Rethinking biometrics in the age of AI: Navigating the regulatory landscape boosting trust, transparency, and accountability

February 2026

As artificial intelligence (AI) systems increasingly integrate biometric technologies, the traditional regulatory focus on identification is no longer sufficient. Behavioural and physiological data are now being used to profile individuals in ways that challenge existing privacy frameworks.

This article explores the evolving regulatory landscape in the EU, including the European Parliament's 2025 briefing and the AI Act, and argues for a broader, rights-based approach to biometric governance. It outlines key risks, regulatory responses, and strategic considerations for organisations deploying biometric AI, presenting a structured framework of five actionable steps for assessing and implementing biometric technologies responsibly.

In addition, it offers C-level leaders key considerations for ethical, compliant, and future-proof innovation, including crucial insights into redefining biometrics beyond identification, operationalising risk-based compliance, and embedding transparency and user empowerment.

Table of contents

Introduction

Biometric technologies are no longer confined to fingerprint scanners or basic facial recognition at border controls. In today's AI-driven world, they are embedded in systems capable to interpret everything from emotional states to behavioural patterns, potentially without the subject's consent and / or awareness. Given that many biometric applications involve processing of special category data under GDPR and the AI Act, and in some cases may even be prohibited or strictly limited, organisations need to prioritise compliance, governance, and privacy-by-design from the earliest stages of deployment. This presents a profound challenge to existing legal definitions and compliance frameworks, which remain largely focused on identification.
In this context, the European Parliament's 2025 briefing on biometrics, along with the AI Act, highlights the growing complexity in how biometric data is interpreted and regulated. how biometric data is understood and regulated. These developments signal a move toward a broader, more nuanced governance model that recognises the ethical and societal implications of biometric AI beyond mere identification.

For organisations relying on AI and biometrics, adequately managing privacy and compliance is not just a compliance issue, it's a strategic imperative. The ability to deploy biometric AI responsibly will increasingly define organisational trust, brand integrity, and market access. This article explains the regulatory trajectory, highlights potential risks, and offers actionable insights for organisations navigating this complex terrain.

Technology & biometrics in the AI era

As AI and biometrics become part of everyday business operations, staying compliant with EU regulations become essential. The table below provides a clear overview of the latest regulatory requirements and key considerations that organisations should consider to manage risk.

Regulatory body update	Compliance requirement	Key considerations
European Data Protection Board (EDPB) 2024 annual report position on responsible deployment of biometrics, transparency and oversight This report reinforces GDPR principles in the context of biometric AI, calling for stronger safeguards, transparency, and oversight.	**Transparency in biometric data processing** Organisations must ensure individuals are clearly informed when biometric data is collected or used, with accessible privacy notices and voluntary participation options.	• Develop user-centric privacy notices • Operationalise informed consent Embed transparency-by-design • Enable cross-functional collaboration • Stay ahead of regulatory updates
	Human oversight and accountability Biometric systems must be subject to meaningful human control, with trained personnel, oversight protocols, and audit trails to prevent errors and bias.	• Establish clear accountability structures • Train staff on biometrics and AI driven processes • Implement oversight mechanisms • Maintain audit trails • Adopt an AI governance maturity model
	Alignment with EU digital regulation Biometric governance should be harmonised with broader EU legislation (e.g. GDPR, AI Act), reflecting a unified, rights-based regulatory approach.	• Integrate regulatory frameworks • Embed regulatory intelligence into product development • Conduct regulatory reviews
European Parliament briefing on biometrics highlights Proposes a broader, rights-based regulatory framing of biometrics to address emerging AI risks beyond identification.	**Broader legal definition of biometrics** Calls for expanding the scope of biometric regulation to include behavioural and physiological data that impact privacy and fundamental rights.	• Reassess data classification frameworks • Update Data Protection Impact Assessments (DPIAs) • Review vendor contracts • Revise internal policies and training
	Regulation of Remote Biometric Identification (RBI) Strong restrictions on live facial recognition in public spaces, requiring prior authorisation and limited use cases to prevent mass surveillance.	• Conduct rigorous legal assessments • Perform risk assessments to the use of biometrics
	Biometric categorisation and profiling The EU Parliament highlights the risks of profiling individuals based on biometric traits, urging stricter controls to prevent discrimination and bias from opaque algorithms and unverifiable assumptions.	• Invest in algorithmic transparency tools • Implement bias mitigation techniques • Adopt fairness KPIs and reporting mechanisms
	Emotion recognition technologies The briefing criticises emotion AI for its potential misuse in sensitive contexts, recommending bans or strict limitations.	• Critically evaluate the business case • Apply strict contextual safeguards • Conduct red-teaming exercises • Consider alternative approaches
	Rights-based governance model Advocates for embedding ethical principles, transparency, and stakeholder engagement into the lifecycle of biometric AI systems.	• Embed privacy-by-design and ethics-by-design • Conduct Fundamental Rights Impact Assessments (FRIAs) • Establish internal AI ethics committees • Publish transparency and accountability reports

Regulatory body update	Compliance requirement	Key considerations
AI Act considerations The AI Act provides a structured legal framework that addresses many of the same concerns as the EDPB and EU Parliament, specifically around the ethical use of biometric technologies, transparency, and fundamental rights.	**Risk-based classification of biometric systems** Introduces a tiered risk framework for AI systems, with biometric technologies often falling under high or unacceptable risk categories.	• Map biometric use cases to risk categories • Maintain a centralised AI risk register • Align with international standards • Prepare and perform internal/external audits For high-risk systems perform Fundamental Rights Impact Assessments (FRIAs), third-party conformity assessments and post-market monitoring, where applicable.
	Transparency and documentation High-risk biometric systems must clearly inform users about purpose, performance, limits, and when they interact with or are subject to AI.	• Provide concise user documentation and instructions • Label AI interactions and AI generated content • Communicate system accuracy and key limitations • Keep technical documentation and logs for audits
	Human oversight High-risk biometric systems must allow for meaningful human intervention to prevent automation bias, discrimination, and unjustified surveillance.	• Embed human-in-the-loop mechanisms • Train personnel to monitor decisions • Create oversight playbooks, and documentation
	Regulatory alignment and governance The AI Act complements GDPR, and other EU laws, promoting a unified, rights-based framework. It also establishes the European AI Office and expert panels for oversight.	• Monitor regulatory updates • Foster a culture of responsible AI throughout your organisation
	Enforcement and penalties Noncompliance can result in fines up to €35 million or 7% of global turnover, especially for banned practices or failures in high-risk system obligations.	• Ensure board-level oversight • Test organisational readiness for regulatory investigations • Maintain defensible documentation

Biometrics in the AI era

As biometric technologies become increasingly integrated into AI-driven systems, organisations must navigate a complex landscape of technical, ethical, and regulatory challenges. The following considerations are critical for ensuring that biometric AI solutions are not only effective but also compliant, secure, and trustworthy.

- **The limits of anonymisation in biometrics**

Biometric information is inherently linked to an individual's physical or behavioural characteristics and is therefore challenging to fully anonymise. Even when identifiers are removed, advanced AI models may re-identify individuals by correlating patterns across datasets. This presents a significant challenge for data minimisation and privacy compliance, particularly under the GDPR and the AI Act. Organisations must adopt robust data governance strategies that go beyond traditional anonymisation techniques.

> Biometric information is inherently linked to an individual's physical or behavioural characteristics and is therefore challenging to fully anonymise.

- **Privacy-preserving machine learning**

To mitigate privacy risks while enabling innovation, organisations are increasingly adopting privacy-preserving technologies. Two notable approaches include:

- **Federated learning**, is a method of training AI models without centralising sensitive data. Instead of collecting biometric data (like facial images or voice recordings) in one location, the AI model is sent to where the data resides, such as on users' devices or local servers. The model learns from the data locally, and only the updated model parameters (not the raw data) are shared back to a central server. This significantly reduces the risk of data breaches or misuse, as the biometric data never leaves its original location.

- **Differential privacy**, is a technique that protects individual privacy by adding mathematical noise to datasets. This noise is carefully calibrated so that the overall patterns in the data remain useful for analysis, but it becomes difficult to trace any specific data point back to an individual.

These methods support compliance with data protection regulations and help build public trust in biometric applications.

- **Explainability and auditability of biometric AI**

Biometric systems often operate as opaque "black boxes" making it difficult to understand or challenge their outputs. The integration of explainable AI (XAI) techniques is therefore essential. XAI enhances transparency by providing clear, interpretable insights into how decisions are made. This is particularly important in high risks contexts such as law enforcement, healthcare, or financial services. It also facilitates internal audits and regulatory reporting which are increasingly expected under the AI Act.

- **Digital identity wallets: enabling privacy by design**

As biometric authentication becomes more prevalent, digital identity wallets are emerging as a privacy-enhancing solution. These secure, user-controlled tools allow individuals to store and selectively share biometric credentials, such as facial templates or age verification tokens, without exposing full profiles.
By supporting data minimisation, granular consent, and purpose limitation, ID wallets align with GDPR and AI Act requirements for transparency and user empowerment. They also enable verifiable audit trails, strengthening accountability and compliance. With the EU's upcoming European Digital Identity (EUDI) Wallet under eIDAS 2.0, these tools are being standardised for cross-border use, offering a scalable, interoperable foundation for trusted biometric AI deployment.

The practical application of these strategies will be illustrated through the use cases below, demonstrating their real-world benefits and considerations.

Biometrics in action: use cases, risks and regulatory implications

As biometric technologies become more embedded in everyday services, from healthcare to banking, their intersection with AI introduces both transformative potential and significant regulatory scrutiny. Under the EU's AI Act and GDPR, organisations deploying biometric AI must navigate a complex web of compliance obligations, ethical considerations, and technical safeguards.

Below, we explore two high-impact use cases that illustrate how these technologies are being applied in practice, the risks they pose, and the measures organisations can take to mitigate them. These illustrative examples aim to highlight real-world complexities, clarify the implications of regulatory requirements, and provide practical guidance to organisations as they implement biometric solutions in alignment with ethical and legal standards.

Case 1: Facial recognition in emergency healthcare access

In emergency medical settings, time is critical. Hospitals are increasingly exploring facial recognition systems to identify patients who are unconscious, non-verbal, or lack documentation. By linking facial data to electronic health records, healthcare practitioners can access vital information, such as chronic conditions and medical treatments, in seconds.

Regulatory classification:

This is a high-risk application under the AI Act, given its potential to significantly affect individuals' rights and safety. It also involves the processing of special categories of personal data under the GDPR, including both biometric and health data.

Key Risks:

- **Misidentification** could result in incorrect treatment or delays in care.
- **Algorithmic bias** may reduce accuracy for certain demographic groups, exacerbating health disparities.
- **Consent and data protection** are particularly challenging in emergency contexts where patients cannot provide informed consent.

Mitigation strategies:

- To conduct a **Fundamental Rights Impact Assessment (FRIA)** to evaluate the system's necessity, proportionality, and potential harms.
- Conduct a **Data Protection Impact Assessment (DPIA)** specifically addressing the privacy risks associated with using AI-driven facial recognition for patient identification.
- Implement **human-in-the-loop verification**, ensuring that medical staff can confirm that the identity matches before acting on merely AI outputs.
- Use **federated learning** to train models locally within hospital networks, reducing the need to centralise sensitive biometric data.

This use case demonstrates how biometric AI can enhance patient care, but also keeping in mind that rigorous safeguards and ethical oversight is required throughout the deployment and implementation.

Case 2: Biometric authentication and synthetic identity risks in financial services

In the financial sector, biometric authentication is rapidly becoming the norm. Banks and fintech platforms are leveraging facial recognition and voice biometrics to verify customer identity in mobile apps, ATMs, and call centres. While these technologies offer convenience and enhanced security, they are also increasingly vulnerable to synthetic identity attacks, particularly through voice cloning and image spoofing.

Regulatory classification:
These systems are classified as high-risk under the AI Act, requiring third-party conformity assessments, human oversight, and post-market monitoring. Under the GDPR, biometric data used for authentication is considered a special category of personal data, requiring explicit consent, purpose limitation, and robust security controls.

Key risks:
- **Voice cloning** technologies can replicate a customer's speech patterns with high accuracy, enabling attackers to bypass voice-based authentication systems.
- **Image spoofing** using deepfakes or high-resolution photos can deceive facial recognition systems, especially those lacking liveness detection.
- **Opacity in data processing** may leave users unaware of how their biometric data is stored, used, or shared, raising concerns under GDPR's transparency and accountability principles.

Mitigation Strategies:
- Implement **liveness detection** and anti-spoofing mechanisms to distinguish real users from synthetic imposters.
- Apply **differential privacy** to anonymise biometric data used in training, reducing the risk of re-identification, and minimising the effects of the data being intercepted in a cyber-attack.
- Ensure **clear and accessible user disclosures**, including opt-out options and the right to contest automated decisions, in line with GDPR requirements.
- Conduct a **Fundamental Rights Impact Assessment (FRIA)** to evaluate the ethical and legal implications of biometric authentication systems.
- Conduct a **Data Protection Impact Assessment (DPIA)** with particular focus on AI-driven privacy risks in biometric authentication systems

This example emphasises the need for a layered security approach, combining technical safeguards, regulatory compliance, and user awareness, to protect against the evolving threat landscape in biometric authentication.

Conclusion: leading responsibly in the age of biometric AI

As artificial intelligence continues to advance, biometric technologies are no longer limited to identification they are now embedded in systems capable of interpreting behaviour, emotions, and much more. This evolution demands a parallel transformation in governance. The European Union's AI Act, alongside the GDPR and the European Parliament's 2025 briefing, marks a pivotal shift toward a rights-based, risk-calibrated regulatory framework for AI.

For organisations, this is more than a compliance challenge, it is a strategic inflection point. The ability to deploy biometric AI responsibly will increasingly define competitive advantage, brand trust, and regulatory resilience. It also implies significant opportunities for innovation underpinning in ethics and transparency.

C-level leaders aiming to use biometrics have the challenge to embed governance, privacy, and accountability into the core architecture of biometric AI systems. Doing so will not only mitigate potential legal and reputational risk but also position their organisations as trusted stewards of emerging technologies in a rapidly evolving digital landscape.

Five key steps organisations should take to assess and/or implement biometrics

Step 0: Define the biometrics purpose and evaluate alternatives (applicable to organisations not using biometrics)

This step is particularly relevant for new biometric AI initiatives. It ensures that organisations do not implement biometric solutions without first considering its purpose, value and alternatives.

Actions:

- **Clearly define the intended purpose and business value** of the biometric application.
- **Assess whether the same objective can be achieved through less intrusive or non-biometric means**, in line with the principles of necessity and proportionality under the GDPR and AI Act.
- **Engage relevant stakeholders** early (e.g., Legal, Compliance, IT, Privacy) to evaluate feasibility, risks, and alignment with organisational values.
- **Document the rationale for selecting biometric technologies**, including expected benefits, risk trade-offs, and ethical considerations.

Key roles:

- Chief Information Officer (CIO), Chief Privacy Officer (CPO)/ Data Protection Officer (DPO), Legal and Compliance, AI Officer.

Step 1: Map and classify your biometric data

This step is relevant for **organisations already using biometrics**. Mapping and classifying biometric data is the foundation for compliance and governance. It enables organisations to identify high-risk processing, ensure lawful use, and apply appropriate safeguards under the GDPR and AI Act.

Actions:

- **Prepare an inventory all biometric data** collected or processed (e.g., facial recognition, finger prints, voiceprints, behavioural patterns analysis).
- **Map data flows** across internal systems, third-party vendors, and cloud environments, if applicable.
- **Classify personal data processing systems and activities** under the AI Act (e.g., high-risk, prohibited) and GDPR (special category data).
- **Identify cross-border data transfers** and assess compliance with updated international data transfer rules (e.g. EU-US Data Privacy Framework).
- **Document processing purposes**, legal bases, and data retention policies.

Key roles:

- Chief Information Officer (CIO), Chief Privacy Officer (CPO)/ Data Protection Officer (DPO), Legal and Compliance, Data Analyst

Step 2: Assess risks and legal compliance

Actions:

- **Conduct a Fundamental Rights Impact Assessment (FRIA)** to evaluate the system's impact on privacy, equality, and freedom. Note. This is applicable to deployers that are bodies governed by public law and operators providing high-risk AI systems.
- **Conduct a Data Protection Impact Assessment (DPIA)**, paying special attention to biometric-specific risks such as re-identification, automated decision-making, and the processing of sensitive or special category personal data.
- **Assess necessity and proportionality** of biometric use. It is important to evaluate whether the same goal can be achieved with less intrusive means.
- Prepare for AI Act obligations: third-party conformity assessments, human oversight, and post-market monitoring.
- **Align with GDPR principles**: Particularly purpose limitation, data minimisation, and lawful processing shall be reviewed and considered prior to deploying new biometrics systems.
- **Engage stakeholders** (e.g., legal, compliance, IT, HR) early to ensure cross-functional input and compliance with regulatory requirements.

Roles:

- CPO/DPO, Legal/Compliance, CEO, Privacy Officer, AI Officer

Step 3: Biometrics & technology review: Embed privacy and security by design

Based on the biometrics technical requirements used, the following actions could be used:

- **Implement federated learning** to train AI models locally without centralising sensitive biometric data.
- **Apply differential privacy** to anonymise datasets used for model training and analytics.
- **Deploy digital identity wallets** to allow users to control and selectively share biometric credentials.
- **Integrate liveness detection and anti-spoofing** to prevent deepfake and synthetic identity attacks.
- **Adopt zero-trust security architecture** to protect biometric data at rest and in transit.

Roles:

- Chief Technology Officer (CTO), CIO, CPO/DPO, Privacy Officer, AI Officer, Data Analyst, Cybersecurity Expert

Step 4: Ensure transparency, explainability and user rights

Expanded actions:

- **Integrate Explainable AI (XAI)** to provide interpretable outputs and decision rationales.
- **Maintain audit logs** of biometric processing activities for accountability and regulatory reporting.
- **Enable human-in-the-loop** decision-making in high-risk or sensitive contexts (e.g., healthcare, finance).
- **Provide clear user disclosures** about data use, rights, and risks and **enable users rights**. Inform users about the user of their biometrics data and ensure opt-out mechanisms, access, changes and deletion of their personal data are available.

Roles:

- CTO, CPO/DPO, COO (Chief Operating Officer), AI Officer, Privacy Officer, UX/UI Specialist

> Mapping and classifying biometric data enables organisations to identify high-risk processing, ensure lawful use, and apply appropriate safeguards under the GDPR and AI Act.

Step 5: Establish continuous governance and monitoring

Expanded actions:

- **Create a biometric AI governance board** with cross-functional representation (i.e. Legal, IT, Compliance, Operations).
- **Schedule periodic self-assessments / audits and bias testing** to ensure fairness, accuracy, and compliance.
- **Monitor regulatory developments** (e.g., updates to the AI Act, GDPR enforcement trends).
- **Review vendor and third-party compliance** with your biometric governance standards and ensure processors (if available) biometrics practice are aligned.
- **Continuously update risk assessments** and mitigation strategies as systems evolve.
- **Plan for adequate decommissioning** of biometric systems when applications reach end-of-life, including secure deletion, revocation of access, among others.

Roles:

- CEO, CIO/CTO, CPO/DPO, Governance Board, AI Officer

Key takeaways for organisations aiming or already implementing biometrics

- **Redefine biometrics beyond identification**

Traditional definitions of biometric data are no longer sufficient. Organisations must expand their governance frameworks to include behavioural and physiological data that, while not uniquely identifying individuals, it can also carry significant privacy and ethical implications.

- **Operationalise risk-based compliance**

The AI Act introduces a tiered risk model that mandates proactive governance. High-risk biometric systems must undergo Fundamental Rights Impact Assessments (FRIAs), third-party conformity assessments, and continuous post-market monitoring. Embedding these processes into your AI lifecycle is essential for regulatory alignment and reputational resilience.

- **Strengthen privacy and ethical safeguards**

The convergence of biometrics and AI introduces complex privacy risks, particularly in areas like facial recognition, emotion detection, and synthetic identity fraud. Implementing liveness detection, anti-spoofing technologies, and privacy-preserving techniques such as federated learning and differential privacy is critical to mitigating these threats.

- **Embed transparency and user empowerment**

Ethical AI requires more than technical robustness, it demands transparency. Organisations must provide clear disclosures, opt-out mechanisms, and avenues for individuals to contest automated decisions. These practices not only support GDPR compliance but also build trust with users and regulators alike.

- **Align with a converging global regulatory landscape**

The regulatory environment is rapidly evolving, with the AI Act, GDPR, Digital Markets Act, and international frameworks increasingly converging. Cross-border cooperation, as championed by the EDPB, underscores the need for harmonised internal policies that can adapt to global standards and ensure long-term compliance.

- **Engage C-leaders through strategic alignment and risk framing**

Ensure effective executive engagement by clearly linking biometric initiatives to strategic business priorities, quantifying the business impact of risks and opportunities, and providing concise, executive-friendly summaries of compliance and ethical considerations.

Key sources:

- European Parliament 2025 briefing on biometrics
- EU Artificial Intelligence Act (Regulation (EU) 2024/1689)
- EDPB Annual Report (2024)
- GDPR Recital 51 and Article 9 (special categories of data)

“ The regulatory environment is rapidly evolving, with the AI Act, GDPR, Digital Markets Act, and international frameworks increasingly converging.

EDPB's 2024 annual report position on responsible deployment of biometrics, transparency and oversight

The European Data Protection Board (EDPB), in its 2024 Annual Report, reaffirmed its commitment to protect fundamental rights in the context of biometric technologies. As biometric systems become increasingly embedded in AI-driven applications, the EDPB has called for stronger safeguards, greater transparency, and more robust oversight to ensure these technologies are deployed responsibly and lawfully.

Transparency and user awareness

The EDPB emphasises that transparency is essential for lawful biometric data processing. In 2024, the Board issued a consistency opinion under Article 64(2) GDPR concerning the use of biometric systems in public and semi-public environments, such as airports and retail spaces. It stressed that individuals must be:

- Clearly informed when biometric data is being collected or processed.
- Provided with accessible and understandable privacy notices, including the purpose, legal basis, and retention period.
- Offered genuine

The Board warned against the "normalisation" of biometric surveillance and urged organisations to consider less intrusive alternatives where possible.

Human oversight and accountability

Biometric systems, particularly those used for identification, categorisation, or behavioural inference, must be subject to meaningful human oversight. The EDPB highlighted the need for:

- Trained personnel capable of monitoring and intervening in automated processes.
- Oversight protocols that allow for the review and correction of errors or biased outcomes.
- Audit trails to support accountability and facilitate regulatory inspections.

These principles are reinforced by the AI Act, which mandates AI literacy of their staff and other personnel dealing with the operation and use of AI systems, human-in-the-loop mechanisms, automatic recording of events, and third-party conformity assessments for high-risk biometric systems.

Regulatory alignment and governance

The EDPB's 2024 activities reflect a broader effort to align biometric governance with the EU's digital regulatory framework. The Board actively contributed to the development of the AI Act and the draft procedural regulation for GDPR enforcement, advocating for a cohesive, rights-based approach to emerging technologies.

Key developments include:

- The launch of the EDPB's 2024–2027 strategy, which prioritises modernising enforcement, enhancing cooperation with other regulators, and addressing AI-related risks.
- Expanded guidance on legitimate interest, data transfers, and AI model training, helping organisations navigate complex compliance challenges.
- Continued emphasis on international regulatory cooperation, recognising the global nature of biometric data flows and AI deployment.

> The EDPB's 2024 activities reflect a broader effort to align biometric governance with the EU's digital regulatory framework.

EU Parliament briefing on biometrics highlights

Rethinking the scope of biometrics

According to the European Parliament briefing from March 2025, the current legal definition of biometric data, which is traditionally focused on identification (e.g. fingerprints, facial recognition), is no longer adequate to safeguard personal data in the age of AI. Many modern AI systems process behavioural or physiological data that may not uniquely identify an individual but still carry significant implications for fundamental rights such as autonomy, dignity, and freedom of expression.

For example, AI-powered surveillance systems in retail environments may track body posture, or micro-expressions to detect suspicious behaviour or emotional states. While these data points may not directly identify a person, they can still be used to profile, categorise, or target individuals, potentially leading to discriminatory outcomes, subject manipulation, among others. Such uses fall outside the traditional scope of biometric regulation, yet they pose equally serious risks to privacy and subject rights.

As the Parliament notes, “The current legal approach to biometric data in EU law, centred on the use of such data for identification purposes, overlooks numerous present and foreseeable developments that are not centred on the identification of individuals, but would nevertheless have a serious impact on their fundamental rights and on democracy.”

This evolving landscape calls for a broader conceptual and regulatory framing of biometrics, one that includes non-identifying but sensitive bodily and behavioural data processed by AI systems. The Parliament advocates for updating legal definitions and compliance frameworks to reflect this shift, ensuring that all forms of biometric processing are subject to appropriate safeguards.

Remote Biometric Identification (RBI)

Strong concerns are noted about live facial recognition in public spaces, especially when deployed without consent or judicial oversight. It warns that RBI can lead to mass surveillance, disproportionately affecting marginalised groups and undermining democratic freedoms. The AI Act reflects this by classifying real-time RBI for law enforcement as an unacceptable risk, effectively banning it except in narrowly defined scenarios, such as locating missing persons, preventing imminent terrorist threats, or identifying suspects of serious crimes, all of these requiring prior judicial or administrative authorisation.

Biometric categorisation and profiling

AI systems that classify individuals based on biometric traits, such as age, gender, or ethnicity, are flagged as high-risk due to their potential to reinforce bias and discrimination. The Parliament stresses that such systems often rely on opaque algorithms and unverifiable assumptions, making them difficult to audit or verify its source input.

Emotion recognition

The briefing is particularly critical of emotion recognition technologies, which attempt to infer emotional states from facial expressions, voice, or physiological signals. These systems pose a significant risk of being abused, for example, in recruitment, education, or policing. The Parliament calls for strict regulation or outright bans on such applications, aligning with the AI Act's cautious stance.

Policy recommendations:

The European Parliament advocates for a rights-based governance model to ensure biometric AI systems respect fundamental rights and democratic values. Key recommendations include:

- **Broader legal definitions**
  Update the legal scope of biometric data to include bodily and behavioural traits that, while not uniquely identifying, still pose significant privacy and ethical risks.
- **Mandatory risk assessments**
  Require fundamental rights impact assessments for high-risk biometric applications to evaluate potential harms before deployment.
- **Transparency**
  Ensure individuals are clearly informed when subject to biometric processing and have accessible mechanisms to challenge or appeal automated decisions.
- **Ethical and inclusive design**
  The Parliament promotes embedding privacy by design, non-discrimination, and human oversight in biometric AI. It also supports multi-stakeholder governance to ensure accountability and ethical compliance across the AI lifecycle.

> "The European Parliament advocates for a rights-based governance model to ensure biometric AI systems respect fundamental rights and democratic values.

AI Act considerations

In line with the European Parliament's 2025 briefing on biometrics, the AI Act provides a structured legal framework that addresses many of the same concerns, specifically around the ethical use of biometric technologies, transparency, and fundamental rights. While the EU Parliament's briefing offers a forward-looking, rights-based critique of biometric AI, the AI Act translates many of these principles into enforceable obligations. Together, they form a complementary foundation for regulating biometric systems in the EU, balancing innovation with the protection of individual freedoms. Here is an outline of the key AI Act considerations:

Risk-based classification

The AI Act adopts a four-tier risk model, with biometric systems frequently falling under **high-risk** or **unacceptable risk** categories:

Unacceptable risk:

These AI applications are **prohibited** due to their inherent threat to fundamental rights, democracy, and public trust. In biometrics, this includes:

- **Real-time biometric identification in public spaces** (e.g. live facial recognition), which can lead to mass surveillance and chilling effects on free expression.
- **Emotion recognition in sensitive environments**, such as schools or workplaces, where it may manipulate behaviour or reinforce bias.
- **Social scoring**, where individuals are evaluated or ranked based on behaviour or traits, often leading to discrimination or exclusion.

- These uses are banned unless narrowly justified (e.g. imminent threats), and even then, require **judicial or administrative authorisation**.

High risk:

These systems are **permitted but tightly regulated** due to their potential to significantly affect individuals' rights or safety. In biometrics, this includes:

- **Facial recognition for law enforcement or border control,** where misuse could lead to wrongful identification or profiling.
- **Biometric access to essential services**, such as healthcare or banking, where errors or bias could deny critical services.

Requirements include:

- **Fundamental Rights Impact Assessments (FRIAs)**
  Before deploying high-risk biometric systems, "deployers that are bodies governed by public law or private operators providing public services, as well as operators providing high-risk AI systems" must conduct a FRIA to evaluate potential impacts on rights such as privacy, equality, and access to services. This includes identifying risks, justifying the system's necessity, and outlining safeguards. FRIAs must be updated if the system evolves or new risks emerge.

- **Third-party conformity assessments**: Under the AI Act, providers of high-risk **biometric systems** must perform **third-party conformity assessments** before rolling it out on the market. These assessments verify that the system complies with legal requirements around data quality, transparency, human oversight, and risk mitigation. The process ensures that only **safe, lawful, and rights-respecting** biometric technologies are deployed.

- **Human oversight mechanisms** to prevent automation bias. Trained personnel must be able to monitor, intervene in, or override automated decisions. Oversight ensures accountability, prevents automation bias, and helps detect errors or discriminatory outcomes in real time.

- **Post-market monitoring** to detect emerging risks. Once deployed, biometric AI systems are subject to **continuous monitoring obligations** to detect and address emerging risks. Providers must implement mechanisms for **incident reporting**, performance tracking, and user feedback collection. This ensures that systems remain compliant and safe over time, especially as real-world conditions evolve. It also supports **regulatory oversight and public trust** in biometric technologies.

These safeguards aim to ensure that high-risk systems are transparent, accountable, and fair.

Limited risk:

These systems pose **moderate risks** and are subject to **transparency obligations** rather than full regulatory scrutiny. Examples include:

- **Demographic analysis tools** that estimate age or gender from facial features for marketing or UX purposes.
- **Behavioural analytics** that track non-identifying traits (e.g. posture or gaze) in non-sensitive contexts.

Obligations include:

- **Clear user notification** that AI is in use
- **Instructions for safe and appropriate use**
- **Opt-out options**, where feasible

While not inherently harmful, these systems can still influence perceptions or decisions and must be deployed responsibly.

Minimal Risk:

Applies to **low-impact systems** with negligible effects on rights or safety. These are exempt from specific regulatory obligations, however, ethical design is encouraged. For instance, spam filters, basic chatbots that don't process sensitive data and AI-generated media without biometric analysis.

Although regulation is minimal, developers are encouraged to follow **voluntary codes of conduct** and ensure systems are not repurposed for higher-risk uses.

Transparency and user awareness

The Act mandates that users must be clearly informed when interacting with AI systems, particularly those that simulate human behaviour or generate synthetic content. This is especially relevant in biometric contexts, where individuals may be unaware of being analysed or categorised.

Human Oversight

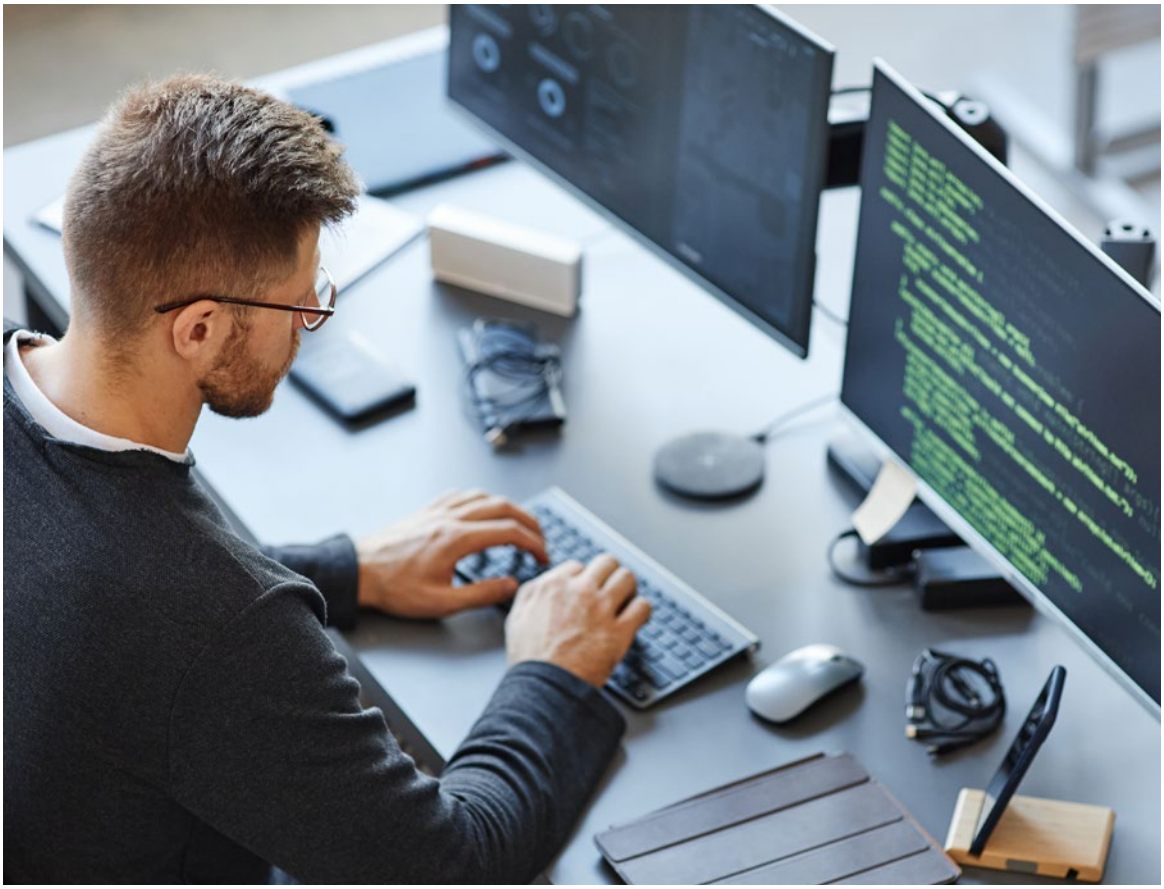
High-risk biometric systems must be designed to ensure meaningful human oversight. This includes the ability to monitor, intervene, and override automated decisions, a safeguard against automation bias, discrimination, and unjustified surveillance.

Regulatory alignment and governance

The AI Act complements existing EU laws such as the GDPR and Digital Markets Act, reinforcing the Parliament's call for a cohesive, rights-based regulatory framework. It also establishes the European AI Office and a scientific expert panel to support enforcement and monitor systemic risks.

Enforcement and penalties

Noncompliance with the AI Act can result in fines of up to €35 million or 7% of global annual turnover, particularly for the use of banned practices or failure to meet obligations for high-risk systems. This underscores the importance of robust governance, especially in the deployment of biometric technologies.



Contact

Stephanie Rojas Diestra
Author
Manager Cybersecurity and Privacy
E: stephanie.rojas.d.diestra@pwc.com

Bram van Tiel
Partner Cybersecurity,
resilience & privacy,
PwC Netherlands
E: bram.van.tiel@pwc.com