DIGIDEFENCE ASSESSMENT TOOL

[COMPANY NAME] [Company address]

DIGIDEFENCE ASSESSMENT TOOL

Name of the AI System	
Organisation Details	
Report Details	
Assessment Type	
Document Date	
Document Owner	
Document Authors	

DISCLAIMER

Thank you for using DIGIDEFENCE Assessment. Please be advised of the following:

- This self-assessment tool is intended to support parts of the process of achieving compliance with legal frameworks such as EU AI Act, GDPR (Regulation 2016/679 and Directive 2016/680) and any other legal provisions of which the DIGIDEFENCE Assessment question set could interact with. However, this self-assessment tool is neither conclusive nor does it certify compliance. It does especially not substitute the responsibility of the user of the tool to ensure conclusive compliance. The tool is only meant to give generic guidance and shall not be construed as being official advise.
- The reports generated, that are solely based on the input provided by the user is not a formal certification and does not constitute or replace legal advice for compliance with the aforementioned legal frameworks.
- Participation is voluntary. Users are encouraged to exercise their own discretion when using this tool and provide accurate information where requested.
- The regulatory landscape is subject to change, and interpretations of legal provisions may evolve. The DIGIDEFENCE Assessment self-assessment and its EU AI Act element are based on information available up to its last update and may not reflect subsequent changes in the law.
- Users bear the responsibility for the accuracy and completeness of the information provided in response to the tool's questions.
- By choosing to use the DIGIDEFENCE Assessment tool, you acknowledge and agree to the terms of this disclaimer.

Content

Table of Contents

Assessment

1. General

This section collects information about the context of the assessment. It further aims to determine whether the AI system is subject to the provisions of the EU AI Act, whether its implementation is classified under prohibited AI practices, or is considered a high-risk application.

1.1. What is the name of the AI System?
[*insert your response here*]
1.2. Please provide a short description of the AI system, the functionalities it has and how it will be used.
[*insert your response here*]
1.3. Which statement best describes your organisation?
☐ My organisation places on the market or puts into service an AI system in the EU, irrespective of where my organisation/entity is located. ☐ My organisation deploys an AI system and is an entity established in the EU. ☐ My organisation is an entity established outside the EU, where either Member State law applies by virtue of a public international law or the output produced by the AI system is used in the EU. ☐ My organisation is an entity established outside the EU. ☐ My Organisation is a public authority in a third country or an international organisation falling under options 1, 2. or 3, above and uses AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the EU or with one or more Member States, and my third country or international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals.
1.4. What is the role of your organisation with respect to the AI system? *(Please mark all that apply)*
☐ **Provider**: means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge, Art. 3(3); Note that there may be multiple providers along the AI lifecycle and that there are obligations on former providers. ☐ **Downstream Provider**: means a provider of an AI system, including a general-purpose AI system, which integrates an AI model, regardless of whether the AI model is provided by themselves and vertically integrated or provided by another entity based on contractual relations, Art. 3(68). ☐ **Deployer**: means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity, Art. 3(4). ☐ **Distributor**: any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market, Art. 3(7).

☐ **Importer**: means any natural or legal person located or established in the EU that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country, Art. 3(6).

☐ **Product Manufacturer**: considered to be the provider of the high-risk AI system, and shall be subject to the obligations under Article 16 under either of the following circumstances: (a) the high-risk AI system is placed on the market together with the product under the name or trademark of the product manufacturer; (b) the high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market, Art. 25(3).

☐ **Authorised Representative**: means any natural or legal person located or established in the EU who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by the EU AI Act, Art. 3(5).

1.5. Which statement best describes your work on the AI system?

'Substantial modification' means a change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider and as a result of which the compliance of the AI system with the requirements set out in Chapter II, Section 2 is affected or results in a modification to the intended purpose for which the AI system has been assessed.

☐ Put a different name/trademark on an existing high-risk AI system.
☐ Modify an existing high-risk AI system.
☐ Modify an existing AI system, that is not high-risk, in a way that makes it a high-risk system.
☐ None of the above.

1.6. What is the intended purpose of the AI system? *(Mark all that apply)*

Art. 5 defines prohibited AI practices. Art. 50 (1) to (4) contains transparency obligations which do not apply if the AI system is authorised by law to detect, prevent, investigate or prosecute criminal offences, as long as there are appropriate safeguards for the rights and freedoms of third parties. This exemption for law enforcement puposes does not apply to AI systems that are available for the public to report a criminal offence.

☐ Use for military, defence or national security purposes.
☐ Use solely for scientific research and development.
☐ Use by a public authority in third country or by an international organisation within the framework of international cooperation or agreement for law enforcement and judicial cooperation with the EU or with at least one Member State; and the third country or the international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals.
☐ AI system is released under a free and open-source licence and is neither placed on the market or put into service as high-risk AI system or as an AI system that falls under Art. 5 or 50.
☐ Use by natural persons as deployers in the course of a purely personal non-professional activity.
☐ None of the above.

1.7. Which statements best describe the nature of the AI system? *(Mark all that apply)*

☐ System that deploys subliminal techniques to materially distort a person's behaviour by impairing their ability to make an informed decision, thereby causing them or another person significant harm.
☐ System that exploits vulnerabilities of a person or group to materially distort their behaviour which is reasonably likely to cause them or another person significant harm.
☐ Social scoring leading to detrimental or unfavourable treatment either in unrelated contexts or disproportionately.
☐ Biometric categorisation based on race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.

☐ Predictive policing (risk assessments of natural persons to assess/predict the risk of them committing a criminal offence, based solely on profiling of the natural person or on assessing their personality traits and characteristics).
☐ Real-time remote biometric identification in publically accessible spaces for the purposes of law enforcement which is not strictly necessary for one of the following objectives: (i) targeted search for specific victims of abduction, trafficking in or sexual exploitation of human beings, or the search for missing persons, (ii) prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and either present or foreseeable threat of a terrorist attack; (iii) localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences.
☐ Create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.
☐ Infer emotions of natural persons in the areas of workplace and education institutions.
☐ Untargeted use for post-remote biometric identification without any link to a criminal offence, a criminal proceeding, a genuine and either present or foreseeable threat of a criminal offence, or the search for a specific missing person.
☐ None of the above.

1.8. Is the AI system intended for any of the following deployment areas (Annex III)? *(Mark all that apply)*

These categories are only relevant to the internal security domain. For a full list of high-risk AI applications, please refer to Annex III of the EU AI Act.

☐ Biometrics other than the prohibited practices.
☐ Critical infrastructure.
☐ Educational and vocational training.
☐ Law enforcement.
☐ Migration, asylum and border management.
☐ Administration of justice and democratic processes.
☐ None of the above.

1.9. Does the AI system meet the requirements of a General-Purpose AI Model?

'A 'general-purpose AI model' is an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are released on the market, Art. 3 No. 63.

☐ Yes
☐ No

1.10. Has an ethics assessment been carried out on the AI System?

Ethics checks represent a broad consideration of relevant standards of conduct and behaviour, progressing beyond legality. Please consider national standards, principles and codes of practice, including non-statutory expectations. Assessment List for Trustworthy AI (ALTAI) is an example of an ethics assessment.

☐ Yes
☐ No

If yes , detail which ethics framework or policy has been used.

[*insert your response here*]

1.11. Does the AI system pose a significant risk of harm to the health, safety or fundamental rights of natural persons (including by not materially influencing the outcome of decision making)?

This refers to scenarios where one or more of the following conditions are fulfilled:
(a) the AI system is intended to perform a narrow procedural task;
(b) the AI system is intended to improve the result of a previously completed human activity;
(c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
(d) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III. However, an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons.

☐ Yes
☐ No

1.12. Please explain what the purpose/focus of the AI model is within your tool?

Clearly outline the purpose or focus of the AI aspect of the system, for example, include whether it is for the development of an AI model, enhancement of an existing AI model, or adding usability, frontend, and related features. Ensure you have explicit permission to use the model for these specific purposes before proceeding. Where there are multiple models contained within an overall AI System, each model should have a separate accountability assessment. If a single model performs multiple functions, state them all in a single assessment.

[*insert your response here*]

1.13. What type of AI model is used?

☐ An existing model trained externally (outside your organisation).
☐ A model trained internally (within your organisation or by a Project Consortium Member).
☐ A combination of self-trained models and models trained by another organisation(s).

2. Accountability

To make AI Accountability assessable, report defines 12 Accountability Principles that together create AI Accountability:

Lawfulness

Lawfulness includes compliance with specific legal requirements (such as the EU AI Act where applicable) and – going beyond law in a narrow sense – the principle of also includes your organizational policies which must be clearly identified and readily available.

Completeness

Accountability arrangements must cover all relevant aspects of AI deployments, including partners and sub-contractors. This principle effectively extends the reach of the accountability arrangements and reflects the fact that AI applications are necessarily multi-partner input programmes. Public trust and confidence must extend to the whole AI ecosystem including design, development and supply. Where there are any gaps in the accountability arrangements (such as areas not expressly covered by the law), the protection and promotion of fundamental rights and freedoms should prevail.

Inclusivity

Oversight must involve all relevant stakeholders engaged in and affected by a specific AI deployment. The principle of inclusivity builds in diversity and reduces the risk of bias (actual or perceived) where everyone regulating the AI system seems to come from the same background as those who are using it. Inclusivity can be achieved by having broad participation of stakeholders in creating policy, reviewing deployment and looking for learning points.

Transparency

Accountability needs clear, accurate and meaningful information. This Principle is intended to ensure such information about AI systems is available (subject to operational sensitivities); it is also about the overall accountability arrangements. Information should establish the necessity and proportionality of use of AI systems and highlight foreseeable risks. This principle aims to promote public trust and confidence by enabling those directly and indirectly affected to make informed judgments and risk assessments about the use of an AI system and the accountability arrangements.

Impartiality

Accountability bodies need to be impartial and independent without any conflict of interest. For external accountability paths - such as courts and regulators - this is usually built in. Complete independence internally is almost impossible as many key decision makers will be from the same organisations. Wherever practicable, individuals and organisations involved in the accountability mechanisms for AI systems should have a degree of independence from the line management structure of those involved in their design, development, supply and deployment. This applies in a personal, political, financial and functional way; any conflict of interest must be identified and addressed.

Proof

Follow the evidence law enforcement bodies are very familiar with capturing, analysing and presenting relevant, reliable evidence. Accountability requires a forensic approach to all aspects of AI systems and of the accountability process itself, demanding and following clear evidence. The quality of that evidence should reflect the potential impact of the AI system's use/ non-use and mirror the standards of operational evidence gathering in terms of integrity, credibility and continuity.

Enforceability and Redress

Without a 'so what?' element, accountability will be heavily diluted. For it to be meaningful to stakeholders, accountability must be underpinned by mechanisms giving people an effective remedy. These will include external legal and procedural routes for complaint and challenge but internal mechanisms for individual enforceability and redress (such as professional and policy standards) and contractual arrangements are vital. Enforceability and Redress is closely linked to the principle of lawfulness and can be achieved via national regulators, however, the ability of oversight bodies to intervene, to require policy reviews and to publish findings are also an important part of accountability.

Compellability

Closely linked to enforceability and redress, this principle means oversight bodies must be in position to make the accountability arrangements work. External compellability will usually come from legal or democratic frameworks, while internal frameworks should authorise the provision of necessary information and access by creating formal obligations and without the need to deploy external legal powers. For example, there should be mechanisms to access the necessary information about the deployment and functioning of AI systems. Policies should give relevant bodies the ability to compel the sharing of necessary information and evidence required under some of the other principles without having to invoke the legal powers of courts and tribunals. The timely provision of relevant, up to date and accurate information in an intelligible format contributes to the accountability process. Linked closely with enforceability and redress, this principle will be supported by contracts and Data Sharing Agreements.

Explainability

Those using AI systems need to provide information about it in a meaningful way that is easily understood by the relevant participants/audience. Being able to explain the AI system in a technical and legal setting is one part of this principle. A harder challenge is being able to explain it more generally in non-technical language so that the citizen and their representatives can understand, participate and challenge the use of AI. As with compellability, requirements for a basic level of explainability might be written into contractual agreements with designers, providers and partners.

Constructiveness

Accountability is more than criticism. This Principle means all stakeholders participating constructively with a shared aim of improvement. This may include considering different perspectives, inviting challenge and recognising how disagreement can lead to beneficial solutions. Constructive accountability will be needed to build trust and confidence in the use of AI, internally and externally.

Conduct

The conduct of policing will increasingly include the use of AI technology and this Principle is both individual and organisational. It relates to professional standards, values and expected behaviours which incorporate integrity and ethics. This Principle extends the formal responsibilities to an AI context, where adherence to agreed AI-specific standards is of crucial importance to trust and confidence. Where partners using the AI system are from different jurisdictions, with different legal systems and cultures, there may be a requirement for closer scrutiny and review mechanisms. The European Code of Police Ethics states, "the condition of a democracy can often be determined just by examining the conduct of its police" and the expectations of individuals or organisations involved in AI systems should be expressly identified in advance. In this respect the approach may vary according to the country or agency involved, ranging from internal complaints handling, dispute resolution and mediation frameworks to formal professional proceedings before courts or tribunals.

Learning

This principle promotes the willingness of organisations and people to improve AI in every respect through the application of (new) knowledge and insights. It applies to everyone, and everything involved in the design, use and oversight of AI in the internal security domain (security practitioners and partners, industry, oversight bodies, etc.). Learning includes the modification and improvement of systems, structures, practices, processes, knowledge and resources, as well as the development of professional doctrine and agreed standards.

2.1. Does the AI system have a clearly defined purpose?

☐ Yes
☐ Partially
☐ No

Please describe the purpose.

[*insert your response here*]

2.2. Can the purpose be achieved by alternative means, i.e., without involving the AI system?

☐ Yes
☐ Partially
☐ No

Describe why not, or if yes, why the AI system is preferable.

[*insert your response here*]

2.3. Are decisions made by the AI able to be influenced or changed?

The AI system, and AI models within it, should be resilient against adversarial machine learning.

☐ Yes
☐ Partially
☐ No

Please provide all details of this vulnerability, and steps taken to mitigate this risk.

[*insert your response here*]

2.4. Are wrong decisions or outcomes by the AI system fully reversible?

☐ Yes
☐ Partially
☐ No

Please describe the procedure by which decisions/outcomes can be reversed.

[*insert your response here*]

2.5. Are decisions of the AI system, and how those decisions are reached, documented?

☐ Yes
☐ Partially
☐ No

Please provide details of how decisions are logged, both by the system itself and responsible actors using it.

[*insert your response here*]

2.6. Are the features of the AI system and the rationale for the choice of these features clearly documented?

☐ Yes
☐ Partially
☐ No

Provide rationale for choice of features.

[*insert your response here*]

2.7. Is it clearly documented who is responsible for the AI system design, procurement, implementation or modification, including feature selection?

☐ Yes
☐ Partially
☐ No

Provide a list responsible actors.

[*insert your response here*]

3. DATA

The "Data" topic collects information on the types and sources of the data used for the development and deployment of the AI system, procedures for data acquisition and management and responsible actors.

3.1. Are the nature and source(s) of training, validation and test data documented?
☐ Yes ☐ Partially ☐ No **Describe the nature and source of the data, documentation process and responsible actor(s).** [*insert your response here*]
3.2. Is any data used in the development of the AI system acquired from a third-party or re-purposed from existing datasets?
☐ Yes ☐ Partially ☐ No **Please list relevant data, its original source and how the data was obtained.** [*insert your response here*]
3.3. Does any data used in the development or deployment of the AI system include information from marginalised or vulnerable groups?
☐ Yes ☐ Partially ☐ No **Provide a list of group(s).** [*insert your response here*]
3.4. Is the processing of personal data for the development and/or deployment of the AI system necessary and proportionate?
☐ Yes ☐ Partially ☐ No **Provide basis for necessity and proportionality.** [*insert your response here*]
3.5. Are procedures in place to inspect and control the processing of personal data, inlcuding data of special categories (Art. 9 of the GDPR)?
Special categories of data can only be processed when meeting one of the exceptions listed below (Article 9(2) GDPR): *1. Explicit consent;*

2. Necessary for employment and social security purposes;
3. Protection of the vital interests of the data subject or of another natural person;
4. In the course of legitimate activities by a foundation and similar bodies;
5. Related to personal data which are manifestly made public by the data subject;
6. Necessary for the establishment, exercise or defence of legal claims;
7. Necessary for reasons of substantial public interest, on the basis of the EU or member state law;
8. Necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

☐ Yes
☐ Partially
☐ No

Provide details of the process and responsible actors.

[*insert your response here*]

3.6. Does the processing of personal data have human oversight?

☐ Yes
☐ Partially
☐ No

Provide details, including actors/roles involved.

[*insert your response here*]

3.7. Does the processing of personal data for the AI system adhere to retention policies?

☐ Yes
☐ Partially
☐ No

Provide details of policies and procedures.

[*insert your response here*]

3.8. Is it documented how training, validation and test data was chosen, designed, collected and prepared (e.g., annotation, labelling, cleaning)?

☐ Yes
☐ Partially
☐ No

Describe relevant procedures and rationale for their choice, including actors responsible.

[*insert your response here*]

3.9. Are clear rules and responsibilities established on how data is collected, collated and shared?

☐ Yes
☐ Partially

☐ No

Provide details on procedures and responsible actors.

[*insert your response here*]

3.10. Are clear rules and responsibilities established regarding data publication?

☐ Yes
☐ Partially
☐ No

Describe procedures and responsible actors.

[*insert your response here*]

3.11. Is compliance with the GDPR principles assured?

Article 5 of the GDPR sets out the following principles:
1. Lawfulness, fairness and transparency: data processing must be conducted according to current legislation, in a transparent and fair manner;
2. Purpose limitation: data processing must take place to achieve specified, explicit and legitimate purposes;
3. Data minimisation: data collected must be adequate, relevant and limited to the purposes;
4. Accuracy: personal data must be accurate and, if necessary, kept up to date;
5. Storage limitation: personal data must be stored in a form that allows the identification of the data subject only for the time strictly necessary to achieve the purposes for which they were collected; and
6. Integrity and confidentiality: personal data must be processed in a manner that ensures the avoidance of unauthorized or unlawful process, loss, destruction or damage.

☐ Yes
☐ Partially
☐ No

Provide your reasoning.

[*insert your response here*]

3.12. Is a DPIA (Data Protection Impact Assessment) in place?

☐ Yes
☐ Partially
☐ No

Provide your reasoning.

[*insert your response here*]

3.13. Is the Data Protection Impact Assessment (DPIA) regularly updated?

☐ Yes
☐ Partially
☐ No

Describe frequency of updates and responsible actors.

[*insert your response here*]

3.14. Is an appropriate data protection policy in place?

☐ Yes
☐ Partially
☐ No

Describe procedures and responsible actors.

[*insert your response here*]

3.15. Are appropriate technical and organisational measures in place to integrate data protection into all processing activities?

Appropriate technical and organisational measures may include, but are not restricted to (Article 32 GDPR): Pseudonymisation and encryption of personal data; Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing and systems; Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures can ensure the security of the project.

☐ Yes
☐ Partially
☐ No

Describe measures and responsible actors.

[*insert your response here*]

3.16. Is an effective process in place to identify and report any personal data breaches?

☐ Yes
☐ Partially
☐ No

Describe process and responsible actors.

[*insert your response here*]

3.17. Have written contracts been signed with all data processors?

☐ Yes
☐ Partially
☐ No
☐ Not-Applicable

Provide your reasoning.

[*insert your response here*]

3.18. Is compliance with data protection policies monitored and the effectiveness of data handling and security controls regularly reviewed?

☐ Yes
☐ Partially
☐ No

Describe procedures and responsible actors.

[*insert your response here*]

3.19. Is data protection awareness training provided for all staff?

☐ Yes
☐ Partially
☐ No

Describe type and regularity of training.

[*insert your response here*]

4. Laws and regulations

The 'Laws and regulation' topic identifies the relevant laws, regulations and policies for the AI system and purpose under assessment. For a comprehensive assessment, please refer to AI Act part.

4.1.	**Have all applicable laws, regulations and policies for the deployment of the AI system and its purpose been identified, including legal exemptions and safeguards?**
☐ Yes ☐ Partially ☐ No **List the relevant laws, regulations and policies.** [*insert your response here*]	
4.2.	**Is the use of the AI system necessary and proportionate for the given purpose?**
☐ Yes ☐ Partially ☐ No **Provide basis for necessity and proportionality.** [*insert your response here*]	

5. Risk assessment and management

The 'Risk assessment and management' topic collects information about the (possible) risks, harms and impacts related to the deployment of the AI system, the mitigation measures to address/mitigate these risks/impacts and the actors responsible.

5.1. Does the deployment of the AI system pose risks for specific groups and communities?
☐ Yes ☐ Partially ☐ No **Describe type of risks and groups affected.** [*insert your response here*]
5.2. Is the deployment of the AI system associated with any other risks (apart from those affecting specific groups or communities)?
☐ Yes ☐ Partially ☐ No **Describe type of risks.** [*insert your response here*]
5.3. Are there potential residual risks despite legal compliance and procedures to address them?
☐ Yes ☐ Partially ☐ No **Describe residual risk.** [*insert your response here*]
5.4. Can harms occur if the AI system is misused or not used properly?
☐ Yes ☐ Partially ☐ No **Describe type of harms.** [*insert your response here*]
5.5. Can harms occur if the AI system is NOT used?
☐ Yes

☐ Partially
☐ No

Describe type of (potential) harms.

[*insert your response here*]

5.6. Is there any risk of bias in the processing of personal data?

☐ Yes
☐ Partially
☐ No
☐ Not Applicable

Describe type of biases.

[*insert your response here*]

5.7. Are there any other risks regarding AI systems processing personal data?

☐ Yes
☐ Partially
☐ No

Describe impacts.

[*insert your response here*]

5.8. Has a formal risk assessment been carried out?

☐ Yes
☐ Partially
☐ No

Provide the source and overall outcome of the risk assessment.

[*insert your response here*]

5.9. Are there measures in place to prevent or rectify data bias?

☐ Yes
☐ Partially
☐ No

Describe procedures and responsible actors.

[*insert your response here*]

5.10. Are there measures in place to address security, privacy and confidentiality risks?

☐ Yes
☐ Partially
☐ No

Describe the measures and roles responsible.

[*insert your response here*]

5.11. Are there measures in place to address unintended consequences of the AI system?

☐ Yes
☐ Partially
☐ No

Describe procedures and roles responsible.

[*insert your response here*]

5.12. Are there measures in place for managing information risks?

☐ Yes
☐ Partially
☐ No

Describe procedures and responsible actors.

[*insert your response here*]

6. Oversight and redress

The 'Oversight and redress' topic identifies the relevant oversight bodies responsible to monitor, assess and enforce the appropriate use of the AI system under assessment, as well as the oversight process and redress process.

6.1.	**Has it been identified who is responsible for monitoring, assessing and enforcing the appropriate use of the AI system, including potential conflicts of interests/dependencies?**
This may include individuals and oversight bodies. ☐ Yes ☐ Partially ☐ No **Please list the relevant people and/or oversight bodies and possible conflicts of interests.** [*insert your response here*]	
6.2.	**Is it clearly identified which information is shared (or restricted from sharing) with relevant oversight bodies and on how the information is shared?**
☐ Yes ☐ Partially ☐ No ☐ Not Applicable **Please describe shared/restricted information and procedures for sharing.** [*insert your response here*]	
6.3.	**Have the procedures and responsible actors for informing and overseeing communication with oversight bodies, including procedures to compel provision of information, been established?**
☐ Yes ☐ Partially ☐ No ☐ Not Applicable **Please list processes and responsible actor(s).** [*insert your response here*]	
6.4.	**Are measures in place for affected stakeholders to complain/request redress?**
☐ Yes ☐ Partially ☐ No ☐ Not Applicable **Please describe complaint and/or redress measures.**	

[*insert your response here*]

7. Stakeholders

The 'Stakeholder' topic identifies the stakeholders involved and/or affected by the deployment of the AI system. It further considers effective engagement, responsible actors and societal interests/concerns.

7.1. Are there clear criteria for identifying relevant stakeholder groups?
☐ Yes ☐ Partially ☐ No **Please list the inclusion/exclusion criteria.** [*insert your response here*]
7.2. Have all stakeholders that will use the AI system been identified?
☐ Yes ☐ Partially ☐ No **Please list the stakeholders.** [*insert your response here*]
7.3. Have all stakeholders that need to be informed about the deployment of the AI system been identified?
☐ Yes ☐ Partially ☐ No **Please list the stakeholders.** [*insert your response here*]
7.4. Have all stakeholders that will/may be affected by the deployment of the AI system been identified?
☐ Yes ☐ Partially ☐ No **Please list the stakeholders.** [*insert your response here*]
7.5. Do any of the stakeholders possess protected characteristics?
☐ Yes ☐ Partially ☐ No

Please list the groups and characteristics.

[*insert your response here*]

7.6. Are adequate mechanisms in place to ensure meaningful engagement and communication with all key stakeholders?

☐ Yes
☐ Partially
☐ No

Please describe mechanisms and responsible actors.

[*insert your response here*]

7.7. Are there stakeholder groups that will be challenging to inform or engage with?

☐ Yes
☐ Partially
☐ No

Please list the groups and type of challenges.

[*insert your response here*]

7.8. Do all relevant stakeholders have a sufficient understanding of the purposes, risks and consequences of the AI system?

☐ Yes
☐ Partially
☐ No

Please describe measures how understanding is ensured.

[*insert your response here*]

7.9. Are efforts made to understand and address concerns and expectations of society?

☐ Yes
☐ Partially
☐ No

Provide your reasoning.

[*insert your response here*]

8. Accountability evidence

The 'Accountability evidence' topic collects information about the type of evidence used to demonstrate accountability, the criteria to determine that the evidence is robust, as well as the process to collect and manage the evidence and responsible actors.

8.1. Are clear criteria in place on how to define and assess sufficient 'robustness' of information used to show appropriate AI use?

☐ Yes
☐ Partially
☐ No

Please describe the criteria.

[*insert your response here*]

8.2. Are procedures in place to ensure that the evidence used to demonstrate accountability remains relevant and consistent?

Periodic review is needed to ensure that evidence proving accountability continues to be valid over time. There also may be a need for review triggered by a key event, such as system updates or an adverse incident. There is a need to maintain a consistency in how this evidence is presented and records of the update process.

☐ Yes
☐ Partially
☐ No

Please describe the procedures.

[*insert your response here*]

8.3. Are the policy documents, and other relevant records governing accountability, protected from subsequent alterations?

☐ Yes
☐ Partially
☐ No

Please describe processes and procedures in place.

[*insert your response here*]

8.4. Is the evidence used to demonstrate accountability subject to legal or sector-specific constraints?

☐ Yes
☐ Partially
☐ No

If yes, describe relevant constraints.

[*insert your response here*]

8.5.	**Is the evidence used to demonstrate accountability accessible to all relevant stakeholder/oversight bodies?**

☐ Yes
☐ Partially
☐ No

Please describe measures to achieve this and possible limitations of access.

[*insert your response here*]

8.6.	**Is evidence to demonstrate accountability provided in an understandable way to all relevant stakeholders?**

☐ Yes
☐ Partially
☐ No

Please describe measures.

[*insert your response here*]

9. Adaptability and learning

The topic 'Adaptability and learning' collects information about mechanisms and responsible actors to ensure that necessary improvements to the AI system and the accountability process are made.

9.1.	**Are all people involved in developing, deploying and using the AI system aware of their responsibilities with respect to AI Accountability?**

☐ Yes
☐ Partially
☐ No

Please provide details of procedures and responsible actors to achieve and maintain this.

[*insert your response here*]

9.2.	**Are processes in place to ensure meaningful improvements to the AI system and/or its deployment?**

☐ Yes
☐ Partially
☐ No

Please describe the process and means to compel improvements.

[*insert your response here*]

9.3.	**Is a process in place to review and, if needed, to update AI accountability procedures?**

☐ Yes
☐ Partially
☐ No

Please describe the process and responsible actors.

[*insert your response here*]

10. Fundamental Rights Impact Assessment (FRIA)

The aim of the fundamental rights impact assessment is for the deployer to identify the specific risks to the rights of individuals or groups of individuals who are likely to be affected and identify measures to be taken in the case of materialisation of those risks. The impact assessment should apply to the first use of the high-risk AI system and should be updated when the deployer considers that any of the relevant factors have changed. The impact assessment should identify the deployer's relevant processes in which the high-risk AI system will be used in line with its intended purpose, and should include a description of the period of time and frequency in which the system is intended to be used as well as of specific categories of natural persons and groups who are likely to be affected in the specific context of use.

10.1. Is an accurate description of the deployer's process and the intended purpose of the high-risk AI system available?
☐ Yes ☐ No
10.2. Is information available about the period of time within which the high-risk AI system is intended to be used, and the frequency of its use?
Article 27 (b) requires a time frame and how often a high-risk AI system will be used for the specific purpose it is intended for. If the AI system operates continuously please state that. ☐ Yes ☐ Partially ☐ No **Provide your reasoning.** [*insert your response here*]
10.3. Are there categories of natural persons and groups that are likely to be affected by the system's use in a specific context? If yes, please list these groups.
You must provide a description of the natural persons your system will impact. ☐ Yes ☐ Partially ☐ No **Provide your reasoning.** [*insert your response here*]
10.4. Are measures in place if these risks were to materialise, including arrangements for internal governance and complaint mechanisms?

You must provide measures to mitigate against if these risks were to materialise as per Article 27(1) (f). The response to this question should be related to your risk management compliance measures as detailed in Article 9.

☐ Yes
☐ Partially
☐ No

Provide your reasoning.

[*insert your response here*]

11. Project-Specific Research and Innovation Context: OSOTS

The aim of this section is to evaluate other regulatory and societal context that may be relevant to the development of the particular project.

11.1.	**What legal and regulatory frameworks govern the monitoring and data collection from OT/ICS networks, particularly in critical infrastructure sectors (e.g., energy, water, transport)?**
[*insert your response here*]	
11.2.	**How does the project ensure that the collection and processing of network communication data from sensors and industrial systems complies with national cybersecurity laws and sector-specific regulations?**
[*insert your response here*]	
11.3.	**What legal obligations apply to the deployment of AI-based anomaly detection systems in safety-critical environments, and how are these obligations addressed in the system's design and testing phases?**
[*insert your response here*]	
11.4.	**How is legal accountability established for false positives or missed detections that may impact operational continuity, safety, or compliance in industrial environments?**
[*insert your response here*]	
11.5.	**What certification or conformance requirements (e.g., IEC 62443, NIS2 Directive) must the system meet before it can be deployed in production OT environments?**
[*insert your response here*]	
11.6.	**How does the project address the legal implications of integrating machine learning models into real-time industrial control systems, particularly in terms of explainability, auditability, and human oversight?**
[*insert your response here*]	
11.7.	**If the system is deployed across multiple jurisdictions or sectors, how are legal responsibilities, data ownership, and liability distributed among stakeholders (e.g., developers, operators, infrastructure owners)?**
[*insert your response here*]	
11.8.	**Are there any other considerations that may affect the development of the project?**
☐ Yes ☐ No **Provide a list of such legislation and reasoning how it can affect the implementation of the project.**	

[*insert your response here*]