

EUROPEAN COMPLIANCE SUITE

EU AI Act Compliance Evidence Templates

EXPLANATORY NOTICE AND TEMPLATE

Prohibition Screen and Applicability Assessment for emotion recognition and biometric categorisation systems under Article 5 and Article 50(3) of Regulation (EU) 2024/1689 (AI Act)

Template reference	ECS-AIA-50-3-SCOPE
Version	1.0
Issued	July 2026
Obligation addressed	Article 5 AI Act — prohibited practices screen; Article 50(3) AI Act — determination of the deployer information duty
Addressee	Deployers of emotion recognition or biometric categorisation systems; providers assessing what their systems permit
Position in the pack	Entry document, and the most important. Completed before ECS-AIA-50-3-RECORD; a prohibited use ends the exercise
Companion templates	ECS-AIA-50-3-RECORD — the Record; ECS-AIA-50-3-NOTICE — information to exposed persons; ECS-AIA-50-3-DATA — data protection interface

This Explanatory Notice and the Template annexed to it are issued by European Compliance Suite as private compliance documentation. They are not a Union instrument, are not endorsed by the European Commission or the AI Office, and do not constitute legal advice. Where the Commission adopts an official template, guidance or implementing act covering the same obligation, that instrument prevails.

1. Background and purpose

- (1) Article 50(3) of Regulation (EU) 2024/1689 (the ‘AI Act’) requires deployers of an emotion recognition system or a biometric categorisation system to inform the natural persons exposed to it of the operation of the system, and to process personal data in accordance with Union data protection law. The obligation applies from 2 August 2026.
- (2) Article 50(3) cannot be assessed in isolation, and this is what distinguishes it from the other transparency duties in Chapter IV. Several uses of emotion recognition and biometric categorisation are not merely subject to disclosure but are prohibited outright under Article 5 AI Act, which has applied since 2 February 2025. A deployer that begins with the question ‘how do we inform people?’ has already skipped the question that matters more: ‘are we permitted to do this at all?’
- (3) The consequences of that error are not symmetrical with the other transparency provisions. Infringement of Article 5 attracts the highest tier of administrative fines under Article 99(3) AI Act — up to EUR 35 000 000 or 7 % of total worldwide annual turnover, whichever is higher — as against the lower ceiling applicable to the Article 50 transparency duties. A deployer that documents a careful disclosure for a practice it was never permitted to carry out has documented its own infringement.
- (4) This Assessment therefore proceeds in two stages. The first is a prohibition screen against Article 5. Only if the intended use survives that screen does the second stage — the applicability assessment for Article 50(3) — arise. Where the screen identifies a prohibited use, the exercise ends and the outcome is that the use must not proceed, not that it must be disclosed.
- (5) The Assessment is completed by the deployer, because Article 50(3) binds the deployer. A provider of such a system may also complete it, in order to determine what uses its system permits and what it must tell its deployers; where a provider does so, it should record that it is assessing prospective deployer use rather than its own.

RELEVANT LEGAL TEXT

Article 50(3) AI Act.

Deployers of an emotion recognition system or a biometric categorisation system shall inform the natural persons exposed thereto of the operation of the system, and shall process the personal data in accordance with Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, as applicable. This obligation shall not apply to AI systems used for biometric categorisation and emotion recognition, which are permitted by law to detect, prevent or investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, and in accordance with Union law.

Article 5(1)(f) AI Act.

the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

Article 5(1)(g) AI Act.

the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;

Article 3(39) and (40) AI Act.

‘emotion recognition system’ means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data; ‘biometric categorisation system’ means an AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons.

2. How to use this Assessment

- (6) The Assessment proceeds through two stages and seven determinations. The stages are sequential and the first is dispositive: a use that is prohibited does not become permissible by being disclosed.
- Stage 1 — the prohibition screen. Determination A: is the system an emotion recognition or biometric categorisation system as defined? Determination B: does the use fall within the workplace or education prohibition? Determination C: does the use fall within the sensitive-inference prohibition?
 - Stage 2 — the Article 50(3) applicability assessment. Determination D: is the entity a deployer? Determination E: is there a Union nexus? Determination F: is the law-enforcement exception engaged? Determination G: which application dates govern?
- (7) Each determination requires reasoning, not only an answer. In this area more than most, the reasoning is the document's value: the definitions turn on contested technical questions, the prohibitions turn on purpose and context, and an unreasoned conclusion that a practice is permitted will not withstand examination.

3. Stage 1 — the prohibition screen

3.1. Determination A — is the system within the definitions?

- (8) An emotion recognition system is an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data. A biometric categorisation system is an AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless the categorisation is ancillary to another commercial service and strictly necessary for objective technical reasons.
- (9) Three points of difficulty recur. First, both definitions require processing of biometric data, and a system that infers state from non-biometric signals — for example typing speed, message content or purchase history alone — falls outside them, however similar its purpose. Second, the reference to 'intentions' in the emotion recognition definition extends the concept beyond emotion narrowly understood. Third, the ancillary exclusion for biometric categorisation is narrow: it requires the categorisation to be both ancillary to another commercial service and strictly necessary for objective technical reasons, and a deployer relying on it should record why both limbs are satisfied rather than asserting the exclusion generally.
- (10) Recital 18 AI Act indicates that the notion of emotion recognition refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement, and that it does not extend to physical states such as pain or fatigue, nor to the detection of readily apparent expressions, gestures or movements unless these are used to infer emotions. A deployer whose system is characterised as detecting states rather than emotions should record the basis for that characterisation with care, since it is the point on which the whole analysis may turn.

3.2. Determination B — the workplace and education prohibition

- (11) Article 5(1)(f) prohibits AI systems used to infer emotions of a natural person in the areas of workplace and education institutions, except where the system is intended to be put in place or on the market for medical or safety reasons. This prohibition is broad in its subject-matter and narrow in its exception, and it is the provision most likely to catch a deployer who has assumed that disclosure is sufficient.
- (12) Three features determine its application. The prohibition attaches to the area of use, not to the employment status of the individual: candidates in a recruitment process, contractors and trainees are within the workplace context as much as employees. The exception is confined to medical or safety reasons, which are not satisfied by productivity, engagement, wellbeing analytics framed as a benefit, or security in a general sense; the safety limb is directed at protecting life and health, such as monitoring a driver or operator for signs of fatigue that create physical danger. And the exception concerns

intended purpose, so a deployer relying on it should be able to show that the medical or safety purpose is the reason for deployment rather than a justification found afterwards.

3.3. Determination C — the sensitive-inference prohibition

- (13) Article 5(1)(g) prohibits biometric categorisation systems that categorise individual natural persons on the basis of their biometric data to deduce or infer race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. The prohibition does not cover labelling or filtering of lawfully acquired biometric datasets, such as images, on the basis of biometric data, nor categorisation of biometric data in the area of law enforcement.
- (14) The operative words are ‘deduce or infer’. The prohibition is not confined to systems that announce a sensitive category as their output; it reaches systems whose categorisation has the effect of deducing one. A deployer should therefore consider not only what the system reports but what can be derived from its categories in the deployment context, and should record that consideration.

3.4. Outcome of the screen

- (15) Where the screen identifies a prohibited use, the use must not proceed and no disclosure cures it. The Assessment records the determination, the reasoning and the decision taken, and the exercise ends. Where the intended use is adjacent to a prohibition but is considered to fall outside it, the reasoning for that conclusion is the single most important passage in the document and should be written accordingly.

4. Stage 2 — the Article 50(3) applicability assessment

4.1. Determination D — deployer status

- (16) Article 50(3) binds the deployer, being the entity using the system under its own authority, other than in the course of a personal non-professional activity. This allocation differs from Article 50(1) and 50(2), which bind providers, and it means that the obligation to inform exposed persons falls on the organisation operating the system in context, which is also the organisation that knows who is exposed and how they can be reached.
- (17) A provider that also operates the system in its own business is a deployer in respect of that use. A provider that only supplies the system does not bear the Article 50(3) duty, but should record what it tells deployers about the duty and about the configuration necessary to discharge it.

4.2. Determination E — Union nexus

- (18) The AI Act applies to deployers of AI systems that have their place of establishment or are located within the Union, and in defined circumstances to deployers in third countries where the output produced by the system is used in the Union. A deployer should record the basis on which it considers itself within or outside scope, and where the assessment turns on where output is used, the reasoning for that conclusion.

4.3. Determination F — the law-enforcement exception

- (19) The second sentence of Article 50(3) disapplies the information duty for systems used for biometric categorisation and emotion recognition that are permitted by law to detect, prevent or investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties and in accordance with Union law.
- (20) The exception has three cumulative conditions and a deployer relying on it must satisfy all three: an identifiable legal permission for the purpose stated, appropriate safeguards for third parties, and conformity with Union law including data protection law. The absence of a citable legal basis is determinative against the claim. The exception disapplies the information duty only; it does not

disapply Article 5, so a prohibited practice remains prohibited even where a law-enforcement purpose is asserted, save to the extent the prohibitions themselves provide otherwise.

4.4. Determination G — applicable dates

- (21) The prohibitions in Article 5 have applied since 2 February 2025. The transparency obligation in Article 50(3) applies from 2 August 2026. A deployer that began an emotion recognition or biometric categorisation deployment before those dates should assess both, since the earlier date governs the prohibition screen and the later date governs the information duty. Dates should be verified against the consolidated text of the AI Act as amended, and the date of verification recorded.

5. Outcome of the Assessment

- (22) The Assessment produces one of four outcomes, each with a defined consequence.
- Prohibited — the use falls within Article 5. It must not proceed. The Assessment is retained as the record of that determination and of the decision taken.
 - In scope — the use is permitted and the Article 50(3) information duty applies. The deployer completes the Record (ECS-AIA-50-3-RECORD), issues the information to exposed persons (ECS-AIA-50-3-NOTICE), and completes the data protection interface (ECS-AIA-50-3-DATA).
 - In scope, law-enforcement exception relied upon — the information duty is disapplied for the identified use. The Record is completed to evidence the three conditions of the exception, and the data protection obligations continue to apply in full.
 - Out of scope — the system is not an emotion recognition or biometric categorisation system as defined, the entity is not a deployer, or there is no Union nexus. The Assessment is the retained evidence of that conclusion.
- (23) An out-of-scope conclusion reached because the system falls outside the definitions is materially different from one reached because the entity is not the deployer. The first changes if the system's function changes; the second changes if the entity's role changes. They should not be recorded interchangeably.

6. Relationship with other obligations

- (24) A conclusion under this Assessment does not dispose of adjacent obligations. Emotion recognition systems and biometric categorisation systems are, in defined cases, high-risk under Annex III AI Act, engaging Chapter III obligations for providers and Article 26 obligations for deployers including, where applicable, a fundamental rights impact assessment under Article 27. Remote biometric identification is a distinct matter governed by its own provisions and is not addressed here.
- (25) The processing of biometric data for the purpose of uniquely identifying a natural person is processing of a special category of personal data under Article 9 GDPR, and inference of the categories named in Article 5(1)(g) engages Article 9 directly. The data protection analysis is not an adjunct to this Assessment but a condition of lawfulness in its own right, and is addressed in ECS-AIA-50-3-DATA.

7. Review and re-assessment

- (26) The Assessment is repeated on any of the following triggers: a change in the system's function or the categories it assigns; a change in the context of deployment, in particular any extension into a workplace or education setting; a change in the entity's role or in the Union nexus; a change in the legal basis relied upon for the law-enforcement exception; and the publication of Commission guidelines bearing on Article 5 or Article 50(3).
- (27) In the absence of a trigger the Assessment is reviewed at intervals of no more than twelve months, and a review resulting in no change is nonetheless recorded.

8. What follows the Assessment

- (28) Where the Assessment concludes that the use is permitted and the information duty applies, its determinations are the starting point for the rest of the pack. The categories and contexts identified here carry into the Record (ECS-AIA-50-3-RECORD), which evidences how exposed persons are informed and, where relied upon, the conditions of the law-enforcement exception. The information itself is drafted and evidenced under ECS-AIA-50-3-NOTICE. The lawfulness of the underlying processing, including the Article 9 GDPR analysis and any data protection impact assessment, is addressed in ECS-AIA-50-3-DATA.
- (29) Where the Assessment concludes that the use is prohibited, no further document in this pack is required. This Assessment is the retained record of the determination, and the appropriate follow-up is the decision to discontinue or not to commence the use, recorded in Section 6 of the Template.

Annex

Template for the Prohibition Screen and Applicability Assessment under Article 5 and Article 50(3) of Regulation (EU) 2024/1689 (AI Act)

Version of the Assessment	<i>Version identifier, with references to previous versions where applicable.</i>
Last update	<i>DD/MM/YYYY</i>
Prepared by	<i>Name, role and function responsible for the accuracy of this Assessment.</i>
Reviewed by	<i>Where the organisation has a data protection officer or legal function, identify who reviewed this Assessment.</i>
Classification	<i>Internal / disclosable to authorities / disclosable to customers.</i>

1. Entity, system and intended use

Entity name and establishment	<i>Legal name, registered address, and country of establishment.</i>
System name, provider and version	<i>Identify the system assessed and its provider.</i>
Intended use in plain terms	<i>What the system will be used to do, in two or three sentences a non-specialist can follow. Write this before completing the screen; a use that is hard to state plainly is often one that needs closer examination.</i>
Deployment context(s)	<i>Where and in what setting the system will operate (e.g. retail premises, contact centre, vehicle cabin, public space, recruitment process, classroom).</i>
Persons exposed	<i>Who will be exposed to the system — customers, employees, candidates, students, members of the public, others.</i>
Date of assessment	<i>DD/MM/YYYY.</i>
Consolidated text verified at	<i>Date on which the applicable provisions and dates were verified against the consolidated text of the AI Act as amended.</i>

2. Stage 1 — prohibition screen

Complete this stage first and in full. A prohibited use is not cured by disclosure and the exercise ends here.

2.1. Determination A — within the definitions

Does the system process biometric data?	<i>Yes / no, with the basis. Where no, explain what data is processed instead and why it is not biometric data.</i>
Emotion recognition system?	<i>Does the system identify or infer emotions or intentions of natural persons on the basis of biometric data? Address 'intentions' as well as emotions.</i>
Physical states distinction	<i>Where the system is characterised as detecting physical states such as pain or fatigue rather than emotions, state the basis for that characterisation and how the distinction holds in operation.</i>
Biometric categorisation system?	<i>Does the system assign natural persons to categories on the basis of biometric data? Identify every category the system can assign.</i>
Ancillary exclusion	<i>Where the ancillary exclusion is relied upon for biometric categorisation, explain why the categorisation is both ancillary to another commercial service and strictly necessary for objective technical reasons. Both limbs must be addressed.</i>
Conclusion	<i>The system is / is not an emotion recognition system; is / is not a biometric categorisation system. If neither, Article 50(3) does not apply — record and stop, subject to Section 5.</i>

2.2. Determination B — workplace and education prohibition

Is emotion inference involved?	<i>Yes / no. Where no, mark this determination not applicable.</i>
Is the area of use a workplace or education institution?	<i>Address the area of use rather than the contractual status of individuals. Recruitment, contractors, trainees and volunteers within a workplace setting should be addressed expressly.</i>
Medical or safety exception relied upon?	<i>Yes / no. Where yes, identify the medical or safety purpose precisely.</i>
Justification for the exception	<i>Explain why the purpose is genuinely medical or safety-related, directed at life or health. State expressly whether any productivity, engagement, wellbeing or general security purpose is also served, and why the medical or safety purpose is nonetheless the intended purpose.</i>
Conclusion	<i>The use is / is not prohibited under Article 5(1)(f). If prohibited, go to Section 6.</i>

2.3. Determination C — sensitive-inference prohibition

Categories assigned	<i>List every category the system can assign, including categories not used in this deployment.</i>
Do any deduce or infer a protected characteristic?	<i>Address each of race, political opinions, trade union membership, religious or philosophical beliefs, sex life and sexual orientation in turn.</i>
Derivable inferences	<i>Consider not only what the system reports but what can be deduced from its categories in this deployment context, and record that consideration.</i>
Labelling or filtering carve-out	<i>Where relied upon, explain why the activity is labelling or filtering of a lawfully acquired biometric dataset rather than categorisation of individuals.</i>
Conclusion	<i>The use is / is not prohibited under Article 5(1)(g). If prohibited, go to Section 6.</i>

2.4. Screen outcome

Screen outcome	<i>Not prohibited / prohibited under Article 5(1)(f) / prohibited under Article 5(1)(g).</i>
Reasoning where the use is adjacent to a prohibition	<i>Where the use is close to a prohibition but considered outside it, set out the reasoning in full. This is the most important passage in this Assessment.</i>
Who approved this conclusion	<i>Name and role. Where legal or data protection review was obtained, record it.</i>

3. Stage 2 — Article 50(3) applicability

Complete only where the screen outcome is 'not prohibited'.

3.1. Determination D — deployer status

Role claimed	<i>Deployer / provider / both. State the basis.</i>
Authority for use	<i>Confirm the system is used under the entity's own authority and not in the course of a personal non-professional activity.</i>
Where the entity is the provider only	<i>Record what the entity tells deployers about the Article 50(3) duty and the configuration needed to discharge it.</i>

3.2. Determination E — Union nexus

Basis of Union nexus	<i>Establishment or location in the Union, or use of the system's output in the Union. State which applies and why.</i>
Conclusion	<i>The deployer is / is not within the territorial scope of the Regulation for this use.</i>

3.3. Determination F — law-enforcement exception

Complete only where the exception is relied upon. All three conditions must be satisfied.

Use concerned	<i>Identify the specific use for which the exception is claimed.</i>
Legal permission	<i>Cite the Union or national provision permitting the use to detect, prevent or investigate criminal offences. Absence of a citable provision is determinative against the claim.</i>
Safeguards for third parties	<i>Describe the appropriate safeguards in place for the rights and freedoms of third parties.</i>
Conformity with Union law	<i>Confirm and explain conformity with Union law, including applicable data protection law. Cross-refer to ECS-AIA-50-3-DATA.</i>
Scope of reliance	<i>State precisely which uses are covered and what information duty remains for uses outside the exception.</i>

3.4. Determination G — applicable dates

Date use commenced or will commence	<i>DD/MM/YYYY.</i>
Article 5 position	<i>Confirm the prohibition screen has been applied by reference to the date the prohibitions took effect.</i>
Article 50(3) compliance date	<i>The date by which the information duty must be met for this use.</i>

4. Outcome and consequential actions

Outcome	<i>Prohibited / in scope / in scope with law-enforcement exception / out of scope.</i>
Basis of the outcome in one sentence	<i>Written so a reader who has not seen the reasoning can understand the conclusion.</i>
Records required	<i>Which of ECS-AIA-50-3-RECORD, ECS-AIA-50-3-NOTICE and ECS-AIA-50-3-DATA are required.</i>
Other obligations identified	<i>Annex III high-risk classification, Article 26 deployer obligations, Article 27 fundamental rights impact assessment, GDPR Article 9 and any data protection</i>

	<i>impact assessment, worker consultation duties, or other. Identify the owner of each.</i>
Owner and target dates	<i>Who is responsible for each consequential action and by when.</i>

5. Where the use is out of scope

Basis of the out-of-scope conclusion	<i>Outside the definitions / not a deployer / no Union nexus. State which.</i>
What would change the conclusion	<i>The change in function, role or deployment that would bring the use into scope.</i>

6. Where the use is prohibited

Complete where the screen outcome is prohibited. The purpose of this section is to record the decision taken, not to justify continuing.

Prohibition engaged	<i>Article 5(1)(f) / Article 5(1)(g).</i>
Decision taken	<i>Use not commenced / use discontinued / functionality disabled / deployment redesigned. State which, and the date.</i>
If redesigned	<i>Describe the change and confirm that this Assessment has been repeated against the redesigned use.</i>
Notification and escalation	<i>Who within the organisation was informed, and whether external advice was obtained.</i>

7. Review

Next scheduled review	<i>DD/MM/YYYY, no more than twelve months from the date of assessment.</i>
Trigger events registered	<i>The changes that would require re-assessment before that date, and how they will be detected.</i>

8. Version history and declaration

Version	Date	Nature of the change or review	Approved by

Declaration

The determinations recorded above are made in good faith and, to the best of the knowledge of the person signing, are accurate and complete as at the date of signature. Where a determination could not be made on the information available, the gap and the reason for it have been recorded in the relevant field.

Name	
-------------	--

Role	
Date	
Signature	