Procurement of AI Community

● **PUBLIC BUYERS COMMUNITY**

Model contractual clauses for the public procurement of High-Risk AI ("MCC-AI-High-Risk")

Version February 2025 – Procurement of High-Risk AI

DISCLAIMER

This working document is created by the European Commission to support the Community of Practice on the Procurement of AI to guide public administrations in procuring AI solutions. It is a working document in progress and does not reflect an official position of the European Commission.

Actors that decide to make use of this working document carry full responsibility for its use in public procurement.

These Model Clauses for High-Risk AI are without the prejudice to the requirements stemming from the AI Act.

Section A – Definitions

Article 1 Definitions: Capitalised terms used in these MCC-AI-High-Risk will have the meaning as defined in this article.

Agreement: the entire agreement of which the MCC-AI-High-Risk, as a schedule, are an integral part;

AI System: the machine-based system(s) that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments, further specified and described in **Annex A**, including any new versions thereof[1];

MCC-AI-High Risk: these contractual clauses for the public procurement of High-Risk AI by public organisations;

Public Organisation Data Sets: the Data Sets (or parts of) (i) provided by the Public Organisation to the Supplier under the Agreement or (ii) to be created or collected as part of the Agreement, including any modified or extended versions of the Data Sets referred to under (i) and (ii) (for example due to annotation, labelling, cleaning, enrichment or aggregation);

Data Sets: all data sets used in the development of the AI System, including the data set or data sets as described in **Annex B**;

Delivery: the time at which the Supplier informs the Public Organisation that the AI System satisfies all agreed conditions and is ready for use;

Intended Purpose: the use for which an AI System is intended by the Public Organisation, including the specific context and conditions of use, as specified in Annex B, the information supplied by the Supplier in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

Reasonably Foreseeable Misuse: the use of the AI System in a way that is not in accordance with its Intended Purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems, including other AI systems;

---

[1] The Commission publishes guidelines on AI system definition to facilitate the first AI Act's rules application | Shaping Europe's digital future

Substantial Modification: a change to the AI System after the Delivery which is not foreseen or planned in the initial conformity assessment carried out by the Supplier and as a result of which the compliance of the AI System with the requirements set out in these MCC-AI-High-Risk is affected (without the prejudice to Chapter III Section 2 of the AI Act) or results in a modification to the Intended Purpose for which the AI system has been assessed;

Supplier: the natural or legal person, public authority, agency or other body that supplies the AI System to the Public Organisation pursuant to the Agreement;

Supplier Data Sets and Third-Party Data Sets: the Data Sets (or parts of) that do not qualify as Public Organisation Data Sets.

Section B – Essential requirements in relation to the AI-system

Article 2 Risk management system

2.1. The Supplier ensures that, prior to the Delivery of the AI System, a risk management system shall be established, implemented, documented and maintained in relation to the AI System.

2.2. The risk management system shall at least comprise the following steps:

    a. identification, estimation and evaluation of the known and reasonably foreseeable risks that the AI System can pose to health, safety or fundamental rights when the AI System is used in accordance with the Intended Purpose;

    b. the estimation and evaluation of the risks that may emerge when the AI System is used in accordance with the Intended Purpose, and under conditions of Reasonably Foreseeable Misuse;

    c. evaluation of other possibly arising risks, based on the analysis of data gathered from the post-market monitoring system;

    d. adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point a, of this paragraph in accordance with the provisions of the following paragraphs.

2.3. The risks referred to in this article shall concern only those which may be reasonably mitigated or eliminated through the development or design of the AI System, or the provision of adequate technical information.

2.4. The risks referred to in this article shall give due consideration to the effects and possible interaction resulting from the combined application of the requirements set out in Section B, with a view to minimising risks more effectively while achieving an appropriate balance in implementing the measures to fulfil those requirements.

2.5. The risk management measures referred to in paragraph 2.2, point (d) shall be such that relevant residual risks associated with each hazard as well as the overall residual risk of the AI system is judged to be acceptable by the Supplier, provided that the AI System is used in accordance with the Intended Purpose or under conditions of Reasonably Foreseeable Misuse.

2.6. In identifying the most appropriate risk management measures referred to in paragraph 2.2, point (d), the following shall be ensured:

    a. elimination or reduction of risks identified and evaluated pursuant to paragraph 2.2 in as far as technically feasible through adequate design and development of the AI System;

    b. where appropriate, implementation of adequate mitigation and control measures addressing risks that cannot be eliminated;

    c. provision of adequate information to the Public Organisation and if applicable, training to deployers.

2.7. The Supplier ensures that, prior to the Delivery of the AI System, the AI System is tested in order to identify whether the AI System complies with the MCC-AI-High-Risk and whether the risk management measures referred to in paragraph 2.2, point (d) are effective in light of the Intended Purpose and Reasonably Foreseeable Misuse. If

requested by the Public Organisation, the Supplier is obliged to test the AI System in the environment of the Public Organisation. ,

2.8. The testing of the AI System shall be performed, as appropriate, at any time throughout the development process, and, in any event, prior to the Delivery. Testing shall be carried out against prior defined metrics and probabilistic thresholds that are appropriate to the Intended Purpose of the AI System.

2.9. All risks identified, measures taken and tests performed in the context of compliance with this article must be documented by the Supplier. The Supplier must make this documentation available to the Public Organisation at least at the time of the Delivery of the AI System. This documentation can be part of the technical documentation and/or instructions for use.

2.10. The risk management system shall be understood as a continuous and iterative process planned and run throughout the entire duration of the Agreement. After the Delivery of the AI System the Supplier must therefore:
    a. regularly review and update the risk management process, to ensure its continuing effectiveness;
    b. keep the documentation described in article 2.7 up to date; and
    c. make every new version of the documentation described in article 2.7 available to the Public Organisation without delay.

2.11. If reasonably required for the proper execution of the risk management system by the Supplier, the Public Organisation will provide the Supplier, on request, with information insofar as this is not of a confidential nature.

2.12. **<Optional>** If the Public Organisation's use of the AI System continues beyond the term of the Agreement, at the end of the term of the Agreement, the Supplier shall provide the Public Organisation with the information necessary to maintain the risk management system by itself.

Article 3 **< Article 3 is only relevant for AI Systems which make use of techniques involving the training of models with data. Article 3 presupposes the Supplier (or its subcontractors) has (have) full access to the Data Sets. If the Data Sets are exclusively held by the Public Organisation, it is necessary to make other arrangements.>** Data and data governance

3.1. The Supplier ensures that the Data Sets used in the development of the AI System, including training, validation and testing, have been and shall be subject to data governance and management practices appropriate for the Intended Purpose of the AI System. Those measures shall concern in particular:
    a. the relevant design choices;
    b. data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection
    c. relevant data preparation for processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;
    d. the formulation of assumptions, with respect to the information that the data are supposed to measure and represent;

e.   an assessment of the availability, quantity and suitability of the data sets that are needed;

f.   examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations;

g.   appropriate measures to detect, prevent and mitigate possible biases identified according to point (f);

h.   the identification of relevant data gaps or shortcomings that prevent compliance with these MCC-AI-High-Risk, and how those gaps and shortcomings can be addressed.

3.2.   The Supplier ensures that the Data Sets used in the development of the AI System are relevant, sufficiently representative, and to the best extent possible, free of errors and complete e in view of the Intended Purpose. The Supplier ensures that Data Sets have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the AI System is intended to be used. These characteristics of the Data Sets shall be met at the level of individual data sets or a combination thereof.

3.3.   The Supplier ensures that the Data Sets used in the development of the AI System considered, to the extent required by the Intended Purpose or Reasonably Foreseeable Misuse, the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting within which the AI System is intended to be used.

3.4.   The obligations under this article apply not only to the development of the AI System prior to Delivery, but also to any use of Data Sets by the Supplier that may affect the functioning of the AI System at any other time during the term of the Agreement.

Article 4 Technical documentation and instructions for use

4.1.   The Delivery of the AI System by the Supplier includes the handover of the technical documentation and instructions for use.

4.2.   The technical documentation must enable the Public Organisation or a third party to assess the compliance of the AI System with the provisions of the requirements set in these MCC-AI-High-Risk and at least satisfy the conditions described in **Annex C**.

4.3.   The instructions for use shall include concise, complete, correct and clear information that is relevant, accessible and comprehensible to the Public Organisation. The instructions for use must at least satisfy the conditions described in **Annex D**.

4.4.   The Supplier must update this documentation at least with every Substantial Modification during the term of the Agreement, and subsequently make it available to the Public Organisation.

4.5.   **<optional>** The technical documentation and instructions for use must be drawn up in English.

4.6.   **<optional>** The Public Organisation has the right to make copies of the technical documentation and instructions for use to the extent necessary for internal use within

the organisation of the Public Organisation, without prejudice to the provisions of article 6 and article 14.

Article 5 Record-keeping

5.1.   The Supplier ensures that the AI System shall technically allow for the automatic recording of events ('logs') over the lifetime of the AI System.

5.2.   The logging capabilities shall ensure a level of traceability of the AI System's that is appropriate to the Intended Purpose of the system and Reasonably Foreseeable Misuse. In particular, they shall enable the recording of events relevant for the identification of situations that may:
   a.   result in the AI System presenting a risk to the health or safety or to the protection of fundamental rights of persons; or
   b.   lead to a Substantial Modification.

5.3.   **<Optional>**The Supplier will allow the Public Organisation to access the logs automatically generated by the AI System on a real time basis.

5.4.   The Supplier shall keep the logs automatically generated by the AI System, to the extent such logs are under its control based on the Agreement, for the duration of the Agreement. At the end of the term of the Agreement, the Supplier will provide these logs to the Public Organisation without delay.

Article 6 Transparency of the AI System

6.1.   The Supplier ensures that the AI System has been and shall be designed and developed in such a way that the operation of the AI System is sufficiently transparent to enable the Public Organisation to interpret the system's output and use it appropriately.

6.2.   To ensure appropriate transparency, before the Delivery of the AI System at least the technical and organisational measures described in **Annex E** shall be implemented by the Supplier.

Article 7 Human oversight

7.1.   The Supplier ensures that the AI System has been and shall be designed and developed in such a way, including with appropriate human-machine interface tools, that it can be effectively overseen by natural persons during the period in which it is in use.

7.2.   Human oversight shall aim to prevent or minimise the risks to health, safety or fundamental rights that may emerge when an AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, where such risks persist despite the application of other requirements set out in this Section.

7.3.   The oversight measures shall be commensurate with the risks, level of autonomy and context of use of the AI system, and shall be ensured through either one or both of the following types of measures:

7.4.   The Supplier ensures that, prior to the Delivery, appropriate measures shall be embedded in the AI System and taken to ensure human oversight. These measures, shall enable the natural persons to whom human oversight is assigned are enabled, as appropriate and proportionate:

    a.   to properly understand the relevant capacities and limitations of the AI System and be able to duly monitor its operation, including in view of detecting and addressing anomalies, dysfunctions and unexpected performance;

    b.   to remain aware of the possible tendency of automatically relying or over-relying on the output produced by the AI System ('automation bias'), in particular if the AI System is used to provide information or recommendations for decisions to be taken by natural persons;

    c.   to correctly interpret the AI System's output, taking into account, for example, in particular the characteristics of the system and the interpretation tools and methods available;

    d.   to decide, in any particular situation, not to use the AI System or otherwise disregard, override or reverse the output of the AI System;

    e.   to intervene on the operation of the AI System or interrupt the system through a "stop" button or a similar procedure that allows the system to come to a halt in a safe state;

7.5.   **<optional>** To ensure appropriate human oversight, the Supplier shall at least implement the technical and organisational measures described in **Annex F** before the Delivery of the AI System**.**

Article 8 Accuracy, robustness and cybersecurity

8.1.   The Supplier ensures that the AI System has been and shall be designed and developed in such a way that it achieves an appropriate level of accuracy, robustness, safety and cybersecurity, and perform consistently in those respects.

8.2.   The levels of accuracy and the relevant accuracy metrics of the AI System are described in **Annex G**.

8.3.   To ensure an appropriate level of robustness, safety and cybersecurity, the Supplier shall at least implement the technical and organisational measures described in **Annex H** before the Delivery of the AI System.

8.4.   This requirement is without the prejudice to the requirements stemming from Article 15 of the AI Act;

Section C – Obligations of the Supplier in relation to the AI System

Article 9 Compliance with Section B

The Supplier must ensure that from the Delivery of the AI System until the end of the term of the Agreement the AI System complies with the requirements established in Section B of these MCC-AI-High-Risk.

Article 10   Quality management system

10.1.   Before the Delivery of the AI System, the Supplier shall put a quality management system in place that ensures compliance with these MCC-AI-High-Risk.

10.2.   The quality management system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:

a.   a strategy for regulatory compliance;

b.   techniques, procedures and systematic actions to be used for the design, design control and design verification of the AI System;

c.   techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the AI System;

d.   examination, test and validation procedures to be carried out before, during and after the development of the AI System, and the frequency with which they have to be carried out;

e.   technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full, or do not cover all of the relevant requirements, the means to be used to ensure that the AI System complies with the requirements set out in Section B of these MCC-AI-High-Risk;

f.   systems and procedures for data management, including data collection, data acquisition, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before the Delivery of the AI System;

g.   the risk management system referred to in article 2;

h.   procedures related to the reporting of serious incidents;

i.   the handling of communication with national competent authorities, other relevant authorities, including those providing or supporting the access to data, notified bodies, other operators, customers or other interested parties;

j.   systems and procedures for record keeping of all relevant documentation and information;

k.   resource management, including security of supply related measures;

l.   an accountability framework setting out the responsibilities of the management and other staff regarding all aspects listed in this paragraph.

10.3.   During the term of the Agreement, the Supplier must keep the documentation concerning the quality management system available. On first request of the Public Organisation, the Supplier will hand over the most recent version of the documentation concerning the quality management system to the Public Organisation.

Article 11   Conformity assessment

11.1.   The Supplier shall ensure that the AI System undergoes the following conformity assessment procedure prior to the Delivery of the AI System:

a.   The Supplier verifies that the established quality management system is following the requirements of article 10.

b.   The Supplier examines the information contained in the technical documentation to assess the compliance of the AI System with the relevant essential requirements set out in Section B of these MCC-AI-High-Risk.

c.   The Supplier also verifies that the design and development process of the AI System is consistent with the technical documentation.

11.2.   The Supplier ensures that the AI System shall undergo a new conformity assessment procedure whenever the AI System is Substantially Modified by the Supplier during the term of the Agreement.

Article 12   **<Optional>**Fundamental rights impact assessment

<Optional>On first request of the Public Organisation, the Supplier shall cooperate in the Public Organisation's performance of an assessment of the impact on fundamental rights that the use of the AI System may produce.

Article 13   Corrective actions

If during the term of the agreement the Supplier considers or has reason to consider that the AI System is not in conformity with these MCC-AI-High-Risk, whether in response to a comment by the Public Organisation or not, it shall immediately take the necessary corrective actions to bring the system into conformity. The Supplier shall inform the Public Organisation accordingly.

Article 14   **<optional>** Obligation to an explanation of individual decision-making

14.1.   **<optional>** In addition to the obligations described in Article 6, the Supplier is obliged to assist the Public Organisation at the Public Organisation's first request in providing a clear and meaningful explanation of the role of the AI system in the decision-making procedure. This meaningful explanation should particularly (but not exclusively) provide insight in the main elements of the decision(s) taken to any affected person who is subject to Public Organisation decision(s) based on the output of the AI System.

14.2.   **<optional>** The obligation as described in article 14.1 comprises the provision to the Public Organisation of all the technical and other information required in order to explain how the AI System produced a particular output and to offer the affected persons the opportunity to verify the way in which the AI System produced a particular output. The Supplier hereby grants the Public Organisation the right to use, share and disclose this information, if and to the extent necessary to inform the affected persons accordingly.

14.3.   **<optional>** The obligations referred to in article 14.1 and article 14.2 include the source code of the AI System, the technical specifications used in developing the AI System, the Data Sets, technical information on how the Data Sets used in developing the AI System were obtained and edited, information on the method of development used and the development process undertaken, substantiation of the choice for a particular model and its parameters, and information on the performance of the AI System.

Section D – Rights to use the Data Sets

Article 15   Rights to Public Organisation Data Sets

15.1.   All rights, including any intellectual property right, relating to Publication Organisation Data Sets will accrue to the Public Organisation or a third party designated as such by the Public Organisation.

15.2.   The Supplier is not entitled to use Publication Organisation Data Sets for any purpose other than the performance of the Agreement, except as otherwise provided in Annex B.

15.3.   On first request of the Public Organisation, the Supplier must destroy Publication Organisation Data Sets, except as otherwise provided in Annex B. If the Public Organisation so demands, the Supplier must provide feasible evidence of the destruction of Publication Organisation Data Sets.

Article 16   Rights to Supplier Data Sets and Third-Party Data Sets

16.1.   All rights, including any intellectual property right, relating to Supplier Data Sets and Third-Party Data sets will accrue to the Supplier or a third party.

16.2.   The Supplier grants the Public Organisation a non-exclusive right to use Supplier Data Sets and Third-Party Data Sets that is in any event sufficient for performance of the provisions of the Agreement, including the MCC-AI-High-Risk, except as otherwise provided in Annex B.

16.3.   **<optional>** The right of use described in article 16.2 includes the right to use Supplier Data Sets and Third-Party Sets for the further development of the AI System, including any new versions thereof, by the Public Organisation or a third party.

Article 17   Handover of the Data Sets

17.1.   On first request of the Public Organisation, the Supplier will handover the most recent version of Public Organisation Data Sets to the Public Organisation.

17.2.   On first request of the Public Organisation, the Supplier will handover the most recent version of the Supplier Data Sets and Third-Party Data Sets to the Public Organisation, except as otherwise provided in Annex B.

17.3.   The Data Sets must be handed over to the Public Organisation by the Supplier in a common file format to be designated by the Public Organisation. **<optional> The Data Sets will be returned as follows: [file format].**

Article 18   Indemnifications

18.1.   The Supplier shall indemnify the Public Organisation from all claims brought by third parties, including supervisors, arising out of any infringement of intellectual property rights, data protection rights or equivalent rights resulting from the use of the AI System, the Supplier Data Sets and/or Third Party Data Sets by the Public Organisation.

18.2.   The Public Organisation shall indemnify the Supplier from all claims brought by third parties, including supervisors, arising out of any infringement of their intellectual property rights, privacy rights or equivalent rights resulting from the use of the Public Organisation Data Sets.

Section E – AI register and audit

Article 19   **<Optional>** AI register

19.1.   At the Public Organisation's first request, the Supplier will provide the Public Organisation with the most recent version of the information described in Annex C and Annex D.

19.2.   The Public Organisation will be entitled to share the information described in article 19.1 with third parties and to disclose it, for example in a register for AI Systems.

19.3.   If the Public Organisation so demands, the Supplier will assist in registering the AI Systems in any relevant register.

Article 20   Compliance and audit

20.1.   At first request of the Public Organisation, the Suppliers must make available to the Public Organisation all information necessary to demonstrate compliance with these MCC-AI-High-Risk.

20.2.   The Supplier is obliged to cooperate in an audit or other type of inspection to be carried out by or on behalf of the Public Organisation to assess whether the Supplier complies with its obligations laid down in these MCC-AI-High-Risk at all times. Such cooperation will include providing all information required by the Public Organisation, providing an insight into the risk management system implemented, making Supplier staff available for interviews and providing access to the locations of the Supplier.

20.3.   The Public Organisation will prepare, or cause the preparation of, a report in which the conclusions of the audit are recorded. In the report, the Public Organisation will record the extent to which the Supplier complies with the obligations under the Agreement. If the Public Organisation establishes that the Supplier does not comply with the obligations under this article, the Supplier will be obliged to remedy the

defects identified by the Public Organisation within the reasonable term set by the Public Organisation in the report. If the Supplier fails to remedy the defects identified by the Public Organisation within the term set in the report for remedying such defects, the Supplier will be in default by operation of law.

20.4. The Public Organisation will be entitled to publish the conclusions of the report referred to in article 20.3.

20.5. The Public Organisation will be entitled to perform, or cause the performance of, an audit once per calendar year or in relation to any Substantial Modification.

20.6. The Public Organisation may decide to have all or part of the audit performed by an independent auditor.

20.7. The costs of the auditor to be engaged by the Public Organisation, if any, will be paid by the Public Organisation. The Public Organisation will pay the Supplier a reasonable fee for any costs to be incurred by the Supplier in the context of the audit. In no event will a dispute about the amount of such fee give the Supplier the right to suspend its obligations under these MCC-AI-High-Risk. No such fee will be owed by the Public Organisation if the audit reveals that the Supplier has failed to perform its obligations under these MCC-AI-High-Risk.

Section F – Costs

Article 21   Costs

Unless agreed otherwise between the parties or expressly provided otherwise in these MCC-AI-High-Risk, no additional fee will be owed to the Supplier by the Public Organisation in consideration of the work ensuing from these MCC-AI-High-Risk.

Annex A – The AI System and the Intended Purpose

Description of the AI System

Within the scope of these MCC-AI-High-Risk are the following systems or components of systems:

Please provide a description of the AI System(s). This can also be an algorithmic system that does not qualify as an AI System under the AI Act.

Intended Purpose

Please provide a description of the use for which the AI System is intended.

Annex B – The Data Sets

Please provide a description of the Data Sets used for the training (if applicable), validation and testing of the AI System. Distinguish between Public Organisation Data Sets and Supplier Data Sets and Third-Party Data Sets. In the case of Public Organisation Data Sets, describe the purposes for which the Supplier may use the Data Sets (other than the performance of the Agreement) and whether the Supplier is required to destroy the Data Set at the end of the term of the Agreement. In the case of Supplier Data Sets and Third-Party Data Sets describe the purposes for which the Public Organisation may use the Data Sets and whether the Supplier is obliged to hand over the Data Sets.

the Public Organisation Data Sets

The following Data Sets are provided by the Public Organisation to the Supplier under the Agreement or to be created or collected as part of the Agreement:

Description of the Data Set	Rights of use of the Supplier	Obligation to destroy the Data Set at the end of the term of the Agreement
		Yes/No
		Yes/No
		Yes/No
		Yes/No

Supplier Data Sets and Third-Party Data Sets

The following Supplier Data Sets and Third-Party Data Sets will be or were used for the training (if applicable), validation and testing of the AI System:

Description of the Data Set	Rights of use of the Public Organisation	Obligation to hand over[2]
		Yes/No
		Yes/No
		Yes/No
		Yes/No

---

[2]   A limitation of the obligation to hand over Supplier Data Sets and Third Party Data Sets, does not limit Supplier's obligations described in article 6 and article 14.

Annex C – Technical documentation

The technical documentation shall contain at least the following information, as applicable to the AI System:

1.   a general description of the AI System including:
    - 1.1.   its intended purpose, the name of the Supplier, and the version of the system reflecting its relation to previous versions;
    - 1.2.   how the AI System can interact or can be used to interact with hardware or software, including other AI systems, that are not part of the AI System itself, where applicable;
    - 1.3.   the versions of relevant software or firmware and any requirement related to version update;
    - 1.4.   the description of hardware on which the AI System is intended to run;
    - 1.5.   where the AI System is a component of products, photographs or illustrations showing external features, marking and internal layout of those products;
    - 1.6.   a basic description of the user-interface provided to the Public Organisation;
    - 1.7.   instructions for use for the deployer, and a basic description of the user-interface, where applicable ▎

2.   a detailed description of the elements of the AI System and of the process for its development, including:
    - 2.1.   the methods and steps performed for the development of the AI System, including, where relevant, recourse to pre-trained systems or tools provided by third parties and how these have been used, integrated or modified by the Supplier including a description of any licencing or other contractual arrangements related to such third-party inputs;
    - 2.2.   the design specifications of the system, namely the general logic of the AI System and of the algorithms; the key design choices including the rationale and assumptions made, also with regard to persons or groups of persons on which the system is intended to be used; the main classification choices; what the system is designed to optimise for and the relevance of the different parameters; the description of the expected output and output quality of the system; the decisions about any possible trade-off made regarding the technical solutions adopted to comply with the requirements set out in these MCC-AI-High-Risk;
    - 2.3.   the description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing; the computational resources used to develop, train, test and validate the AI System;
    - 2.4.   where relevant, the data requirements in terms of datasheets describing the training methodologies and techniques and the training data sets used, including a general description of these data sets, information about their provenance, scope and main characteristics; how the data was obtained

and selected; labelling procedures (e.g. for supervised learning), data cleaning methodologies (e.g. outliers detection);

2.5.   assessment of the human oversight measures needed in accordance with these MCC-AI-High-Risk, including an assessment of the technical measures needed to facilitate the interpretation of the outputs of AI systems by the Public Organisation, in accordance with these MCC-AI-High-Risk;

2.6.   where applicable, a detailed description of pre-determined changes to the AI System and its performance, together with all the relevant information related to the technical solutions adopted to ensure continuous compliance of the AI System with the relevant requirements set out in these MCC-AI-High-Risk;

2.7.   the validation and testing procedures used, including information about the validation and testing data used and their main characteristics; metrics used to measure accuracy, robustness and compliance with other relevant requirements set out in these MCC-AI-High-Risk as well as potentially discriminatory impacts; test logs and all test reports dated and signed by the responsible persons, including with regard to pre-determined changes as referred to under point 2.5;

2.8.   cybersecurity measures put in place.

3.   Detailed information about the monitoring, functioning and control of the AI System, in particular with regard to: its capabilities and limitations in performance, including the degrees of accuracy for specific persons or groups of persons on which the system is intended to be used and the overall expected level of accuracy in relation to its intended purpose; the foreseeable unintended outcomes and sources of risks to health and safety, fundamental rights and discrimination in view of the intended purpose of the AI System.

4.   A description of the appropriateness of the performance metrics for the AI System;

5.   A detailed description of the risk management system in accordance with article 2;

6.   A description of any relevant change made by the Supplier to the system through its lifecycle.

Annex D – Instructions for use

The instructions for use shall contain at least the following information, as applicable to the AI System:

1.   the identity and the contact details of the Supplier and, where applicable, of its authorised representatives;

2.   the characteristics, capabilities and limitations of performance of the AI System, including where appropriate:
   2.1.   the Intended Purpose;
   2.2.   the level of accuracy, including its metrics, robustness and cybersecurity referred to in article 8 against which the AI System has been tested and validated and which can be expected, and any clearly known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;
   2.3.   any known or foreseeable circumstance, related to the use of the AI System in accordance with the Intended Purpose or under conditions of Reasonably Foreseeable Misuse, which may lead to risks to the health and safety or fundamental rights;
   2.4.   where applicable, the technical capabilities and characteristics of the AI System to provide information that is relevant to explain its output;

   2.5.   when appropriate, its performance regarding specific persons or groups of persons on which the AI System is intended to be used;
   2.6.   when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI System;
   where applicable, information to enable the Public Organisation to interpret the output of the AI System and use it appropriately;

3.   the changes to the AI System and its performance which have been pre-determined by the Supplier, if any;

4.   the human oversight measures referred to in article 7, including the technical measures put in place to facilitate the interpretation of the outputs of the AI System by the Public Organisation;

5.   the computational and hardware resources needed, the expected lifetime of the AI System and any necessary maintenance and care measures, including their frequency, to ensure the proper functioning of that AI System, including as regards software updates;

6.   where relevant, a description of the mechanisms included within the AI System that allows the Public Organisation to properly collect, store and interpret the logs in accordance with article 5 of these MCC-AI-High-Risk.

Annex E – Measures to ensure transparency

Please provide here a description of the technical and organisational measures to be taken by the Supplier to ensure transparency in accordance with article 6 of the MCC-AI-High-Risk.

Annex F – Measures to ensure human oversight

Please provide here a description of the technical and organisational measures to be taken by the Supplier to ensure human oversight in accordance with article 7 of the MCC-AI-High-Risk.

Annex G – Levels of accuracy

21

Describe here the required levels of accuracy.

Annex H – Measures to ensure an appropriate level of robustness, safety and cybersecurity

Please provide here a description of the technical and organisational measures to be taken by the Supplier to ensure an appropriate level of robustness, safety and cybersecurity in accordance with article 8 of the MCC-AI-High-Risk.

These measures must ensure that the AI System shall be as resilient as possible regarding errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems.

The AI System shall be resilient as regards to attempts by unauthorised third parties to alter their use, behaviour, outputs or performance by exploiting the system's vulnerabilities. The technical solutions to address AI specific vulnerabilities may include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training dataset ('data poisoning'), or pre-trained components used in training ('model poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples' or 'model evasion'), confidentiality attacks or model flaws, which could lead to harmful decisionmaking.