Contribution ID: 518fd485-5bdd-4cf8-a4e3-21eefa71f182
Date: 18/07/2025 17:16:37

Targeted stakeholder consultation on classification of AI systems as high-risk

Fields marked with * are mandatory.

Targeted stakeholder consultation on the implementation of the AI Act's rules for high-risk AI systems

Disclaimer: This document is a working document of the AI Office for the purpose of consultation and does not prejudge the final decision that the Commission may take on the final guidelines. The responses to this consultation paper will provide important input to the Commission when preparing the guidelines.

This consultation is targeted to stakeholders of different categories. These categories include, but are not limited to, providers and deployers of (high-risk) AI systems, other industry organisations, as well as academia, other independent experts, civil society organisations, and public authorities.

The Artificial Intelligence Act (the 'AI Act')[1], which entered into force on 1 August 2024, creates a single market and harmonised rules for trustworthy and human-centric Artificial Intelligence (AI) in the EU.[2] It aims to promote innovation and uptake of AI, while ensuring a high level of protection of health, safety and fundamental rights, including democracy and the rule of law. The AI Act follows a risk-based approach classifying AI systems into different risk categories, one of which is the high-risk AI systems (Chapter III of the AI Act). The relevant obligations for those systems will be applicable two years after the entry into force of the AI Act, as from 2 August 2026.

The AI Act distinguishes between two categories of AI systems that are considered as 'high-risk' set out in Article 6(1) and 6(2) AI Act. Article 6(1) AI Act covers AI systems that are embedded as safety components in products or that themselves are products covered by Union legislation in Annex I, which could have an adverse impact on health and safety of persons. Article 6(2) AI Act covers AI systems that in view of their intended purpose are considered to pose a significant risk to health, safety or fundamental rights. The AI Act lists eight areas in which AI systems could pose such significant risk to health, safety or fundamental rights in Annex III and, within each area, lists specific use-cases that are to be classified as high-risk. Article 6(3) AI Act provides for exemptions for AI systems that are intended to be used for one of the cases listed in Annex III, but which do not pose significant risk since they fall under one of the exceptions listed in Article 6(3).

AI systems that classify as high-risk must be developed and designed to meet the requirements set out in Chapter III Section 2, in relation to data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security. Providers of high-risk AI systems must ensure that their high-risk AI system is compliant with these requirements and must themselves comply with a number of obligations set out in Chapter III Section 3, notably the obligation to put in place a quality management system and ensure that the high-risk AI system undergoes a conformity assessment prior to its being placed on the market or put into service. The AI Act also sets out obligations for deployers of high-risk AI systems, related to the correct use, human oversight, monitoring the operation of the high-risk AI system and, in certain cases, to transparency vis-à-vis affected persons.

Pursuant to Article 6(5) AI Act, the Commission is required to provide guidelines specifying the practical implementation of Article 6, which sets out the rules for high-risk classification, by 2 February 2026. It is further required that these guidelines should be accompanied with a comprehensive list of practical examples of use cases of AI systems that are high-risk and not high-risk. Moreover, pursuant to Article 96(1)(a) AI Act, the Commission is required to develop guidelines on the practical application of the requirements for high-risk AI systems and obligation for operators, including the responsibilities along the AI value chain set out in Article 25.

The purpose of the present targeted stakeholder consultation is to collect input from stakeholders on practical examples of AI systems and issues to be clarified in the Commission's **guidelines** on the classification of high-risk AI systems and future guidelines on high-risk requirements and obligations, as well as responsibilities along the AI value chain.

As not all questions may be relevant for all stakeholders, respondents may reply only to the section(s) and the questions they would like. Respondents are encouraged to provide **explanations and practical cases** as a part of their responses to support the practical usefulness of the guidelines.

The targeted consultation is available in English only and will be open for **6 weeks starting on 6 June until 18 July 2025.**

The questionnaire for this consultation is structured along 5 sections with several questions.

Regarding section 1 and 2, respondents will be asked to provide answers pursuant to the parts of the survey they expressed interest for in Question 13, whereas all participants are kindly asked to provide input for section 3, 4 and 5.
Section 1. Questions in relation to the classification rules of high-risk AI systems in Article 6(1) and the Annex I to the AI Act

- This section includes questions on the concept of a safety component and on each product category listed in Annex I of the AI Act.

Section 2. Questions in relation to the classification of high-risk AI systems in Article 6(2) and the Annex III of the AI Act. This category includes questions related to:

- AI systems in each use case under the 8 areas referred to in Annex III.
- The filter mechanism of Article 6(3) AI Act allowing to exempt certain AI systems from being classified as high-risk under certain conditions.
- If pertinent: Need for clarification of the distinction between the classification as a high-risk AI system and AI practices that are prohibited under Article 5 AI Act (and further specified in the Commission's guidelines on prohibited AI practices[3] from 3 February 2025) and interplay of the classification with other Union legislation.

Section 3. General questions for high-risk classification. This category includes questions related to:

- The notion of intended purpose, including its interplay with general purpose AI systems.
- Cases of potential overlaps within the AI Act classification system under Annex I and III.

Section 4. Questions in relation to requirements and obligations for high-risk AI systems and value chain obligations. This category includes questions related to:

- the requirements for high-risk AI systems and obligations of providers.
- the obligations of deployers of high-risk AI systems.
- the concept of substantial modification and the value chain obligations in Article 25 AI Act.

Section 5. Questions in relation to the need for amendment of the list of high-risk use cases in Annex III and of prohibited AI practices laid down in Article 5.

- Input for the mandatory annual assessment of the need for amendment of the list of high-risk use-cases set out in Annex III
- Input for the mandatory annual assessment of the list of prohibited AI practices laid down in Article 5

All contributions to this consultation may be made publicly available. Therefore, please do not share any confidential information in your contribution. Individuals can request to have their contribution anonymised. Personal data will be anonymised.

The AI Office will publish a summary of the results of the consultation. Results will be based on aggregated data and respondents will not be directly quoted.

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

[2] Article 1(1) AI Act.

[3]https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act.

Information about the respondent

* First name

Charles

* Surname

LOW

* Email address

clow@accis.eu

* Do you represent an organisation (e.g., think tank or civil society/consumer organisation) or act in your personal capacity (e.g., independent expert or from a downstream provider)?

- (●) Organisation
- ( ) In a personal capacity

* Name of the organisation

Association of Consumer Credit Information Suppliers (ACCIS)

* Type of organisation

Association

* Is a representation of the organisation located in the EU?

- (●) The organisation's headquarter is located in the EU
- ( ) A branch office, or any representation of the organisation is located in the EU
- ( ) None of the representations of the organisation is located in the EU

* Select the EU member state where the organisation's headquarter, or representation is located

BE - Belgium

* Select the size of the organisation

Micro (0-9 employees)

* Sector(s) of activity

- [x] Information technology
- [ ] Employment
- [ ] Transport

- [ ] Public administration
- [ ] Education and training
- [ ] Telecommunications
- [ ] Law enforcement
- [x] Consumer services
- [ ] Retail
- [ ] Justice sector
- [x] Business services
- [ ] E-commerce
- [ ] Legal services sector
- [x] Banking and finances
- [ ] Advertising
- [ ] Cultural and creative sector, including media
- [ ] Manufacturing
- [ ] Consumer protection
- [ ] Healthcare
- [ ] Energy
- [ ] Others

* Describe the activities of your organisation or yourself

1300 character(s) maximum

ACCIS is the voice of organisations responsibly managing data to assess the financial credibility of consumers and businesses. Established as an association in 1990, ACCIS brings together more than 40 members from countries all over Europe as well as associates and affiliates across the globe. ACCIS is active in representing consumer credit information suppliers at EU-level on topics that touch upon credit information, ranging from GDPR to Artificial Intelligence, Financial Data-Sharing, and so on. I am the Chief Policy Officer of the organisation, so I am responsible for gathering views, input and data that can allow ACCIS to contribute positively to ongoing dialogue at EU-level.

---

* All contributions to this consultation may be made publicly available. Therefore, please do not share any confidential information in your contribution. Your e-mail address will never be published. Should your contribution be anonymised in the instance that all contributions are made publicly available?

If you act in your personal capacity: *All contributions to this consultation may be made publicly available. You can choose whether you would like your details to be made public or to remain anonymous. The type of respondent that you responded to this consultation as, your answer regarding residence, and your contribution may be published as received. Your name will not be published. Please do not include any personal data in the contribution itself.*

If you represent one or more organisations: *All contributions to this consultation may be made publicly available. You can choose whether you would like respondent details to be made public or to remain anonymous. Only organisation details may be published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its size, its presence in or outside the EU and your contribution may be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.*

- ( ) Yes, please anonymise my contribution.
- (•) No

* Do you agree that we may contact you in the event of follow-up questions or if we want to learn more about your responses?

- (•) Yes
- ( ) No

- [x] I acknowledge the attached privacy statement.

Privacy_statement_high_risks.pdf

---

* **On which part(s) of the public consultation are you interested to contribute to?** *Multiple answers are possible. Please note that selecting a particular answer will direct you to a set of questions specifically related to subject specified.*

- ☐ Questions in relation to **Annex I of the AI Act.** (Section 1)
- ☑ Questions in relation to **Annex III of the AI Act.** (Section 2)
- ☑ Questions on **horizontal aspects** of the high-risk classification. (Section 3)
- ☑ Questions in relation to **requirements and obligations for high-risk AI systems and value chain obligations**. (Section 4)
- ☑ Questions in relation to the **need for possible amendments of high-risk use cases in Annex III and of prohibited practices in Article 5**. (Section 5)

Section 2. Questions in relation to the classification rules of high-risk AI systems in Article 6(2) and (3) AI Act and Annex III to the AI Act

AI systems classified as high-risk by Article 6(2) AI Act are AI systems which pose a significant risk of harm to the health, safety or fundamental rights of natural persons, and which are intended to be used for specific use cases as explicitly specified in Annex III under each area (cf. Annex III):

- *Biometrics.*
- *Critical infrastructure.*
- *Education and vocational training.*
- *Employment, workers' management and access to self-employment.*
- *Access to and enjoyment of essential private services and essential public services and benefits.*
- *Law enforcement.*
- *Migration, asylum and border control management.*
- *Administration of justice and democratic processes.*

However, in certain cases the use of an AI system does not risk leading to a significant risk of harm to the health, safety or fundamental rights of natural persons, for example by not materially influencing the outcome of decision making. Therefore, even if the AI systems may be referred to in Annex III, paragraph 3 of article 6 AI Act envisages situations when such AI systems would not be classified as high-risk if 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, this exception cannot be applied if the AI system performs profiling of natural persons.
A provider who considers that an AI system referred to in Annex III falls within one or more of the exceptions should document its assessment before that system is placed on the market or put into service and register it according to Article 49(2).

Questions in relation to **Annex III of the AI Act**. *Multiple answers are possible*

- [x] Biometrics
- [ ] Critical infrastructure
- [ ] Education and vocational training
- [ ] Employment, workers' management and access to self-employment
- [x] Access to and enjoyment of essential private services and essential public services and benefits
- [ ] Law enforcement
- [ ] Migration, asylum and border control management
- [ ] Administration of justice and democratic processes

2.A. Questions in relation to biometrics (Annex III, point 1)

The concepts of real-time remote biometric identification at publicly accessible places for law enforcement purposes, biometric categorisation and of emotion recognition are explained in the Guidelines on prohibited AI practices. The feedback given in this consultation should therefore be ***strictly limited to the use of such systems that are not prohibited*** *pursuant to Article 5 AI Act or to questions regarding the delimitation between the prohibited use of such AI systems or their classification as high-risk.*

Point 1 of Annex III to the AI Act distinguishes between three different types of biometrics use cases that are classified as high-risk. All three of them are based on biometric data, i.e. personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics, like the shape of the face, voice or gait:

- *Point 1(a) of Annex III to the AI Act refers to the use of remote biometric identification systems. These systems aim at the remote (at a distance, without the active participation of the person in question) automated recognition of a natural person, for the purpose of establishing the identity of that person, by comparing the biometric data of that individual to biometric data of individuals stored in a database. Verification and authentication, used for the confirmation of the identity of a natural person, are not considered to be high-ris AI systems performing biometric categorisation may fall under the scope of prohibited systems if they fulfil the cumulative conditions defined in Article 5(1)(g) AI Act which are further developed in Section 8 of the Commission Guidelines on prohibited AI practices.*

- *Point 1(b) of Annex III to the AI Act refers to the use of biometric categorisation AI systems that are categorising natural persons according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics, unless the categorisation is ancillary to another commercial service and strictly necessary for objective technical reasons (Article 3(40) AI Act). According to recital 54, AI systems intended to be used for biometric categorisation according to sensitive attributes or characteristics are those attributes and characteristics protected under Article 9 (1) of Regulation (EU) 2016/679. AI systems performing biometric categorisation may fall under the scope of prohibited systems if they fulfil the cumulative conditions defined in Article 5(1)(g) which are further developed in Section 8 of the Commission Guidelines on prohibited AI practices.*

- *Point 1(c) of Annex III to the AI Act refers to the use of emotion recognition systems. These are AI systems for identifying or inferring emotions or intentions of natural persons on the basis of their biometric data. As clarified in recital 18 AI Act, emotion recognition includes for example emotions such as happiness, sadness, or anger. It explicitly excludes the recognition of physical states such as pain or fatigue. AI systems intended to perform emotion recognition may fall under the scope of prohibited systems if they fulfil conditions defined in Article 5(1)(f) AI Act, which are further developed in Section 7 of the Commission Guidelines on prohibited AI practices.*

Question 7. Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems related to biometrics.

Examples may include systems for which you have uncertainties or system that you consider should not be considered high-risk as they are outside the use cases listed in Annex III or they fulfil one or more of the conditions for the exceptions in Article 6(3) AI Act.

	Name and description of the system	Category of biometric system	The system is considered high-risk	Motivate your previous answer	The AI system performs profiling of natural person	The AI system meets at least one of the exception criteria of Article 6(3)	Motivate your previous answer and specify any exception criteria that it meets, if applicable
1	*Name/description* Remote biometric 'KYC' verification service: AI compares a live selfie or video with an official identity document, performs liveness and deep-fake checks, and automatically extracts ID-document data, so that the deployer can confirm that the applicant is the person he or she claims to be before concluding a contract (eg to open an account or grant other financial services).	*Category* Remote biometric identification (Point 1 (a))	*High-risk* No	*Explain* Annex III(1)(a) designates remote biometric identification systems as high risk but explicitly carves out 'AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be'. Consequently, the KYC verifier is outside the high risk category.	*Profiling* No	*Exception* No	*Explain* The carve-out inside Annex III(1)(a) already removes the system from the high-risk category.
2	*Name/description*	*Category* ○ Remote biometric identification (Point 1 (a)) ○ Biometric categorisation (Point 1(b)) ○ Emotion recognition (Point 1(c))	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*
3	*Name/description*	*Category* ○ Remote biometric identification (Point 1 (a)) ○ Biometric categorisation (Point 1(b)) ○	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*

		Emotion recognition (Point 1(c))					
4	*Name/description*	*Category* Remote biometric identification (Point 1 (a)) Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*
5	*Name/description*	*Category* Remote biometric identification (Point 1 (a)) Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*
6	*Name/description*	*Category* Remote biometric identification (Point 1 (a)) Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*
		Category					

7	*Name/description*	Remote biometric identification (Point 1 (a)) Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*
8	*Name/description*	*Category* Remote biometric identification (Point 1 (a)) Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*
9	*Name/description*	*Category* Remote biometric identification (Point 1 (a)) Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*
		Category Remote biometric identification (Point 1 (a))	*High-risk* Yes, completely		*Profiling*	*Exception*	

10	*Name/description*	Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	Partially No Unsure	*Explain*	Yes No Unsure	Yes No Unsure	*Explain*

Question 8. Do you have or know practical examples of AI systems related to biometrics where you need further clarification regarding the **distinction from prohibited AI systems**?

	Name and description of the system	Category of biometric system	Category of prohibited AI system with which there may be an interplay	Motivate your previous answer
1	*Name/description*	*Category* Remote biometric identification (Point 1(a)) Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	*Category* Real time remote biometric identification system (Art. 5(1)(h)) Biometric categorisation system (Art. 5(1)(g)) Emotion inference system (Art. 5(1)(f)) Other Unsure	*Explain*
2	*Name/description*	*Category* Remote biometric identification (Point 1(a)) Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	*Category* Real time remote biometric identification system (Art. 5(1)(h)) Biometric categorisation system (Art. 5(1)(g)) Emotion inference system (Art. 5(1)(f)) Other Unsure	*Explain*
3	*Name/description*	*Category* Remote biometric identification (Point 1(a)) Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	*Category* Real time remote biometric identification system (Art. 5(1)(h)) Biometric categorisation system (Art. 5(1)(g)) Emotion inference system (Art. 5(1)(f)) Other Unsure	*Explain*
4	*Name/description*	*Category* Remote biometric identification (Point 1(a)) Biometric categorisation (Point 1(b)) Emotion recognition (Point 1(c))	*Category* Real time remote biometric identification system (Art. 5(1)(h)) Biometric categorisation system (Art. 5(1)(g)) Emotion inference system (Art. 5(1)(f)) Other Unsure	*Explain*
		Category	*Category* Real time remote biometric identification system (Art. 5(1)(h))	

5	*Name/description*	○ Remote biometric identification (Point 1(a)) ○ Biometric categorisation (Point 1(b)) ○ Emotion recognition (Point 1(c))	○ Biometric categorisation system (Art. 5(1)(g)) ○ Emotion inference system (Art. 5(1)(f)) ○ Other ○ Unsure	*Explain*

Question 9. If you see the need for clarification of the high-risk classification in Point 1 of Annex III to the AI Act and its **interplay with other Union or national legislation**, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay

1500 character(s) maximum

2.E. Questions in relation to the access to and enjoyment of essential private services and essential public services and benefits (Annex III, point 5)

The classification of AI systems as high-risk under Annex III point 5 AI Act targets AI systems which are intended to be used in different contexts of access to and enjoyment of essential private services and essential public services and benefits. According to recital 58, these are generally services necessary for people to fully participate in society or to improve one's standard of living. In particular, natural persons applying for or receiving essential public assistance benefits and services from public authorities namely healthcare services, social security benefits, social services providing protection in cases such as maternity, illness, industrial accidents, dependency or old age and loss of employment and social and housing assistance, are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities.

Point 5 of Annex III to the AI Act distinguishes between four different types of use cases that are classified as high-risk in the area of the access to and enjoyment of services and benefits.

Point 5(a) of Annex III to the AI Act refers to AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services.

Point 5(b) of Annex III to the AI Act refers to AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud. According to recital 58, AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under the AI Act. Point 5(b) of Annex III therefore contains two distinct use cases:

1. *AI systems intended to be used to evaluate the creditworthiness of natural persons.*
2. *AI systems intended to be used to establish their credit score.*

Point 5(c) of Annex III to the AI Act refers to AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance. According to recital 58, AI systems

provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under the AI Act.

Point 5(d) of Annex III to the AI Act refers to AI systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of, emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems. Point 5(d) of Annex III therefore contains four distinct use cases:

1. *AI systems intended to evaluate and classify emergency calls by natural persons.*
2. *AI systems intended to be used to dispatch emergency first response services, including by police, firefighters and medical aid.*
3. *AI systems intended to be used to establish priority in the dispatching of emergency first response services, including by police, firefighters and medical aid.*
4. *AI systems intended to be used as emergency healthcare patient triage systems*

Question 20. Please provide practical examples of AI systems that in your opinion may fall within the scope of high-risk AI systems related to essential private services and essential public services and benefits.

Examples may include systems for which you have uncertainties or system that you consider should not be considered high-risk as they are outside the use cases listed in Annex III or they fulfil one or more of the conditions for the exceptions in Article 6(3) AI Act.

	Name and description of the system	Category of AI system	The system is considered high-risk	Motivate your previous answer	The AI system performs profiling of natural person	The AI system meets at least one of the exception criteria of Article 6(3)	Motivate your previous answer and specify any exception criteria that it meets, if applicable
1	*Name/description* Credit Scoring System: An AI system that may ingest consumer applicants' traditional financial data (eg salary, existing debts, past defaults) together with alternative data (eg open-banking transaction streams). The model outputs a credit score that is used by, for example, banks in automated or largely automated consumer lending decisions. Two deployment patterns are common: • Provider is service provider; deployer is bank: The service provider actively builds or commissions the system and supplies it to a bank that embeds it in its consumer lending processes. • Service provider is provider & deployer: The service provider builds and uses the AI system, sells the resulting scores to banks, who consider the score for consumer lending. Only one product ACCIS member provide clients is in scope: creditworthiness assessments of natural persons using AI as defined in the Act and the Commission's guidelines. Only real-time processing AI-enabled capabilities that directly lead to a credit decision or determine the eligibility of credit recipients should be considered high-risk use cases.	*Category* Evaluation of creditworthiness/ credit score of natural persons (Point 5(b))	*High-risk* Yes, completely	*Explain* Annex III(5)(b) lists 'establishment of a credit score' as a stand-alone high-risk use-case because the output can directly determine access to an essential private service (consumer credit).	*Profiling* Yes	*Exception* No	*Explain* The Art. 6(3) exceptions do not apply due to the profiling of natural persons involved in the credit scoring.
2	*Name/description* Creditworthiness assessment decision engine: An AI system that may ingest data supplied by, for example, a loan applicant (income, liabilities, demographic details) together with internal banking history and third party bureau data. It produces a score and a lending / pricing recommendation that is automatically surfaced in the bank's loan origination workflow. Depending on the business set up: (1) Bank developed: The bank designs, trains & deploys the AI system itself or through subcontractors; the bank is both provider and deployer under the AI Act, while the IT house is merely a component supplier. (2) Service-provider developed: A service provider builds the AI system once and licenses it 'as is' to many banks; here the service provider is the 'provider' under the AI Act and each bank is only a deployer.	*Category* Evaluation of creditworthiness/ credit score of natural persons (Point 5(b))	*High-risk* Yes, completely	*Explain* Annex III(5)(b) designates any AI system used to determine or estimate a natural person's creditworthiness as high risk. The output directly influences access to essential private service (credit) and may have a significant effect on the applicant's fundamental rights (eg non discrimination). Neither of the alternative organisational arrangements (bank as provider vs. service-provider as provider) changes the functional use case; in both, the AI system remains within Annex III(5)(b).	*Profiling* Yes	*Exception* No	*Explain* Art. 6(3) exceptions cover narrow, purely ancillary functions that do not themselves determine the significant outcome of the AI system. An AI system, as described above, however, is the core decision engine: It produces an assessment that directly drives lending approval or pricing and typically includes profiling.

							It therefore does not qualify for an Art. 6(3) carve-out, irrespective of whether the model is owned by the bank or an IT service provider.
3	*Name/description* Transaction Categorisation Engine: AI system that scans payment transactions, maps them to a taxonomy of income and expense categories (eg salary, utilities, groceries), and outputs a structured dataset. The engine may be used in data pipelines that feed credit decision models, KPIs or analytics dashboards, but it typically does not produce a credit score, recommendation or any other human interpretable assessment of an applicant.	*Category* Evaluation of creditworthiness/ credit score of natural persons (Point 5(b))	*High-risk* No	*Explain* The AI system only carries out purely accessory tasks in the sense of Art. 6(3)(a) or (d) and Recital 53 (indexing, organising and classifying data): - It neither evaluates creditworthiness nor influences underwriting thresholds directly. - Its output is one of many data-fields that subsequent (and separately validated) risk-models may or may not consider. - Applicants are never exposed to the system's output in a way that would affect their rights or obligations.	*Profiling* No	*Exception* Yes	*Explain* The AI system satisfies either Art. 6(3)(a) by performing a narrow procedural task, or Art. 6 (3)(d) by performing a preparatory task – pre-processing, structuring and labelling data – for a potential high-risk use case without determining or substantially influencing the final decision.
4	*Name/description*	*Category* ○ Evaluation of eligibility for public assistance benefits and services (Point 5 (a)) ○ Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) ○	*High-risk* ○ Yes, completely ○ Partially	*Explain*	*Profiling* ○ Yes ○ No	*Exception* ○ Yes ○ No	*Explain*

		Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) Evaluation and classification of emergency calls (Point 5(d))	No Unsure		Unsure	Unsure	
5	*Name/description*	*Category* Evaluation of eligibility for public assistance benefits and services (Point 5 (a)) Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) Evaluation and classification of emergency calls (Point 5(d))	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*

6	*Name/description*	*Category* Evaluation of eligibility for public assistance benefits and services (Point 5 (a)) Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) Evaluation and classification of emergency calls (Point 5(d))	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*	
		Category Evaluation of eligibility for public assistance benefits and services (Point 5 (a)) Evaluation of creditworthiness/	*High-risk*					

7	*Name/description*	credit score of natural persons (Point 5(b)) Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) Evaluation and classification of emergency calls (Point 5(d))	Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*
8	*Name/description*	*Category* Evaluation of eligibility for public assistance benefits and services (Point 5 (a)) Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) 	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*

		Evaluation and classification of emergency calls (Point 5(d))					
9	*Name/description*	*Category* Evaluation of eligibility for public assistance benefits and services (Point 5 (a)) Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) Evaluation and classification of emergency calls (Point 5(d))	*High-risk* Yes, completely Partially No Unsure	*Explain*	*Profiling* Yes No Unsure	*Exception* Yes No Unsure	*Explain*
		Category Evaluation of eligibility for public assistance benefits and services (Point 5 (a))					

10	*Name/description*	○ Evaluation of creditworthiness/ credit score of natural persons (Point 5(b)) ○ Risk assessment and pricing in relation to natural persons for life /health insurance (Point 5(c)) ○ Evaluation and classification of emergency calls (Point 5(d))	*High-risk* ○ Yes, completely ○ Partially ○ No ○ Unsure	*Explain*	*Profiling* ○ Yes ○ No ○ Unsure	*Exception* ○ Yes ○ No ○ Unsure	*Explain*

Question 21. If you have or know practical examples of AI systems related to essential private services and essential public services and benefits where you need further clarification regarding the d**istinction from prohibited AI systems**, in particular Art. 5(1)(c) AI Act, please specify

It is our recommendation that the Guidelines on Prohibited AI Systems should make a clearer distinction between 'social scoring' and credit scoring. In those guidelines, the definition of social behaviour and personal characteristics is broad. However, the guidelines acknowledge that a creditworthiness assessment as a process is part of responsible lending as required by the Consumer Credit Directive and the Mortgage Credit Directive, which ultimately contributes to preventing over-indebtedness of consumers. It is therefore listed as one of the examples of legitimate scoring practices in line with Union and national law that are outside the scope of Article 5(1)(c) AI Act. The AI Act makes clear that creditworthiness assessments are not social scoring—only social scoring is prohibited. The guidelines should make that clear.

Question 22. Do you see the need for clarification of one of the various use cases of high-risk classification in *Point 5 of Annex III to the AI Act* and its **interplay with other Union or national legislation**, please specify the practical provision in other Union or national law and where you see need for clarification of the interplay

1500 character(s) maximum

Credit checks intersect the Consumer Credit Directive, Mortgage Credit Directive, GDPR and the upcoming AI Act. Parallel enforcement creates overlapping – and sometimes conflicting – duties that erode legal certainty, complicate operations and chill innovation. The GDPR/AI Act overlap analysed by Judith Arnal (ECRI; retrieved here: https://www.ecri.eu/sites/default/files/unfit_for_purpose_ecri_in_depth_analysis.pdf) shows how one scoring model can face incompatible interpretations: data protection logic when its output feeds an automated decision, AI compliance logic when the model is tagged "high risk". Clarification is most urgent for AI that performs narrow, procedural tasks such as feature engineering, model training or monitoring. These steps improve accuracy but do not decide credit outcomes; they warrant lighter rules than systems that approve or reject applicants. Risks of discrimination are already mitigated by sectoral instruments (Consumer Credit Directive, Mortgage Credit Directive, EBA Guidelines on loan origination and monitoring) and horizontal rules (GDPR). These frameworks ensure relevant, proportional data, require validation and monitoring, and guarantee consumer rights to information, human review and redress. Many AI Act duties duplicate existing GDPR obligations; without a clear line between the two regimes, firms face double regulation and persistent uncertainty.

Question 23. Do you have or know practical examples of AI systems that could fall under the **exception** mentioned in *Point 5 of Annex III to the AI Act* and *recital 58 AI Act*?

	Name and description of the system	Category of exception	Please motivate your answer
1	*Name/description* Certain ACCIS members provide AI systems to prevent financial fraud in the context of a credit application. These systems are not high risk because they are explicitly excluded from the use case definition in Point 5 of Annex III(5)(b).	*Category* Exception of being intended for the purpose of detecting financial fraud (Point 5 (b))	*Explain* Fraud related activities are crucial for complying with AML/CTF (Anti-Money Laundering /Counter-Terrorism Financing) legislation and aiding public authorities in combating fraud. The use of AI in these anti-fraud steps are explicitly excluded in Annex III(5)(b).
2	*Name/description* AI systems may be used to prevent financial fraud in the context of risk assessments and pricing in relation to individuals in the case of life or health insurance.	*Category* Exception of being intended for the purpose of detecting financial fraud (Point 5 (b))	*Explain* The insurance high-risk use cases for life and health insurance under Annex III(5)(c) do not explicitly exclude fraud systems such as the credit use cases in Annex III(5)(b). However, there is no objective reason for differentiation between credit fraud and life/health insurance fraud. The fraud exception must therefore also apply analogously to the fight against fraud in the area of life and health insurance (Hacker, The AI Act between Digital and Sectoral Regulations, page 27, link: https://www.bertelsmann-stiftung.de/en/publications/publication/did/the-ai-act-between-digital-and-sectoral-regulations-en). Rec. 58 supports this view, as the wording outlines systems detecting fraud in the offering of ‘financial services’, which include both credit-related and insurance-related services. A clear position from the Commission on this topic would be helpful.
		Category ○ Exception of being intended for the purpose of detecting financial fraud (Point 5(b)) ○	

3	*Name/description*	Exception of being intended for the purpose of detecting fraud in the offering of financial services or for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements (recital 58)	*Explain*
4	*Name/description*	*Category* ○ Exception of being intended for the purpose of detecting financial fraud (Point 5(b)) ○ Exception of being intended for the purpose of detecting fraud in the offering of financial services or for prudential purposes to calculate credit institutions' and insurance	*Explain*

		undertakings' capital requirements (recital 58)	
5	*Name/description*	*Category* ○ Exception of being intended for the purpose of detecting financial fraud (Point 5(b)) ○ Exception of being intended for the purpose of detecting fraud in the offering of financial services or for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements (recital 58)	*Explain*

Section 3. Questions on horizontal aspects of the high-risk classification

The classification of AI systems as high-risk is made depending on the intended purpose of the AI system.

The intended purpose is defined by Article 3(12) AI Act as the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation.

Question 33. What aspects of the definition of the intended purpose, as outlined in Article 3(12) AI Act, need additional clarification?
Please specify the concrete elements and the issues for which you need further clarification; please provide concrete examples

1500 character(s) maximum

Under Art. 3(12) the 'intended purpose' depends on the specific context and conditions of use found in instructions for use, promotional material and Annex IV technical documentation. Especially for credit scoring AI, four aspects need clarification: 1. Granularity of 'context and conditions': Must providers list factors that significantly affect how the system is designed and used in the instructions for use, promotional material or technical file? 2. Effect of marketing claims: Art. 3(12) covers 'promotional or sales materials'. How can binding performance claims be separated from non-binding claims in promotional or sales materials? 3. Routine model updates vs. 'substantial modification' (Art. 3(23)): Credit scoring models are regularly retrained within the same scope. Criteria would be helpful that indicate when such updates remain inside the original intended purpose and when a new conformity assessment is needed due to a substantial modification (Art. 43(4)). 4. Consistency of documentation: Instructions for use (deployer-facing) and the Annex IV technical file (regulator-facing) differ in detail. Which document prevails if descriptions diverge, and how closely must they mirror each other?

While the high-risk classification pursuant to Article 6(1) and Annex I AI Act is based on the concept of an AI system being used as a safety component of products regulated under Union harmonisation laws referred to in Annex I, Article 6(2) and Annex III AI Act list certain use cases considered to be high-risk. The two categories are in principle intended not to overlap.

Question 34. If you have or know practical examples of AI systems that in your opinion could be relevant for the high-risk classification according to **both Article 6(1) and 6(2) AI Act** and **thus require further clarification**, please specify the concrete AI system, how it is used in practice and how all the necessary elements described above are fulfilled

1500 character(s) maximum

Section 4 – Questions in relation to requirements and obligations for high-risk AI systems and value chain obligations

A. Requirements for high-risk AI systems

The AI Act sets mandatory requirements for high-risk AI systems as regards risk management (Article 9), data and data governance (Article 10), technical documentation (Article 11) and record-keeping (Article 12), transparency and the provision of information to deployers (Article 13), human oversight (Article 14), and robustness, accuracy and cybersecurity (Article 15).

Providers are obliged to ensure that their high-risk AI system is compliant with those requirements before it is placed on the market. Harmonised standards will play a key role to provide technical solutions to providers that can voluntarily rely on them to ensure compliance and rely on a presumption of conformity. The Commission has requested the European standardisation organisations CEN and CENELEC to develop standards in support of the AI Act. This work is currently under preparation.

Question 35. Beyond the technical standards under preparation by the European Standardisation Organisations, are there further aspects related to the AI Act's requirements for high-risk AI systems in Articles 9-15 for which you would seek clarification, for example through guidelines?

If so, please elaborate on which specific questions you would seek further clarification.

3000 character(s) maximum

We believe additional guidance is needed in three inter related areas of Art. 9-15 for high-risk AI systems in the context of creditworthiness assessments and credit scoring: 1. Human oversight: The AI Act requires 'effective' oversight (Art. 14), yet leaves open how this is achieved at industrial scale. We therefore request: • Clarification on the applicable reference standard. ISO/IEC CD 42105 ('Guidance for human oversight of AI systems') is already at Committee Draft stage. Should providers implement it now, or wait for other practical guidance (eg CEN CENELEC deliverable) to implement human oversight requirements? • Definition of proportionality: In credit scoring, manual review of every individual score is infeasible. May 'meaningful' oversight be fulfilled through (i) monitoring tools (eg performance dashboards with threshold based alerts), and (ii) regular audits? • Evidence expectations: Which artefacts may demonstrate that oversight is effective and proportionate to the risks? 2. CEN-CENELEC standards and conformity assessment: The conformity assessment (especially against Art. 9-15) is the backbone of the AI Act, yet the standardisation landscape is still in development: • Mapping obligations to standards: A table or guideline allocating high-risk AI obligations to the supporting CEN CENELEC standard would be invaluable, as would an explicit list of obligations not covered by such standards. • Status of assessment standards: We note that SIST TP CEN/CLC/TR 17894:2025 provides conformity assessment guidance, whereas the Conformity Assessment Framework (project JT021038) is still under preparation. Guidance is needed on how to bridge the gap until the framework is finalised. • 'Stop the clock': Without appropriate CEN-CENELEC standards in due time, compliance with high-risk AI obligations by the application date of 2 August 2026 is severely at risk. 3. Technical documentation (Annex IV & Art. 11): Annex IV lists extensive documentation elements, but practical implementation details remain unclear, particularly for large non SME providers who operate multiple AI systems: • Expected depth and format: Will the Commission, CEN-CENELEC or market surveillance authorities provide a template or reference structure for the technical file? • Digital annexes: May firms supply some elements (eg performance dashboards, lineage metadata) via machine readable repositories or APIs, rather than static documents?

Question 36. Are there aspects related to the requirements for high-risk AI systems in Articles 9-15 which require clarification regarding their interplay with other Union legislation?

If so, please elaborate which specific aspects require clarification regarding their interplay with other Union legislation and point to concrete provisions of specific other Union law.

3000 character(s) maximum

1. High-risk AI obligations vs. financial services law: Financial institutions are subject to financial services law, which requires enterprise-wide risk and internal control frameworks, further specified in regulatory guidance (cf. EBA Guidelines on loan origination and monitoring). Please explain how these frameworks impact provider obligations under Art. 9(10), 17(4), 18(3), 19(2), and explain how this affects a service provider who is classified as: (i) a supplier, i.e. that assists a financial institution classified as a provider and deployer in the sense of the AI Act in developing an AI system within the scope of Annex III(5)(b) or (c) of the AI Act; or (ii) a provider of such an AI system, while the financial institution acts only as a deployer. 2. Art. 10 data governance vs. GDPR lawfulness: Bias testing may involve special categories of personal data. Please explain the acceptable use of Art. 6(1) and (4) and Art. 9 GDPR legal bases for financial institutions and their service providers. Consider that, depending on the use case under Annex III(5)(b) and (c), financial institutions and service providers may not all be considered the provider under the AI Act (that may rely on Art. 10 AI Act). 3. Art. 9-15 vs. GDPR assessments: Please explain how high-risk AI obligations (eg data governance, risk management) affect GDPR assessments, particularly legitimate impact assessments (LIAs) and data protection impact assessments (DPIAs). Does the fulfilment of AI Act's high-risk AI obligations, for example, indicate that the data subjects' interests do not override the interests of the controller, or the data protection risk for individuals is not high? 4. Art. 11, 12 (and Art. 18, 19) documentation and logging vs. GDPR storage limits: Guidance is needed on whether and how personal data should be stored (eg anonymised, pseudonymised) under Art. 6(1)(c) GDPR, where the AI Act sets out documentation and logging, in particular when a bank, insurer or service provider is classified as a provider under the AI Act in the context of use cases under Annex III(5)(b) and (c). 5. Art. 14 human oversight vs. GDPR and Consumer Credit Directive 2023/2225 (CCD2): The mechanisms in the GDPR (eg Art. 22) and the Consumer Credit Directive (eg Art. 18(8)) already ensure the right to human review and explanation for automated credit decisions made about consumers. Please explain how meeting these (non-AI-Act) obligations affects the human oversight duties of providers under Art. 14, in particular when a bank, insurer or service provider is classified as a provider under the AI Act in the context of use cases under Annex III(5)(b) and (c). 6. Art. 15 cybersecurity vs. DORA, NIS2 and CRA: Please provide guidance on how cybersecurity rules in Art. 15 interact with entity-specific cybersecurity obligations in DORA, and NIS2, and product-specific obligations in the CRA for providers, in particular when a bank, insurer or service provider

B. Obligations for providers of high-risk AI systems

Beyond ensuring that a high-risk AI system is compliant with the requirements in Articles 9-15, providers of high-risk AI systems have several other obligations as listed in Article 16 and further specified in other corresponding provisions of the AI Act. These include:

- *Indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trademark, the address at which they can be contacted;*
- *Have a quality management system in place which complies with Article 17;*
- *Keep the documentation referred to in Article 18;*
- *When under their control, keep the logs automatically generated by their high-risk AI systems as referred to in Article 19;*

- *Ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43;*
- *Draw up an EU declaration of conformity in accordance with Article 47;*
- *Affix the CE marking to the high-risk AI system, in accordance with Article 48;*
- *Comply with the registration obligations referred to in Article 49(1);*
- *Take the necessary corrective actions and provide information as required in Article 20;*
- *Cooperate with national competent authorities as required in Article 21;*
- *Ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.*

Question 37. Are there aspects related to the AI Act's obligations for providers of high-risk AI systems for which you would seek clarification, for example through guidelines?

If so, please elaborate on which specific questions you would seek further clarification.

3000 character(s) maximum

Post-market monitoring: Further guidance is needed on the scope and format of relevant data under Article 72 (eg automatically generated logs) and on post-market monitoring plans, in particular when a bank, insurer or service provider is classified as a provider under the AI Act in the context of use cases under Annex III(5)(b) and (c). For example: • What types of events or metrics must be logged? • How long should relevant data be retained, and in what technical format – ensuring AI Act auditability while remaining GDPR-compliant? • What constitutes a 'serious incident' in the context of AI systems used for creditworthiness assessments, establishing a credit score or risk assessments and pricing in relation to individuals in the case of life and health insurance?

Question 38. Are there aspects related to the obligations for providers of high-risk AI systems which require clarification regarding their interplay with other Union legislation?

If so, please elaborate which specific aspects require clarification regarding their interplay with other Union legislation and point to concrete provisions of specific other Union law.

3000 character(s) maximum

Art. 13, 26 instructions for use vs. transparency under GDPR and Consumer Credit Directive 2023/2225 (CCD2): Art. 18(8) of the CCD2 requires creditors (who may deploy AI systems for creditworthiness assessments or to establish credit scores) to provide applicants with a 'clear and comprehensible explanation of the creditworthiness assessment' and a human review of automated credit decisions. An individual's right of access under Art. 15(1)(h) GDPR may also include 'meaningful information' about automated decisions, as defined in Art. 22 GDPR. Please provide guidance on whether and how a provider in the context of use cases under Annex III(5)(b) and (c) must disclose information (eg in instructions for use under Art. 13) to a creditor acting as a deployer under the AI Act (cf. Art. 26(1)), and to which extent the creditor may rely on the provider's information for relevant CCD2 and GDPR information disclosures to consumers/individuals.

C. Obligations for deployers of high-risk AI systems

Article 3(4) defines a deployer as a 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.

Deployers of high-risk AI systems have specific responsibilities under the AI Act. Transversally, Article 26 obliges all deployers of high-risk AI systems to:

- *Take appropriate technical and organisational measures to ensure that AI systems are used in accordance with the instructions accompanying the AI systems;*
- *Assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support;*
- *Ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system;*
- *Monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72;*
- *Keep the logs automatically generated by that high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system of at least six months.*

Additionally, Article 26 foresees the following obligations in specific cases:

- *For high-risk AI system at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system;*
- *Specific authorization requirements and restrictions apply to the deployer of a high-risk AI system for post-remote biometric identification for law enforcement purposes;*
- *Deployers of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the high-risk AI system.*

Question 39. Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems listed in Article 26 for which you would seek clarification, for example through guidelines?

If so, please elaborate on which specific questions you would seek further clarification.

3000 character(s) maximum

Post-market monitoring: Further guidance is needed on the scope of the monitoring obligation under Art. 26(5), in particular when a bank, insurer or service provider is classified as a deployer under the AI Act in the context of use cases under Annex III(5)(b) and (c).

Question 40. Are there aspects related to the obligations for deployers of high-risk AI systems listed in Article 26 which require clarification regarding their interplay with other Union legislation?

If so, please elaborate which specific aspects require clarification regarding their interplay with other Union legislation and point to concrete provisions of specific other Union law.

3000 character(s) maximum

1. Financial services law: Financial institutions are subject to financial services law (eg CRD IV and Solvency II), which requires enterprise-wide risk and internal control frameworks – further specified in regulatory guidances (cf. EBA Guidelines on loan origination and monitoring). Please explain how these frameworks impact deployer obligations under Art. 26(5) and (6), and explain how this affects a service provider who is classified as: (i) a supplier, i.e. that assists a financial institution classified as a provider and deployer in the sense of the AI Act in developing an AI system within the scope of Annex III(5)(b) or (c) of the AI Act; or (ii) a provider of such an AI system, while the financial institution acts only as a deployer. 2. GDPR retention: Guidance is also needed on whether and how personal data should be stored (eg anonymised, pseudonymised) under Art. 6(1)(c) GDPR, where the AI Act sets out documentation and logging, in particular when a bank, insurer or service provider is classified as a deployer under the AI Act in the context of use cases under Annex III(5)(b) and (c). 3. Art. 13, 26 instructions for use vs. transparency under GDPR and Consumer Credit Directive 2023/2225 (CCD2): Art. 18(8) of the CCD2 requires creditors (who may deploy AI systems for creditworthiness assessments or to establish credit scores) to provide applicants with a 'clear and comprehensible explanation of the creditworthiness assessment' and a human review of automated credit decisions. An individual's right of access under Art. 15(1)(h) GDPR may also include 'meaningful information' about automated decisions, as defined in Art. 22 GDPR. Please provide guidance on whether and how a creditor acting as deployer in the context of use cases under Annex III(5)(b) and (c) can rely on information that a provider shared with the creditor (in particular the instructions for use under Art. 13) for CCD2 and GDPR information disclosures to consumers/individuals.

Moreover, according to Article 27, deployers of high-risk AI systems that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an ***assessment of the impact on fundamental rights*** *that the use of such system may produce. The AI Office is currently preparing a template that should facilitate compliance with this obligation.*

Article 27 specifies that where any of its obligations are already met through the data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment.

Question 41. Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems for the fundamental rights impact assessment for which you would seek clarification in the template?

3000 character(s) maximum

The following elements would make the template concise, easy to navigate, and usable across the financial sector without forcing disproportionate detail: 1. Responsibility split: Considering Art. 27(2)(2), clear indicators showing which parts of the FRIA were filled by the provider, by the deployer, or jointly when the same business performs both roles. 2. Scope trigger: A simple decision flow that confirms whether the AI system is actually 'high risk' and deployers know when a FRIA is required (eg credit scoring, yes; fraud detection, no). 3. Reuse & updates: Guidance on when an existing FRIA or DPIA can be reused, and plain criteria for what counts as a change that forces an update under Art. 27(2)(3). 4. Human oversight & redress: High level questions that address human oversight measures (eg override the AI output; Art. 27(1)(e)) and measures to be taken in the

case of the materialisation of risks (eg customers contest AI output; Art. 27(1)(f)), without demanding granular operational detail. 5. Evidence expectations: A checklist of the types of evidence regulators expect (bias test summary, governance policy, etc.) so deployers can attach existing documents rather than creating new ones. 6. Confidentiality & publication: Options to mark sections as commercially sensitive, clarifying what will remain private once the template is submitted to authorities.

Question 42. In your view, how can complementarity of the fundamental rights impact assessment and the data protection impact assessment be ensured, while avoiding overlaps?

3000 character(s) maximum

1. One workflow, two outputs: Run a single assessment process that produces a DPIA section for data protection issues and a FRIA section for broader fundamental rights issues, sharing the same system description and risk register. 2. Mapping table: Include a short cross-reference showing which DPIA paragraphs satisfy which FRIA requirements, so information is written once and simply pointed to. 3. Shared update triggers: Adopt identical change rules so both assessments are reviewed together, never drifting out of sync. 4. Leverage existing GDPR methodologies: Where the DPIA already requires necessity & proportionality tests for data protection risks, the FRIA can explicitly 'inherit' that analysis and focus on additional fundamental right risks, rather than restating the same evaluations. The template may include checkboxes to confirm such inheritance.

Finally, deployers of high-risk AI systems may have to provide an explanation to an affected person upon their request. This right is granted by Article 86 AI Act to affected persons which are subject to a decision, which is taken on the basis of the output from a high-risk AI system listed in Annex III and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights.

Question 43. Are there aspects related to the AI Act's right to request an explanation in Article 86 for which you would seek clarification, for example through guidelines?

If so, please elaborate on which specific questions you would seek further clarification.

3000 character(s) maximum

1. Right to explanation vs. Art. 22 GDPR: Please provide guidance on how Art. 86 interacts with Art. 22 GDPR, particularly whether Art. 86 applies in light of Art. 86(3) in cases where Art. 22 GDPR applies, and whether Art. 86(2) is relevant for the use cases under Annex III(5)(b) and (c). Consider that a bank, insurer or service provider may be classified as a deployer of such AI systems under the AI Act in the context of Annex III(5)(b) and (c). Also, please provide guidance on how Art. 22 GDPR impacts Art. 86 when a service provider (eg a credit bureau) is or is not in scope of Art. 22 GDPR in light of CJEU case law (C-634/21). 2. Right to explanation vs. Art. 18 CCD2: Please provide guidance on how Art. 86 interacts with the information obligations of creditors (often acting as deployers of AI systems under Annex III(5)(b) and (c)) under Art. 18 CCD2. Consider that also a service provider may be classified as a deployer of such AI systems under the AI Act.

D. Substantial modification (Article 25 (1) AI Act)

Article 3 (23) defines a substantial modification as 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. As a result of such a change, the compliance of the AI system with the requirements for high-risk AI systems is either affected or results in a modification to the intended purpose for which the AI system has been assessed.

The concept of 'substantial modification' is central to the understanding of the requirement for the system to undergo a new conformity assessment. Pursuant to Article 43(4), the high-risk AI system should be considered a new AI system which should undergo a new conformity assessment in the event of a substantial modification.

This concept is also central for the understanding of the scope of obligations between a provider of a high-risk AI system and other actors operating in the value chain (distributor, importer or deployer of a high-risk AI system). Pursuant to Article 25, any distributor, importer, deployer or other third-party shall be considered to be a provider of a high-risk AI system and shall be subject to the obligations of the provider, in any of the following circumstances:

(a), they put their name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations are otherwise allocated;

(b), they make a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in such a way that it remains a high-risk AI system;

(c), they modify the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service in such a way that the AI system concerned becomes a high-risk AI system.

Question 44. Do you have any feedback on issues that need clarification as well as practical examples on the application of the concept of 'substantial modification' to a high-risk AI system.

3000 character(s) maximum

The concept of 'substantial modification' is central to determining (i) when a high-risk AI system must undergo a new conformity assessment (Art. 43(4)), (ii) when other actors in the value chain (eg deployers or distributors) may assume the role of provider (Art. 25(1)(b)), and (iii) when the AI Act applies in case of significant changes (Art. 111(2)). While Art. 3(23) defines substantial modification as a change not foreseen in the original conformity assessment that affects compliance or the intended purpose, further clarification is needed for day-to-day operations in the financial sector. Art. 44(4)(2) and Rec. 128 usefully exempts 'pre-determined' updates, including changes occurring to the algorithm and the performance of AI systems which continue to 'learn' after being placed on the market or put into service, but concrete criteria and examples are missing.

Article 43(4) second sentence describes the circumstances under which the change does not qualify as a substantial modification: 'For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.'

Question 45. Do you have any feedback on issues that need clarification as well as practical example of pre-determined changes which should not be considered as a substantial modification within the meaning the Article 43(4) of the AI Act.

3000 character(s) maximum

In practice, many lifecycle updates to high-risk AI systems are routine, pre-planned, and do not alter the risk profile. Further clarification is therefore essential to distinguish these pre-determined, non-substantial changes from those that trigger a new conformity assessment.

E. Questions related to the value chain roles and obligations

Throughout the AI value chain, multiple parties contribute to the development of AI systems by supplying tools, services, components, or processes. These parties play a crucial role in ensuring the provider of the high-risk AI system can comply with regulatory obligations. To facilitate compliance with regulatory obligations, Article 25(4) require these parties to provide the high-risk AI system provider with necessary information, capabilities, technical access and other assistance through written agreements, enabling them to fully meet the requirements outlined in the AI Act.

However, third parties making tools, services, or AI components available under free and open-source licenses are exempt from complying with value chain obligations. Instead, providers of free and open-source AI solutions are encouraged to adopt widely accepted documentation practices, such as model cards and datasheets, to facilitate information sharing and promote trustworthy AI.

To support cooperation along the value chain, the Commission may develop and recommend voluntary model contractual terms between providers of high-risk AI systems and third-party suppliers.

Question 46. From your organisation's perspective, can you describe the current distribution of roles in the AI value chain, including the relationships between providers, suppliers, developers, and other stakeholders that your organisation interacts with?

3000 character(s) maximum

Service providers often develop and operate AI solutions under Annex III(5)(b) and (c), i.e. for (i) creditworthiness assessments, (ii) credit scoring, and (iii) life and health insurance risk/pricing – all generally classed as high risk under Art. 6(2), unless an Art. 6(3) exception applies. Depending on the product and commercial model, a service provider may occupy one or several roles simultaneously; clear allocation of responsibilities, contractual clauses, and documented hand offs with all relevant stakeholders would ensure compliance and accountability. 1. Provider of high risk AI systems • Scenario: Service provider designs, trains, validates and commercially places a creditworthiness or insurance pricing engine that a bank/insurer then deploys. • Responsibilities: Service provider acts as provider in the sense of the AI Act; final lending or underwriting decisions remain with the client; service provider ensures its suppliers provide sufficient information to comply with provider-obligations (eg technical documentation). 2. Supplier of a component or tool • Scenario: A (banking) client builds its own high risk AI system for creditworthiness assessments but licenses a model as a component from a service provider (eg scorecard). • Responsibilities: Service provider delivers the component, shares performance and robustness evidence, and notifies the client-provider of any substantial update. The client provider retains end to end obligations; service provider supports their conformity

assessment. 3. Deployer of an internal system • Scenario: Service provider generates credit scores in house on its own platform and sells the scores (not the model) to multiple lenders. • Responsibilities: Service provider acts as provider and deployer of the underlying high risk AI. 4. Other stakeholders: • Developers & MLOps: Internal teams of service providers, banks and insurers handle data ingestion, feature engineering, model lifecycle, stress-testing, fairness and explainability checks. • Data providers: Banks, insurers, credit bureau contributors, public registries and third-party brokers supply raw data. • Technology partners: Cloud/IaaS vendors, secure model-hosting services, and specialist AI-library suppliers provide infrastructure or tooling for the AI systems and/or components. • End Users / Consumers: Individuals affected by AI-driven decisions receive clear explanations, contestability channels and privacy notices; their feedback feeds in continuous-improvement loops.

Question 47 Do you have any feedback on potential dependencies and relationships throughout the AI value chain that should be taken into consideration when implementing the AI Act's obligations, including any upstream or downstream dependencies between providers, suppliers, developers, and other stakeholders, which might impact the allocation of obligations and responsibilities between various actors under the AI Act? In particular, indicate how these dependencies affect SMEs, including start-ups.

3000 character(s) maximum

Upstream dependencies: Service providers often use tools, data, or software from third-party suppliers to build AI systems or their components. These assets may materially affect performance, fairness and robustness of an AI system; but under the AI Act, the provider role determines main responsibility for a high-risk AI system. • Clarify the Art. 25(4) ‘chain-of-trust’: Suppliers of models, data, or SaaS components may need to provide a standardised compliance packet so, for example, the provider can complete the technical documentation and the deployer can prepare a fundamental rights impact assessment. • Responsibilities: How far is liability shared throughout the chain when a supplier’s component later proves non-compliant? Downstream dependencies: Service providers, banks and insurers may develop AI systems under Annex III(5)(b) and (c) and be classified as providers of such systems. If they provide these AI systems to other third parties acting as deployers, those deployers may (i) re-train or fine-tune a third-party model on local data, (ii) change thresholds or feature sets, or (iii) combine it with additional decision engines. Guidance would be helpful to determine in such cases whether the changes of the deployer make the deployer take on the role of ‘provider’ under Art. 25 of the AI Act.

Question 48. What information, capabilities, technical access and other assistance do you think are necessary for providers of high-risk AI systems to comply with the obligations under the AI Act, and how should these be further specified through written agreements?

3000 character(s) maximum

To comply with Art. 17, providers of high-risk AI systems must secure contractual support from all actors in the relevant value chain under Art. 25, including component suppliers, data vendors, and deployers. Written agreements should: • Allocate responsibilities (risk management, documentation, post market monitoring, serious incident reporting). • Specify the exact information, technical access and assistance each party must supply without impairing IP rights or trade secrets (Rec. 88). • Detail timelines, formats and escalation paths to keep the provider’s technical documentation and risk controls continuously up to date. High risk financial sector AI systems in the context of Annex III(5)(b) and (c) (eg credit scoring, creditworthiness assessments) typically blend proprietary models, bureau data and client side implementation. Unambiguous contractual duties ensure that: • the provider retains a complete, current technical file; • third party updates trigger timely re assessment of risk; • post market evidence flows back to the provider and relevant supplier to detect bias or drift; and • regulators can trace accountability across the supply chain. Detailed, time bound, and IP respectful written agreements are indispensable for providers and the stakeholders they interact with to fulfil AI Act obligations while safeguarding both innovation and fundamental rights.

Question 49. Please specify the challenges in the application of the value chain obligations in your organisation for compliance with the AI Act's obligations for high-risk AI systems and the issues for which you need further clarification; please provide practical examples.

1500 character(s) maximum

Section 5. Questions in relation to the need for possible amendments of high-risk use cases in Annex III and of prohibited practices in Article 5

Pursuant to Article 112(1) AI Act, the Commission shall assess the need to amend the list of use cases set out in Annex III and of the list of prohibited AI practices laid down in Article 5 by 2 August 2025 and once a year from then onwards.

The Commission is empowered to adopt delegated acts to amend Annex III by adding or modifying use-cases of high-risk AI systems pursuant to Article 7(1) AI Act. The findings of the assessment carried out under Article 112(1) AI Act are relevant in this context. The empowerment to amend Annex III requires that both of the following conditions are fulfilled:

- *the AI systems are intended to be used in any of the areas listed in Annex III and*
- *the AI systems pose a risk of harm to health and safety, or an adverse impact on fundamental rights, and that risk is equivalent to, or greater than, the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.*

Article 7(2) AI Act further specifies the criteria that the Commission shall take into account in order to evaluate the latter condition, including:

(a) the intended purpose of the AI system;

(b) the extent to which an AI system has been used or is likely to be used;

(c) the nature and amount of the data processed and used by the AI system, in particular whether special categories of personal data are processed;

(d) the extent to which the AI system acts autonomously and the possibility for a human to override a decision or recommendations that may lead to potential harm;

(e) the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect multiple persons or to disproportionately affect a particular group of persons;

(f) the extent to which the use of an AI system has already caused harm to health and safety, has had an adverse impact on fundamental rights or has given rise to significant concerns in relation to the likelihood of such harm or adverse impact, as demonstrated, for example, by reports or documented allegations submitted to national competent authorities or by other reports, as appropriate;

(g) the extent to which persons who are potentially harmed or suffer an adverse impact are dependent on the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome;

(h) the extent to which there is an imbalance of power, or the persons who are potentially harmed or suffer an adverse impact are in a vulnerable position in relation to the deployer of an AI system, in particular due to status, authority, knowledge, economic or social circumstances, or age;

(i) the extent to which the outcome produced involving an AI system is easily corrigible or reversible, taking into account the technical solutions available to correct or reverse it, whereby outcomes having an adverse impact on health, safety or fundamental rights, shall not be considered to be easily corrigible or reversible;

(j) the magnitude and likelihood of benefit of the deployment of the AI system for individuals, groups, or society at large, including possible improvements in product safety;

(k) the extent to which existing Union law provides for:

- effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;

- effective measures to prevent or substantially minimise those risks.

Question 50. Do you have or know concrete examples of AI systems that in your opinion need **to be added to the list of use cases in Annex III, among the existing 8 areas, in the light of the criteria and the conditions in Article 7(1) and (2)** and should be integrated into the assessment pursuant to Article 112(1) AI Act?

If so, please specify the concrete AI system that fulfils those criteria as well as evidence and justify why you consider that this system should be classified as high-risk.

3000 character(s) maximum

Question 51. Do you consider that some of the use cases listed in Annex III require adaptation in order to fulfil the conditions laid down pursuant to Article 7(3) AI Act and should therefore **be amended** and should be integrated into the assessment pursuant to Article 112(1) AI Act?

- Yes

- No

Please justify why you consider that the use case needs to be adapted in order to fulfil the conditions as per Article 7(3) AI Act

3000 character(s) maximum

Acknowledging that while this question relates to the use case rather than the technology itself, ACCIS uses this passage to reiterate that it is important to make clear the logic of the EU AI Act is to first define whether the system is an AI System or not to then as a second step analyse the use case within the prism of the risk-based categorisation. As we have mentioned in detail above, the use case of credit scoring appearing in the Annex III can be misleading. According to recital 58 of the final AI Act, the intended purpose of considering AI systems used to evaluate the creditworthiness of individuals or to establish their credit score as high-risk is to safeguard those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. ACCIS has in the past mentioned to the European Commission that there is insufficient evidence that creditworthiness assessments or credit scores affect as such or affect decisively access to essential services such as housing, electricity and telecommunications. In fact, there is robust evidence that creditworthiness assessments and credit score have no significant impact on access to those services. Consequently, we are of the view that the categorisation of AI systems as high-risk is creditworthiness assessments or credit scores should be understood in a restrictive way and should only be considered for AI systems deployed in a stage of the creditworthiness evaluation or the establishment of a credit score that directly and significantly influence the outcome of a credit decision. Failing this, ACCIS is of the view that there could be some clarification made distinguishing more clearly AI-powered Credit Scoring from the traditional methods, such as Logistic Regression, which has been used for decades by the industry as recognised in the Guidelines on Definition of AI System.

Question 52. Do you consider that some of the use cases listed in Annex III no longer *fulfil* the conditions laid down pursuant to Article 7(3) AI Act and should therefore **be removed from the list of use cases in Annex III** and should be integrated into the assessment pursuant to Article 112(1) AI Act?

- Yes
- No

Pursuant to Article 112(1) AI Act, the European Commission shall assess the need for amendment of the list of prohibited AI practices laid down in Article 5 once a year. In order to gather evidence of potential needs for amendments, respondents are invited to answer the following questions.

Question 53. Do you have or know concrete examples of AI practices that in your opinion contradict Union values of respect for human dignity, freedom, equality and no discrimination, democracy and the rule of law and fundamental rights enshrined in the Charter and for which there **is a regulatory gap because they are not addressed by other Union legislation**?

If so, please specify the concrete AI system that fulfils those criteria and justify why you consider that this system should be prohibited and why other Union legislation does not address this problem.

3000 character(s) maximum

Question 54. Do you consider that some of the prohibitions listed in Article 5 AI Act are already sufficiently addressed by other Union legislation and should therefore **be removed from the list of prohibited practices in Article 5 AI Act**?

- Yes
- No

Contact

Contact Form