Procurement of AI Community

PUBLIC BUYERS COMMUNITY

Proposal for standard contractual clauses for the procurement of Artificial Intelligence (AI) by public organisations

Version September 2023 (draft) – Non High Risk version

DISCLAIMER

This is a draft document for discussion purposes only to collect initial feedback from stakeholders. This document is developed by Jeroen Naves (Pels Rijcken). This is not an official EU document and it may not in any circumstances be regarded as reflecting an official position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this document. This document is still work-in-progress. No rights can be derived from this document.

Introductory remarks

These standard contractual clauses have been drafted for public organisations wishing to procure an AI System developed by an external supplier. These standard clauses are based on the standard clauses for the procurement of algorithmic systems developed by the City of Amsterdam in 2018 (https://www.amsterdam.nl/innovatie/digitalisering-technologie/algoritmen-ai/contractual-terms-for-algorithms/).

The standard contractual clauses presented are based to a large extent on the requirements and obligations for high-risk AI Systems included in the Title III of the proposal for a Regulation on artificial intelligence* ("AI Act"). This proposal is subject to ongoing negotiations so the clauses will need to be revised to take into account any changes made and fully align them with the final regulation adopted by the Council and the European Parliament.

Considering that the proposed AI Act is still under negotiations, public organisations that decide to use the standard contractual clauses may do that on a voluntary basis assessing on a case-by-case basis whether the various sections of these standard contractual clauses are sufficient and proportionate for procuring a particular AI System. The full version of the standard contractual clauses targets in particular AI systems classified as 'high-risk' within the meaning of Article 6 and listed in one of the areas covered by Annexes II and III of the proposed AI Act.

For non-high risk AI the application of these requirements is not mandatory under the AI Act, but recommended to improve trustworthiness of AI applications procured by public organisations. This light version of the standard contractual clauses targets in particular non-high risk AI systems.

Where appropriate and justified depending on the impact of the system on the individuals and the society, public organisations may also extend the application of these clauses, either the full version or this light version, to other algorithmic systems that may not be necessarily qualified as 'AI' to cover in addition simpler software rule-based systems, considering that their use in the public sector may also require in certain cases increased accountability, control and transparency.

The standard contractual clauses only contain provisions specific to AI Systems and on matters covered by the proposed AI Act, thus excluding other obligations or requirements that may arise under relevant applicable legislation such as the General Data Protection Regulation. Furthermore, these standard contractual clauses do not comprise a full contractual arrangement. For example, these standard contractual clauses do not contain any conditions concerning intellectual property, acceptance, payment, delivery times, applicable law or liability. The standard contractual clauses are drafted in such a way that they can be attached as a schedule to an agreement in which such matters have already been laid down.

* Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain union legislative acts, COM(2021)206 final.

Section A – Definitions

Article 1 Definitions

1.1. Capitalised terms used in these Clauses will have the meaning as defined in this article.

- Agreement: the entire agreement of which the Clauses, as a schedule, are an integral part;
- AI System: the AI system(s) as referred to in **Annex A**, including any new versions thereof;
- Clauses: these standard contractual clauses for the procurement of artificial intelligence 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;
- Substantial Modification: a change to the AI System following the Delivery which affects the compliance of the AI System with the requirements set out in these Clauses or results in a modification to the Intended Purpose;
- 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 and implemented 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 to health, safety and fundamental rights of the European Union that are likely to arise in the light of the Intended Purpose of the AI System and Reasonably Foreseeable Misuse;
   b. evaluation of other possibly arising risks;
   c. adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to points a and b of this paragraph in accordance with the provisions of the following paragraphs.

2.3. The risk management measures referred to in paragraph 2.2, point (c) shall be such that relevant residual risks associated with each hazard as well as the overall residual risk of the AI system is reasonably 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.

2.4. In identifying the most appropriate risk management measures referred to in paragraph 2.2, point (c), the following shall be ensured:
   a. elimination or reduction of identified risks as far as technically feasible through adequate design and development of the AI System;
   b. where appropriate, implementation of adequate mitigation and control measures in relation to risks that cannot be eliminated;
   c. provision of adequate information to the Public Organisation.

2.5. The Supplier ensures that, prior to the Delivery of the AI System, the AI System is tested in order to verify whether the AI System complies with the Clauses and whether the risk management measures referred to in paragraph 2.2, point (c) 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.

2.6. 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.

2.7. The risk management system shall consist of a continuous and iterative process 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 2.6 up to date; and
   c. make every new version of the documentation described in article 2.6 available to the Public Organisation without delay.

2.8. 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.

2.9. **<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, has been and shall be subject to data governance appropriate for the context of use as well as the Intended Purpose of the AI System. Those measures shall concern in particular:

a. transparency as regard the original purpose of data collection;
b. the relevant design choices;
c. data collection processes;
d. data preparation for processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;
e. the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;
f. examination in view of possible biases that are likely to affect health and safety of natural persons or lead to discrimination prohibited by the laws of the European Union;
g. appropriate measures to detect, prevent and mitigate possible biases;
h. the identification of relevant data gaps or shortcomings that prevent compliance with these Clauses, 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, representative, and to the best extent possible free of errors and be as complete as possible 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 on which 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 take into account, 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 Clauses 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 10.

Article 5 Record-keeping

5.1. The Supplier ensures that the AI System has been and shall be designed and developed with capabilities enabling the automatic recording of events ('logs') while the AI System is operating. Those logging capabilities shall conform to state of the art and, if available, recognised standards or common specifications. **<Optional: add, if available, a specific standard>**
5.2. The logging capabilities shall ensure a level of traceability of the AI System's functioning throughout its lifecycle 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 reasonably understand the system's functioning.

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. These measures should result in the Public Organisation being able to understand and use the AI System appropriately by understanding how the AI System works and what data it processes, allowing the Public Organisation to explain the decisions taken by the AI System to the persons or group of persons on which the AI System is (intended to be) used.

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 as proportionate to the risks associated with the system.

7.2. 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, which could include inter alia training of employees of the Public Organisation, shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances:

a. be aware of and sufficiently understand the relevant capacities and limitations of the AI System and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible;

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

d. be able 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. be able to intervene on the operation of the AI System or interrupt the system through a "stop" button or a similar procedure.

7.3. **<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 following the principle of security by design and by default. In the light of the Intended Purpose, it should achieve an appropriate level of accuracy, robustness, safety and cybersecurity, and perform consistently in those respects throughout the lifecycle of the AI System.

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

8.3. In order 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.

Article 9 Compliance

9.1. 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 these Clauses.

9.2. At first request of Public Organisation, the Suppliers must make available to Public Organisation all information necessary to demonstrate compliance with these Clauses.

9.3. 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 Clauses, 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 10 Obligation to explain the functioning of the AI System on an individual level

10.1. In addition to the obligations described in article 6, during the term of the Agreement the Supplier is obliged to assist the Public Organisation at the Public Organisation's first request to explain how the AI System arrived at a particular decision or outcome to the persons or group of persons on which the AI System is (intended to be) used. At the minimum, this assistance will include a clear indication of the key factors that led the AI System to arrive at a particular result and the changes to the input that must be made in order for it to arrive at a different outcome.

10.2. The obligation as described in article 10.1 comprises the provision to the Public Organisation of all the technical and other information required in order to explain how the AI System arrived at a particular decision or outcome and to offer the persons or group of persons on which the AI System is (intended to be) used the opportunity to verify the way in which the AI System arrived at a particular decision or outcome. 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 persons or group of persons on which the AI System is (intended to be) used about the functioning of the AI System and/or in any legal proceedings.

10.3. **<optional>** The obligations referred to in article 10.1 and article 10.2 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 C – Rights to use the Data Sets

Article 11 Rights to Public Organisation Data Sets

11.1. 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.
11.2. 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.
11.3. 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 12 Rights to Supplier Data Sets and Third Party Data Sets

12.1. 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.
12.2. 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 Clauses, except as otherwise provided in Annex B.
12.3. **<optional>** The right of use described in article 12.2 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 13 Hand over of the Data Sets

13.1. On first request of the Public Organisation, the Supplier will hand over the most recent version of Public Organisation Data Sets to the Public Organisation.
13.2. On first request of the Public Organisation, the Supplier will hand over 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.
13.3. 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. **<option**al**> The Data Sets will be returned as follows: [file format]**

Annex A – The AI System and the Intended Purpose

Description of the AI System

Within the scope of these clauses 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**[1]
		Yes/No
		Yes/No
		Yes/No
		Yes/No

[1] 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 10.

Annex C – Technical documentation

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

1. a general description of the AI System including:
   - 1.1. its intended purpose, the name of the Supplier, the date and the version of the system;
   - 1.2. the nature of data likely or intended to be processed by the system and, in the case of personal data, the categories of natural persons and groups likely or intended to be affected;
   - 1.3. how the AI System can interact or can be used to interact with hardware or software that is not part of the AI System itself, where applicable;
   - 1.4. the versions of relevant software or firmware and any requirement related to version update;
   - 1.5. the description of all forms in which the AI System is placed on the market or put into service;
   - 1.6. the description of hardware on which the AI System is intended to run;
   - 1.7. where the AI System is a component of products, photographs or illustrations showing external features, marking and internal layout of those products;
   - 1.8. a detailed and easily intellegible description of the system's main optimisation goal or goals;
   - 1.9. a detailed and easily intellegible description of the system's expected output and expected output quality;
   - 1.10. detailed and easily intellegible instructions for interpreting the system's output;
   - 1.11. examples of scenarios for which the system should not be used.

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 decisions about any possible trade-off made regarding the technical solutions adopted to comply with the requirements set out in these Clauses;
   - 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 information about the provenance of those data sets, their 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. 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 Clauses;

2.6. 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, cybersecurity and compliance with other relevant requirements set out in these Clauses 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;

2.7. cybersecurity measures put in place.

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.

3. a detailed description of the risk management system in accordance with article 2;

4. 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, 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 clearly 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. the degree to which the AI System can provide an explanation for decisions it takes;
   - 2.5. its performance as regards the persons or groups of persons on which the AI System is intended to be used;
   - 2.6. relevant information about user actions that may influence system performance, including type or quality of 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.

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 expected lifetime of the AI System and any necessary maintenance and care measures to ensure the proper functioning of that AI System, including as regards software updates;

6. a description of the mechanisms included within the AI System that allows users to properly collect, store and interpret the logs.

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 Clauses.

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 Clauses.

Annex G – Levels of accuracy

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 Clauses.

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.