06.2026 Clauses on Article 25(4) AIA

Annex - Policy Prototypes

The EU AI Act's value chain requirement

Kenniscentrum Data & Maatschappij

Artificiële Intelligentie Vlaanderen

Overview

1

Prototype 1

Use case 1 - Chatbot insurance industry

Use case 1 - Chatbot insurance industry

1.1 Description

The first use case involves a company that offers various types of AI systems to insurance companies. The company aims to deploy an AI-powered chatbot consisting of a risk-assessment tool for customers of insurance companies to apply for life insurance to pay off their mortgage. The tool uses fully automated decision-making, whereby applications can be accepted or rejected via the system. The risk assessment consists of various elements that are provided by the customer, such as their age, salary, health, and whether they are taking out the insurance alone or with another person. The company licenses the chatbot from a third-party supplier for the core of the AI model as well as the software platform. The tool is categorised as a high-risk AI system under Annex III of the AI Act.

The workshop participants decided to design a clause that focuses on the following aspects: the licence granted by the supplier, the back-end access and technical cooperation, and the protection of intellectual property, trade secrets and data as well as confidentiality.

Overview of the prototype

1.2 Clause on the technical access and use of the AI system

1.2.1 Licence granted by the supplier

1.2.1.1 The Supplier grants to the Provider an **exclusive, non-transferable and sublicensable license** to use the Supplier's AI System, as described in Annex 1, solely for the purpose of integrating, deploying and operating the Provider's AI system in accordance with the Intended Use.

For the purpose of this agreement, "Intended Use" means the deployment of the AI System for the autonomous assessment of the conditions under which natural persons can be granted a life insurance in compliance with applicable law. For the avoidance of doubt, "Intended Use" shall not include using the AI System in a way that is considered to be prohibited under applicable law.

1.2.1.2 The licence is limited to the **Intended Use** of the AI model and does not include any right to:

→ copy, reproduce or distribute the AI model as a standalone product,

→ (modify, retrain, fine-tune or adapt the AI model,)

→ reverse engineer, decompile or otherwise attempt to derive the source code, model architecture, weights or training data, except insofar as strictly required by law.

1.2.2
Back end access and technical cooperation

1.2.2.1 Where necessary for the Provider to comply with applicable law, the Supplier shall provide **limited, controlled and proportionate technical access** to the back-end of the AI System to the Provider, as specified in Annex 2. For this purpose, Supplier shall provide appropriate technical documentation to the Provider.

1.2.2.2 Such access shall:

→ be restricted to clearly defined interfaces, APIs or environments,

→ exclude direct access to source code, model weights and training datasets unless expressly agreed in writing,

→ be subject to appropriate security, authentication, logging and monitoring measures.

1.2.2.3 The Provider shall use any back-end access solely to:
→ (integrate and operate the AI model within the Provider's AI system)

→ perform testing, validation and monitoring activities strictly necessary for compliance with applicable law,

→ meet applicable transparency, risk management or conformity requirements.

1.2.2.4 The Provider shall not use the back-end access to extract, infer or replicate the Supplier's trade secrets or proprietary know-how, nor to access data beyond the scope defined in this Agreement.

1.2.3
Protection of intellectual property, trade secrets and data

1.2.3.1 Each Party retains all rights in its **background intellectual property, proprietary data and trade secrets**.

1.2.3.2 Any technical information, documentation, logs or outputs shared under this Agreement shall remain the confidential information of the disclosing Party,

1.2.3.3 Where the Supplier's AI System processes data provided by or on behalf of the Provider, such data shall remain the property of the Provider or the relevant data owner, and shall not be used by the Supplier for training or improving the AI model unless expressly agreed.

1.2.4
Confidentiality

1.2.4.1 Each Party shall keep strictly confidential all non-public information received from the other Party in connection with the AI System, the back-end access, including technical, commercial and security-related information.

1.2.4.2 Confidential information may be disclosed only:

→ to its staff on a strictly need-to-know basis and subject to confidentiality obligations which are at least as stringent,

→ to the Provider's End Users insofar as strictly required for such End User to perform human oversight and monitoring as required by applicable law, and insofar as such End User is bound by confidentiality obligations which are at least as stringent,

→ where disclosure is required by law or a competent authority, subject to prior notice where legally permitted, and strictly limited to the information required to be disclosed for this purpose.

1.2.4.3 Confidentiality obligations shall survive termination of this Agreement for as long as the information remains confidential.

2

Prototype 2

Use case 2 – Medical device software

Use case 2 - Medical device software

2.1 Description

[1] *Practical note: the design workshop for this specific use case involved three people, two of whom took turns participating, meaning that one of them missed the first part and the other the last part.*

The second use case relates to the development of medical device software that (i) assists physicians in prescribing the appropriate dosage of antibiotics, and (ii) predicts and stays ahead of emerging antibiotics resistance to improve the treatment and prevention of serious infections. Drug-resistant infections are a growing global problem and many believe that superbugs can be defeated by supercomputers. In this regard, the provider and third-party supplier are entering into a partnership in order to achieve the previously mentioned targets. The third-party supplier provides the following to the provider: (i) specific AI models (including the algorithms for decision-making) and (ii) the hardware (GPUs/TPUs) for processing. The AI system is categorised as a high-risk AI system under Annex I of the AI Act.

The participants drafted a clause in which they focused primarily on data governance aspects, given the great importance of reliable data in the medical sector.[1]

Overview of the prototype

2.2 Clause on governance

2.2.1 Scope

Novalyte Therapeutics (hereafter 'Client') shall contract Microsafe (hereafter 'Supplier') to deliver CARP, AI-powered software, that will be developed for the Intended purpose as indicated in Annex A.

2.2.2 Data availability

Client shall make the Data sets available to the Supplier. Supplier shall process the Data sets in line with the data processing agreement.

2.2.3 Data governance

Supplier shall ensure 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. These measures shall concern in particular:

→ Relevant design choices

→ Data collection processed and the origin of data, and in the case of personal data, the original purpose of the data collection

→ Relevant data preparation for processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation

→ The formulation of assumptions, with respect to the information that the data are supposed to measure and represent

[2] *This section was not developed further by the workshop participants.*

- → An assessment of the on the availability, quantity and suitability of the data sets that are needed
- → 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
- → Appropriate measures to detect, prevent and mitigate possible biases identified
- → The identification of relevant data gaps of shortcomings that prevent compliance, and how those gaps and shortcoming can be addressed

The use of Data Sets, originating from other or public sources, will have to be notified and agreed upon by the Client.

The Supplier checks 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 in view of the Intended purpose. Where this can not be ensured the Supplier inform the Client for corrective or mitigating measures.

2.2.4
Data management and record keeping

Periodic evaluation and review
On a yearly basis the Client and Supplier shall evaluate the performance of the software, including post-market feedback and reported incidents, and review where necessary the intended purpose, development or implementation of the CARP software package. Changes necessary will be performed by the Supplier within the first 4 years of the Contract at predefined cost.

2.2.5
Annex A

Intended purpose:
The intended purpose of CARP, AI-powered software, is to

- → Assist physicians in prescribing the appropriate dosage of antibiotics
- → Predict and stay ahead of emerging antibiotics resistance to improve the treatment and prevention of serious infections

3

Prototype 3

Use case 3 – AI system for the ranking and screening of CVs

Use case 3 – AI system for the ranking and screening of CVs

3.1 Description

The AI system in this use case supports recruitment decisions by ranking and screening candidates on the basis of CV data and other inputs. The system is positioned by its provider as a decision-support tool, but in practice it produces outputs that materially influence whether a candidate is invited to interview or hired. The AI system can be categorised as a high-risk AI system under Annex III.

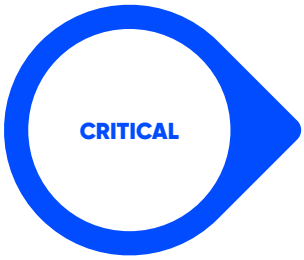
The prototype document developed for this use case focuses on incident handling between the parties (i.e. provider and third-party supplier) to the contract. It is structured in three layers: a high-level colour-coded overview, a light version covering the core obligations, and a full version that elaborates a points-based criticality classification. The full version distinguishes between low, medium, high and critical incidents, and sets out the cooperation expected between the parties at each level.[3]

[3] *Practical note: The choice for incident handling in particular was made during the design workshop by the participants. The main reason for said choice was that this was a matter that the participants agreed was feasible to complete in one day, being aware of the limitation that covering all supply-chain-related aspects would not be feasible in one day for the given use case.*

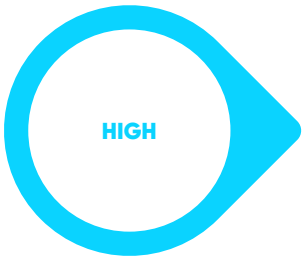
Overview of the prototype

3.2

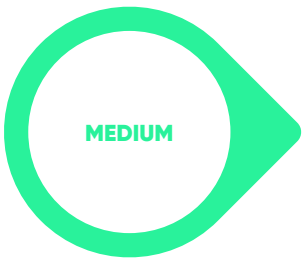
Clause on incident handling



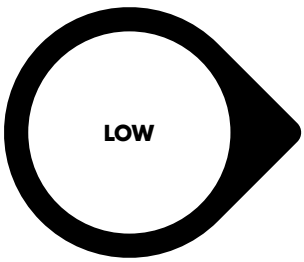
Immediate disclosure +
immediate solution



Immediate disclosure +
fast solution



Disclosure + solution
Normal timeframes (SLA)



Internal logging + solution
Normal timeframes (SLA)

3.2.1
Light version: one-pager - checklist

The purpose of the illustration is to have an instrument for classifying incidents into one of the 4 categories.

The four categories are explained below. In **blue** a number of points is added following the below elements, with also the consequences of each element. The participants also discussed that general descriptions are desirable to overwrite the point system based on common sense.

1. **Low** (1-8) → Internal logging and solution required.
   General description: No real impact on fundamental rights, health or safety.

2. **Medium** (9-14) → Disclosure solution required within normal timeframes (see SLA).
   General description: Incident with limited impact on fundamental rights, health or safety.

3. **High** (15-19) → Immediate disclosure required and fast solution required.
   General description: Incident with high impact on fundamental rights, health or safety.

4. **Critical** (20-...) → Immediate disclosure required and immediate solution necessary.
   General description: Incident with severe impact on fundamental rights, health or safety.

Always critical

→ Can the incident be classified as a serious incident under article 3(49) AIA?
→ Critical

  → "(49) 'serious incident' means an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:
  (a) the death of a person, or serious harm to a person's health;
  (b) a serious and irreversible disruption of the management or operation of critical infrastructure;
  (c) the infringement of obligations under Union law intended to protect fundamental rights;
  (d) serious harm to property or the environment."

→ Does the incident concern a prohibited AI practice under article 5 of the AI Act? → Critical

Risk level

→ Does the incident concern an AI-system that does not fall under one of the risk categories of the AI Act? → + 1

→ Does the incident concern a limited risk AI system under article 50 of the AI Act? (E.g., failure to label that content was AI-generated) → + 2

→ Does the incident concern a high risk AI system under article 6(1) or 6(2) of the AI Act? → + 3

Note participants: These numbers are arbitrary. In reality, this would probably need to be substantiated.

Type of data

→ Are personal data involved? → + 1

→ Are special categories of data involved? → + 2

→ Are vulnerable individuals involved (e.g., minors)? → + 3

Location

→ Is the incident limited to one location? → + 1

→ Is the incident limited to locations in one member state? → + 2

→ Is the incident limited to locations in multiple member states? → + 3

Number of impacted individuals[4]

→ Does the incident affect 100 individuals or less? → + 1

→ Does the incident affect between 100-1.000 individuals? → + 2

→ Does the incident affect 1.000 individuals or more? → + 3

Impact

→ Is the incident easily reversible? → + 1

→ Is the incident hard to reverse? → + 2

→ Is the incident irreversible? → + 3

Human oversight

→ Is the incident caused by an simple human error? → + 1

→ Was the human not able to intervene because of a technical error? → + 2

→ Was the human able to intervene but overruled by the AI-system? → + 3

Additional elements

→ Is there a reporting obligation under another law? → + 2

→ Does the incident lead to an infringement of labour law? → + 3

3.2.2
Two examples of how to use the checklist

Example 1
Employed AI tool displays a bias and led to a wrong hiring / dismissal decision (internal or external cause) in one entity of the company.

Possible trigger of the serious incident classification ("the infringement of obligations under Union law intended to protect fundamental rights") → **critical incident**

If this classification is not triggered, this would be the result of the point system:

→ Risk level → + 3

→ Type of data → + 1

→ Location → + 1

→ Number of impacted individuals → + 1

→ Impact → + 2

→ Human oversight → + 3

→ Additional elements → + 3 + 2

→ TOTAL → + 16 = incident level = high

Example 2
Employed AI tool for HR purposes made a mistake but was corrected by human oversight.

→ Risk level → + 3

→ Type of data → + 1

→ Location → + 1

→ Number of impacted individuals → + 1

→ Impact → + 1

→ Human oversight → + 1

→ Additional elements → + 0

→ TOTAL → + 8 = incident level = low

Citation

Sultan Erdogan, Shannen Verlee, Frederic Heymans and Koen Vranckaert (Knowledge Centre Data & Society), “From Policy To Practice: Prototyping the EU AI Act’s value chain requirement”, July 2026.

Contact
sultan.erdogan@kuleuven.be and frederic.heymans@vub.be.

data-en-maatschappij.ai/en/ →

Kenniscentrum Data & Maatschappij

Artificiële Intelligentie Vlaanderen