products or services.

2) Discrimination: Making decisions that disadvantage people in job offers, goods/services, insurance, or loans based on their health data.

3) Advertising or Marketing: Using health data for promotional activities.

4) Harmful Products/Services: Developing products or services that harm individuals, public health, or society (e.g., illicit drugs, weapons).

5) Ethics Violations: Engaging in activities that conflict with ethical standards under national law.

II. The ALTAI Tool

AI Impact Assessment: For AI Tool developers we recommend using the **Assessment List for Trustworthy Artificial Intelligence (ALTAI)**. ALTAI also offers an online tool that allows you to complete the assessment after registering. At the end, you will receive a comprehensive report. You can access the tool here: https://futurium.ec.europa.eu/en/european-ai-alliance/pages/welcome-altai-portal

Introduced in July 2020, ALTAI translates ethical guidelines into practical steps for AI developers and deployers.

Trustworthy AI is defined by seven key requirements:

1. Human Agency and Oversight: Ensuring AI systems support human autonomy and decision-making.
2. Technical Robustness and Safety: Guaranteeing resilience and reliability of AI systems.
3. Privacy and Data Governance: Protecting personal data and ensuring its proper management.
4. Transparency: Promoting traceability and explainability of AI processes.
5. Diversity, Non-discrimination, and Fairness: Preventing bias and ensuring inclusivity.
6. Societal and Environmental Well-being: Considering the broader impact on society and the environment.
7. Accountability: Establishing mechanisms for responsibility and redress.

ALTAI provides a structured checklist that guides users in evaluating their AI systems against these requirements, facilitating the identification and mitigation of potential risks. The tool is available both as a downloadable PDF and an interactive web-based version, offering flexibility for different organizational needs.

III. Risk Categorization in the AI Act

Developers of AI tools must conduct a risk assessment and categorize their tools according to the Act's risk levels: unacceptable, high, limited, or minimal risk.

Risk Categories:

- **Unacceptable Risk**: Prohibited AI practices like subliminal manipulation or social scoring.

- **High Risk**: Tools impacting healthcare decisions (e.g., diagnostics) require stringent compliance, including transparency, data governance, and monitoring.

- **Limited Risk**: Lower-risk tools (e.g., decision support) must disclose their AI nature.

- **Minimal Risk**: Systems with negligible impact.

VI. Medical Device Regulation

AI tool developers must first determine if their tool qualifies as a medical device under the MDR (Regulation (EU) 2017/745). Tools intended for diagnosis, monitoring, or treatment of diseases typically fall under this category.

V. General Data Protection Regulation (GDPR)

AI tool developers must ensure compliance with the General Data Protection Regulation (GDPR) when processing personal data. D3.1 (Report on the technical and organisational measures to safeguard the rights and freedoms of data subject) contains requirements for complying with the GDPR.

Key requirements include: **Lawful Basis** (Articles 6, 9), **Data Minimization**: Collect only necessary data for specific purposes (Article 5), **Privacy by Design** (Article 25), **User Rights** (Articles 15–22), **Security** (Articles 32–34), **Data Protection Impact Assessment** for high-risk tools (Article 35).

III. AI Tools In EUCAIM

In the EUCAIM project, AI plays a role in developing advanced tools to analyze cancer imaging data. It involves **creating algorithms to support more accurate diagnostics, treatment planning, and research** through data integration from diverse sources across Europe.

In **April 2024, EUCAIM launched an Open Call** for new beneficiaries to join the consortium, aiming to include new cancer image databases in the federation and to incorporate real-world AI use cases to guide the design of the EUCAIM platform, addressing specific scientific and clinical questions.
A total of 66 applications were received and evaluated by the EUCAIM Access Committee against the criteria described in D7.1, and 19 applications were shortlisted and submitted to the European Commission for final approval.
Applicants could belong to one or both of the following groups:
- Data holders: they contribute data to the EUCAIM infrastructure either by: (a) becoming a federated node; or (b) transferring anonymized data directly to the Reference Node.
- Data users: A Data User refers to any natural or legal person who intends to make use of the data accessible through the EUCAIM infrastructure for research, development, and innovation purposes. This includes those wishing to develop/train/benchmark/validate **AI algorithms** using the curated data in EUCAIM.

A **total of 66 applications were submitted and underwent an initial eligibility check** by the EUCAIM Coordination Team to ensure that applicants met the funding criteria under the Digital Europe programme and had provided all the required information. **Four applications were deemed ineligible** because the applicants were from countries not eligible for funding. Of the re**maining 62 applications, 30 were submitted by data holders, 17 by data users** (seeking to use EUCAIM data for AI algorithm development, training, or validation), and **15 by organizations applying as both data holders and data users** (i.e., proposing AI use cases that utilized their own datasets while leveraging the EUCAIM infrastructure to host these data and perform AI development, training, and validation within a secure environment).

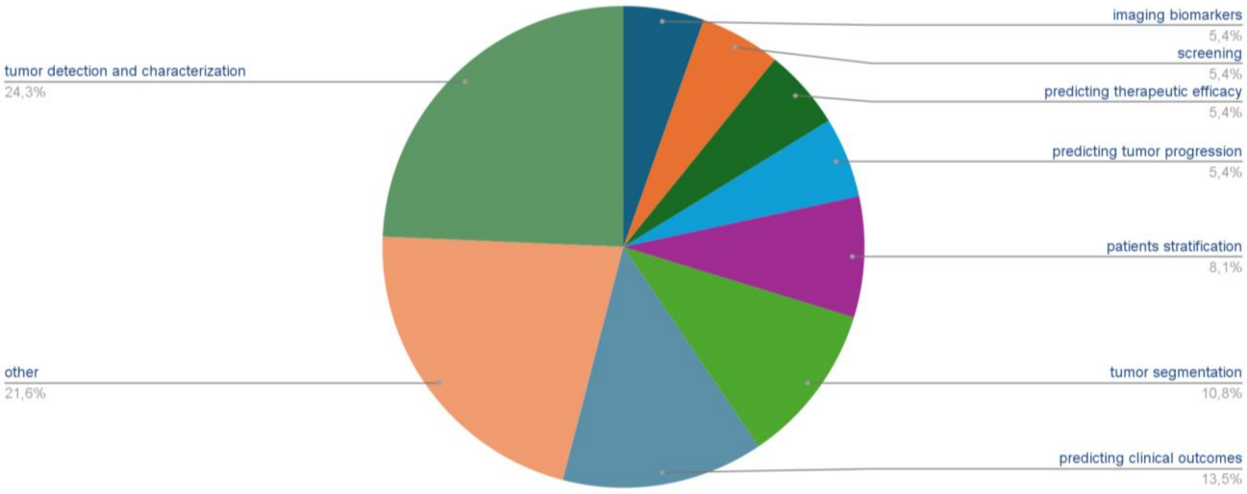
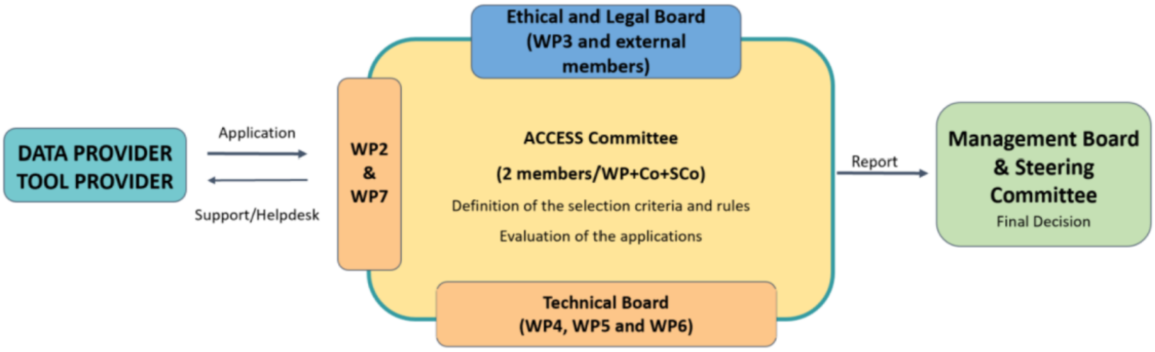


Figure 5 from D7.1 illustrates the main topics of the AI use cases in all the applications received. Most applications focus on developing or validating accurate and automated methods for tumor detection and characterization, and for image segmentation. Predicting clinical outcomes and improving patients' stratification through the application of advanced AI tools on medical images are also areas of high interest.

Application process

A **tool provider may submit an application to incorporate a tool or service into the EUCAIM** marketplace using a standardised form. The proposal will be **evaluated from both technical and legal perspectives**. The procedures that need to be followed by the tool provider will be negotiated with the corresponding technical, legal, ethical, and scientific boards. In this document, a **Tool Provider** refers to the entity that would like to contribute with processing tools, services, or applications they have developed to the EUCAIM's marketplace for use in the federated processing purposes of the platform.



In EUCAIM, WP3 requires all the AI Tool Developers and testers in EUCAIM to do AI Impact Assessment and provide a DPO (Data Protection Officer) statement. Some of them also need to provide ethical review and DPIA (Data Protection Impact Assessment), according to their national regulations.

IV. The risks of software on-boarding of AI-tools

This risk assessment is limited to the context of data processing tools that are executed through the EUCAIM platform, and operate on EUCAIM data, either in the central node or on federated nodes.

Actors in developing AI Tools in EUCAIM

Actor	Perspective
Software provider	can be malicious
Software end-user (i.e. the person who actually looks at a tool's output)	can be malicious
Data scientist doing the model training through the EUCAIM platform	can be malicious
EUCAIM validator	always honest
EUCAIM platform developer	always honest
EUCAIM data provider	always honest
Maintainer of EUCAIM federated node	always honest
Data subject	does not participate in tool usage/training
Software	can be malicious

Source: EUCAIM software on-boarding guideline

Risks in software on-boarding of AI-tool developers

	Risk
Generic risks	An (unknown) vulnerability in the tool's code can be exploited by malicious actors, potentially without the knowledge of the tool provider
	An (unknown) vulnerability in a third-party library can be exploited by malicious actors, potentially without the knowledge of the tool provider
	The tool running in EUCAIM is not the tool that was actually validated (malicious substitution, or human error)

	The combination of multiple tools or datasets allows data leaks/reidentification or other harmful consequences
	A software preempts or uses all of the computational resources available
	A software causes a crash of the whole system
	A software corrupts the data
	The software has been developed based on unethical practices
	A user executes a software for which they did not have the right according to intellectual property or copyright laws
	A software introduces algorithmic bias in the pipeline
	After a harmful event, it is impossible to trace back the history of the software's execution
Risks during AI model training	Training gradients can be "inverted" to identify training data (either by the data scientist, or by other data providers, or by a third-party malicious actor)
	Code for model training (dynamically provided by data scientist) includes malicious procedures
	Malfunctions during model training lead to accidental leak of information (e.g. error logs reveal sensitive information about a data sample)
	Malicious actors with a legitimate role in the training process can "poison" model with ad-hoc data or crafted gradient updates to prevent correct model training
	Malicious actors can "impersonate" a legitimate data provider to perform attacks such as model poisoning
	Malicious actors exploit legitimate training protocols that rely on multiple training of similar models (e.g. leave-one-out cross-validation) to perform statistical attacks
	Training data has been corrupted, leading to a harmful malfunction of the tool
	Model drift in a continual learning setting leads to harmful consequences
Risks related to using an AI model trained on EUCAIM data	Generative models leak training data samples
	Trained model can be "inverted" to identify training data
	A model trained on a data subset (e.g. dataset at time t) turns out to leak sensitive information when used for inference on another dataset (e.g. dataset at time t+delta, or out-of-distribution data)
	The trained model discriminates specific data subpopulations

	The model is trained on a dataset that is too small, thus leading to overfitting that can be exploited for data leaks
	The trained model is also (maliciously) provided a backdoor that causes it to leak data only under specific circumstances (e.g. when presented with a special kind of input)
	The legitimately trained model is used for malicious purposes outside of EUCAIM
	Infringement of intellectual property: a model trained on EUCAIM data is "stolen"
	The trained model is used to make a harmful clinical decision

Source: EUCAIM software on-boarding guideline

V. The regulation of AI in the European Union

The European Union has established a detailed regulatory framework to address the development, deployment, and use of artificial intelligence (AI) systems, ensuring they are safe, transparent, and aligned with fundamental rights. Central to this effort is the Artificial Intelligence Act (AI Act), which provides a risk-based approach to AI regulation, categorizing AI systems by their potential impact and imposing tailored obligations to mitigate risks and uphold societal values.

The European Commission appointed a group of experts to provide advice on its AI strategy, Forming the **High-Level Expert Group on Artificial Intelligence (AI HLEG)**[1], members include representatives from academia, civil society and industry. The HLEG defined the **principles of trustworthy AI**, emphasizing lawfulness, ethics, and robustness, and provided practical recommendations to integrate these principles throughout an AI system's lifecycle.

By combining the AI Act's regulatory structure with the foundational guidance from the HLEG, the EU aims to balance the benefits of AI innovation with the need to protect societal values and individual rights. This section outlines the key aspects of the AI Act and its implications for AI developers, focusing on compliance with EU standards.

Trustworthy AI has three components, which should be met throughout the system's entire life cycle:

(i) it should be **lawful**, complying with all applicable laws and regulations;

(ii) it should be ethical, ensuring adherence to **ethical** principles and values and

(iii) it should be **robust,** both from a technical and social perspective since, even with good intentions, AI systems can cause unintentional harm. Each component in itself is necessary but not sufficient for the achievement of Trustworthy AI.

Ideally, all three components work in harmony and overlap in their operation. If, in practice, tensions arise between these components, society should endeavour to align them.[2]

The AI HLEG provided the following **guidance on how trustworthy AI can be realised**, by listing seven requirements that AI systems should meet. Both technical and non-technical methods can be used for their implementation.[3]

[1] https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

[2] High-Level Expert Group on Artificial Intelligence, Policy and Investment Recommendations for Trustworthy AI, 2019

[3] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2018, p. 6.

i) Ensure that the development, deployment and use of **AI systems meets the seven key requirements for Trustworthy AI**: (1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination and fairness, (6) environmental and societal well-being and (7) accountability.

ii) Consider **technical and non-technical methods** to ensure the implementation of those requirements.

iii) Foster **research and innovation** to help assess AI systems and to further the achievement of the requirements; disseminate results and open questions to the wider public, and systematically train a new generation of experts in AI ethics.

iv) **Communicate,** in a clear and proactive manner, information to stakeholders **about the AI system's capabilities and limitations**, enabling realistic expectation setting, and about the manner in which the requirements are implemented. Be transparent about the fact that they are dealing with an AI system.

v) Facilitate the **traceability and auditability** of AI systems, particularly in critical contexts or situations.

vi) **Involve stakeholders** throughout the AI systems life cycle. Foster training and education so that all stakeholders are aware of and trained in Trustworthy AI.

vii) Be mindful that there **might be fundamental tensions between different principles** and requirements. Continuously identify, evaluate, document and communicate these trade-offs and their solutions.

These principles have been endorsed by the European Union Artificial Intelligence Act (AI Act).

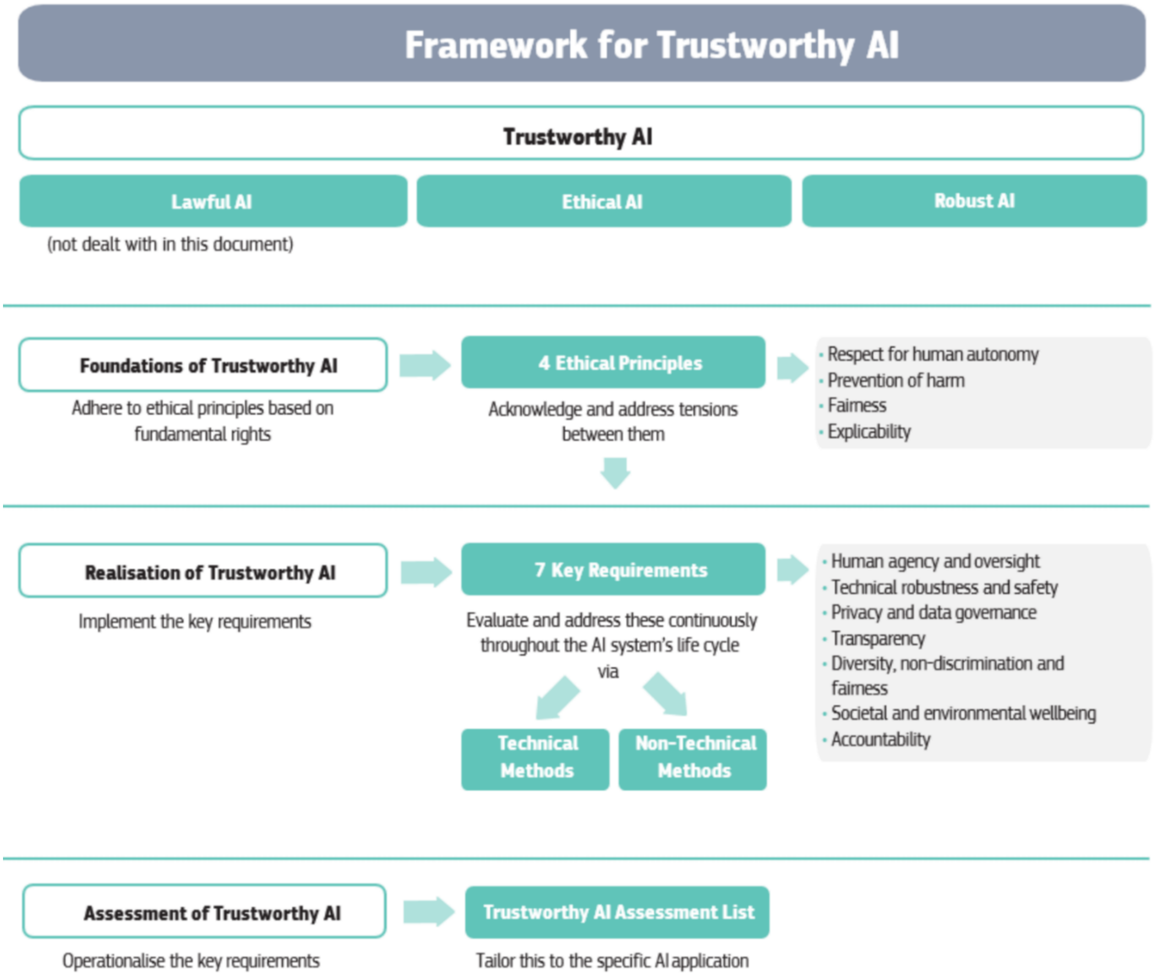

Framework for Trustworthy AI
Trustworthy AI
Lawful AI
Ethical AI
Robust AI
(not dealt with in this document)
Foundations of Trustworthy AI
Adhere to ethical principles based on fundamental rights
4 Ethical Principles
Acknowledge and address tensions between them
· Respect for human autonomy
· Prevention of harm
· Fairness
· Explicability
Realisation of Trustworthy AI
Implement the key requirements
7 Key Requirements
Evaluate and address these continuously throughout the AI system's life cycle via
Technical Methods
Non-Technical Methods
· Human agency and oversight
· Technical robustness and safety
· Privacy and data governance
· Transparency
· Diversity, non-discrimination and fairness
· Societal and environmental wellbeing
· Accountability
Assessment of Trustworthy AI
Operationalise the key requirements
Trustworthy AI Assessment List
Tailor this to the specific AI application

Figure 1. Framework for Trustworthy AI[4]

1) The EU AI Act

The EU AI Act is a regulatory framework designed to govern the development, deployment, and use of AI systems within the EU. Its primary goal is to ensure that AI technologies are safe, transparent, and respect fundamental rights, while also providing clarity for developers and users.

The **AI Act categorizes AI systems according to the risk they pose to safety and fundamental rights**, ranging from minimal risk to unacceptable risk. This risk-based approach dictates the regulatory requirements for each category:

- **Unacceptable Risk:** AI applications that manipulate human behavior to circumvent users' free will are banned.

[4] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2018, p. 10.

- **High-Risk:** AI systems in critical sectors such as healthcare, policing, and transport must undergo strict compliance checks before deployment. This includes ensuring data governance, transparency, and providing detailed documentation to trace the AI's decision-making process.
- **Limited Risk:** AI applications like chatbots must be transparent; users should be informed that they are interacting with a machine.
- **Minimal Risk:** For AI applications deemed to pose minimal risk, such as spam filters, the regulation imposes no additional requirements beyond existing laws.

To align with the AI Act, research projects must develop strategies that include:

- Risk Assessment: Early and ongoing assessments to classify AI systems according to the defined risk levels.

- Transparency Measures: Development of mechanisms to explain AI decisions to end-users (e.g. in the case of EUCAIM, researchers and medical doctors) particularly when using AI in sensitive areas.

- **Data Governance**: Implementation of strict data handling procedures to ensure the integrity and confidentiality of data used by AI systems (in EUCAIM, D3.1 - Report on the technical and organisational measures to safeguard the rights and freedoms of data subject; D3.5 - Report describing the EUICAM's pseudonymisation strategy; D3.6 – Data Management Plan)

Scientific Research Exemptions in the EU AI Act

The EU AI Act includes important provisions that specifically address the use of AI in scientific research. Recognizing the unique needs and benefits of AI applications in the research sector, the legislation aims to facilitate innovation while ensuring that such technologies are used responsibly and ethically within the scientific community. To support scientific advancement and innovation, the **Act provides exemptions for AI systems used exclusively for scientific research purposes**. These exemptions are designed to alleviate some of the regulatory burdens that might hinder the development and application of AI in research settings.

AI systems developed and deployed for the purpose of scientific research may be exempt from some of the stringent compliance checks required for high-risk categories. This includes certain assessments of risk and bias that might be mandatory for commercial AI applications. By reducing these requirements, the Act facilitates a more agile research environment where scientists can experiment and innovate with fewer administrative hurdles.

While the Act provides exemptions, it also emphasizes the **need for ethical oversight** to ensure that research AI systems are developed and used in a manner that respects fundamental rights and safety standards.

Institutions are encouraged to establish internal review boards or similar bodies to oversee AI research activities, mirroring the ethical oversight commonly associated with biomedical research.

In EUCAIM, WP3 requires internal and external applicants developing AI Tools to conduct an AI Impact Assessment, based on ALTAI (Assessment List for Trustworthy AI (ALTAI).[5]

Trustworthy Artificial Intelligence in Medical Imaging

The report titled "FUTURE-AI: Guiding Principles and Consensus Recommendations for Trustworthy Artificial Intelligence in Medical Imaging (realised by the AI4HI Network, comprising the EuCanImage, PRIMAGE, CHAIMELEON, INCISIVE, and ProCancer-I projects) shows us how the imaging AI algorithms should be impartial and maintain the same performance when applied to similarly situated individuals (individual fairness) or different groups of individuals, including under-represented groups (group fairness)'. The Report underlines how the clinical images could be selected to avoid bias in the training of the AI system. The "existing imaging databases are often imbalanced according to sex, ethnicity, geography and socioeconomics." In this case, there is a risk that trained AI algorithms to become biased towards under-represented groups and hence exacerbate existing health disparities." Because of that, AI tools can generate undetected errors, with harmful consequences to the patient, when they are applied to imaging conditions that may differ or unexpectedly deviate, even slightly, from those used for training.

The ALTAI Assessment also measures this issue, asking tool developers on their efforts to avoid bias and discrimination.

2) GDPR and EHDS

For developing and training AI algorithms, personal data need to be collected and processed according to the EU and Member State data protection laws (e.g. the General Data Protection Regulation)[6]

In EUCAIM the **D3.1 (Report on the technical and organisational measures to safeguard the rights and freedoms of data subject)** detailed the requirements for complying with the GDPR.

Internal and external applicants need to fill and sign a **DPO (Data Protection Officer) Statement, and in some cases provide a Data Protection Impact Assessment.**

[5] https://altai.insight-centre.org/

[6] GDPR

3) Medical Device Regulation

Medical Device Regulation (MDR) and AI Imaging Tools

The integration of AI in imaging tools for medical applications is governed by the **Medical Device Regulation (MDR)** (Regulation (EU) 2017/745), which establishes the legal framework for ensuring the safety, efficacy, and quality of medical devices within the European Union. The MDR applies to any software, including AI-driven tools, intended to be used for medical purposes such as diagnosis, prevention, monitoring, or treatment of diseases.[7]

<u>Key MDR Provisions Relevant to AI Imaging Tools</u>

1) Classification of AI Imaging Tools:

AI imaging tools are classified based on their intended use and potential risk to patients, with higher-risk applications (e.g., tools providing diagnostic advice) requiring more stringent conformity assessments. Many AI tools fall under Class IIa, IIb, or III, depending on the complexity and criticality of the tool's function.[8]

2) General Safety and Performance Requirements (GSPRs):

AI imaging tools must meet specific GSPRs outlined in the MDR, ensuring safety, technical performance, and clinical benefit. Particular attention must be paid to risks related to software errors, data integrity, and biases in AI algorithms.[9]

3) Software as a Medical Device (SaMD):

The MDR recognizes software, including AI algorithms, as medical devices when they perform medical purposes independently of hardware. AI tools must demonstrate compliance with requirements for software validation, cybersecurity, and real-world performance.[10]

4) Conformity Assessment:

For AI imaging tools, conformity assessments involve clinical evaluations to verify the device's performance and safety. This includes assessing the accuracy, reproducibility, and reliability of AI-driven outputs using representative datasets to ensure validity.[11]

5) Post-Market Surveillance:

[7] MDR Article 2(1)

[8] MDR Annex VIII

[9] MDR Annex I

[10] MDR Annex I, Section 17

[11] MDR Articles 52–58

Continuous monitoring of AI tools after deployment is required to identify and mitigate risks arising from updates, evolving data environments, or unexpected use cases. AI imaging tools must have mechanisms for real-time performance monitoring and regular updates to meet MDR requirements.

Challenges Specific to AI Imaging Tools

1) Bias and Fairness:

MDR compliance requires that AI tools do not introduce bias that could compromise safety or fairness across patient demographics. Therefore, developers must ensure that training datasets are representative of the target population to avoid biases that could impact diagnosis or treatment recommendations.[12]

2) Transparency and Explainability:

Clear documentation on the algorithms' functioning and limitations must accompany the AI tool.[13]

3) Continuous Learning and Updates:

AI imaging tools with self-learning capabilities (e.g., updating based on new data) must undergo re-certification or demonstrate ongoing compliance.[14]

[12] MDR Annex I, Section 17

[13] MDR Annex I, Section 23

[14] MDR Article 10(14)

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**).

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

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%20leadershi 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/