AI & Partners

Amsterdam - London - Singapore

EU AI Act

Overseeing Biometric Identification

How the world's first comprehensive legislation on artificial intelligence (AI) legislation safeguards digital identity wallet users by imposing regulatory restrictions on biometric identification.

April 2025

AI & Partners

AI & Partners

Amsterdam – London - Singapore

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/.

Contact: Michael Charles Borrelli | Director | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

Our analysis highlights that organizations operating across diverse sectors must ensue alignment with biometric identification requirements when utilising or providing digital identity wallets. These requirements reinforce trust in biometric systems within digital identity wallets, emphasizing the need to integrate privacy, transparency, and accountability into organizational processes and digital tools biometric systems within digital identity wallets. Adhering to biometric requirements is also essential to advancing inclusive digital societies, where AI technologies are increasingly developed and deployed responsibly, due to individuals' health, safety, and fundamental rights.

About this report

This report is based on market research, publicly available data, and interviews with AI specialists in AI & Partners, financial services organisations, and relevant third-parties. Moreover, quotations provided on specific topics reflect those of AI specialists at AI & Partners to be as representative as possible of real-world conditions. All references to EU AI Act reflect the version of text valid as at 13 June 2024. Accessible here.

Contents

Executive Summary

The European Union's ("EU") Artificial Intelligence ("AI") Act ("EU AI Act")[1], which entered into force earlier this year on 1st August 2024, regulates how organisations use, develop, deploy, and market AI in the EU. It improves the safety, security, and trustworthiness of AI systems and, among other things, requires organisations to implement risk management systems for high-risk AI systems. It can be difficult and costly to comply with. Penalties for non-compliance can be as high as €35m or 7% of annual global turnover, whichever is higher.

Overview

The regulation is set to be supervised and enforced by the national competent authorities ("NCAs") in each member state. The European Data Protection Board ("EDPB"), which is made up of representatives from each EU Member State, AI Office ("AIO"), the European Data Protection Supervisor ("EDPS"), and others ensures that EU AI Act will be applied consistently throughout the EU.

The whitepaper examines the integration of biometric identification within EU Digital Identity Wallets and the regulatory oversight provided by the EU AI Act. This intersection is pivotal as it addresses the balance between technological innovation and the protection of privacy and fundamental rights in the digital era. The EU AI Act classifies biometric identification systems as high-risk, necessitating stringent regulatory measures to ensure these systems are used responsibly and ethically.

Purpose

The primary objective of this whitepaper is to explore the regulatory framework established by the EU AI Act for biometric identification in digital identity systems. This framework is essential due to the sensitive nature of biometric data, which includes physical, physiological, and behavioural characteristics used to identify individuals. The whitepaper aims to elucidate how these regulations safeguard personal data and protect fundamental rights, ensuring that digital identity systems are secure, transparent, and trustworthy.

Key Findings

1. High-Risk Classification and Regulatory Safeguards

Biometric identification systems, particularly those used in digital identity wallets, are classified as high-risk under the EU AI Act. This classification is due to their potential impact on privacy and fundamental rights, necessitating comprehensive safeguards. The Act mandates transparency, data protection, and human oversight to ensure these systems are used ethically.

2. Fundamental Rights Impact Assessment

Deployers of high-risk AI systems must conduct a fundamental rights impact assessment to evaluate and mitigate potential risks to individuals' rights. This assessment is crucial for ensuring that the deployment of biometric identification systems considers the impact on privacy and data protection.

[1] European Parliament and The Council of the European Union, (2024), 2024/1689 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), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last accessed 10th July 2024)

3. Data Governance and Protection

The Act requires high-risk AI systems to adhere to strict data governance practices, ensuring that personal data is handled with appropriate safeguards to prevent bias and protect privacy. This includes measures to detect, prevent, and mitigate possible biases that could negatively impact fundamental rights.

4. Compliance and Enforcement

The EU AI Act outlines clear compliance and enforcement mechanisms, including the requirement for deployers to cooperate with competent authorities and submit annual reports on the use of biometric systems. This ensures ongoing oversight and accountability 5. Deployers must also inform individuals when they are subject to the use of high-risk AI systems.

5. Prohibited Practices and Restrictions

Certain uses of biometric identification, such as real-time remote identification in public spaces for law enforcement, are prohibited unless specific conditions are met. This highlights the sensitivity of biometric data use and the need for careful regulation. The Act prohibits indiscriminate surveillance and requires prior authorization for the use of such systems.

6. Enhanced Security and Trust

By regulating biometric identification, the EU AI Act aims to enhance the security and trustworthiness of digital identity systems, ensuring they are used responsibly and ethically. This regulatory framework not only safeguards individuals but also promotes the development of trustworthy AI technologies.

7. Innovation and Compliance

While fostering innovation, the Act ensures that new technologies comply with existing data protection laws, creating a balanced approach to technological advancement and rights protection. This balance is crucial for fostering inclusive digital societies supported by AI.

In conclusion, the EU AI Act provides a robust framework for overseeing biometric identification in digital identity wallets, focusing on transparency, data protection, and fundamental rights. This regulatory approach is essential for fostering trust in digital identity systems while safeguarding individuals' privacy and rights. The whitepaper emphasizes the importance of these regulations in promoting the uptake of trustworthy AI and ensuring the protection of fundamental rights across various sectors.

Introduction

Background: EU Digital Identity Wallets and Biometric Identification

The European Union (EU) is at the forefront of digital transformation, aiming to provide its citizens, residents, and businesses with secure and efficient digital services. A cornerstone of this initiative is the EU Digital Identity Wallet, a digital tool designed to facilitate seamless access to public and private services across the EU. These wallets allow individuals to prove their identity and manage personal information digitally, enhancing convenience and security in an increasingly digital world.

Biometric identification plays a crucial role in the functionality of the EU Digital Identity Wallet. This technology involves the automated recognition of individuals based on their unique physical, physiological, or behavioral characteristics, such as facial images or fingerprints 1. By integrating biometric identification, digital identity wallets offer a robust mechanism for verifying identity, reducing the risk of fraud, and ensuring that only authorized individuals can access sensitive information or services.

The EU AI Act provides a comprehensive regulatory framework for the use of biometric identification within digital identity systems. It classifies biometric identification systems as high-risk due to their potential impact on privacy and fundamental rights 2. This classification subjects these systems to stringent requirements, including transparency, data protection, and human oversight, to ensure they are used responsibly and ethically.

Problem Statement: Issues and Opportunities

The integration of biometric identification in digital identity systems presents both challenges and opportunities. On one hand, biometric technologies enhance security and user convenience by providing a reliable means of identity verification. On the other hand, they raise significant privacy and data protection concerns due to the sensitive nature of biometric data.

Challenges:

- **Privacy and Data Protection**: Biometric data is inherently sensitive, and its misuse can lead to significant privacy violations. The potential for unauthorized access or data breaches necessitates robust data protection measures.
- **Bias and Discrimination**: Biometric systems can produce biased results, leading to discriminatory effects, particularly concerning age, ethnicity, race, sex, or disabilities. Ensuring fairness and accuracy in these systems is a critical challenge.
- **Regulatory Compliance**: The classification of biometric systems as high-risk under the EU AI Act imposes stringent compliance requirements. Providers and deployers must navigate complex regulatory landscapes to ensure adherence to transparency, data protection, and human oversight obligations.

Opportunities:

- **Enhanced Security**: Biometric identification offers a high level of security, reducing the risk of identity theft and fraud. This technology can significantly enhance the security of digital identity systems, fostering trust among users.

- **User Convenience**: By enabling seamless and secure access to services, biometric identification enhances user experience and convenience. This can drive the adoption of digital identity systems across the EU.
- **Innovation and Growth**: The development and deployment of biometric technologies can spur innovation and economic growth, positioning the EU as a leader in digital transformation.

'Quantum safety awareness aligned with securing digital identity', Cystel

The EU AI Act's biometric rules spotlight the urgency of quantum safety awareness. Existing encryption securing digital identity wallets risks obsolescence as quantum computing advances. Specialised quantum safety is needed to bridge this gap, such as quantum safety audits, post quantum cryptography migration, and expert guidance to fortify systems, ensure compliance, and pre-empt breaches in a post-quantum threat landscape.

> **'Quantum safety now a priority'**
>
> *"With quantum threats looming, awareness of vulnerabilities in digital identity systems is urgent. Quantum safety isn't optional—it's a compliance priority. Proactive quantum safe roadmaps and audits ensures organisations future-proof biometric frameworks and align with EU AI Act mandates before 2025's regulatory enforcement."*
>
> **Dr. Meera Sarma***, Founder/CEO,* Cystel

CYSTEL

Scope: Coverage of the Whitepaper

This whitepaper aims to provide a comprehensive analysis of the regulatory framework established by the EU AI Act for biometric identification in digital identity wallets. It will cover the following key areas:

1. Regulatory Framework:

- Examination of the EU AI Act's provisions related to biometric identification, including the classification of high-risk systems and the associated compliance requirements.
- Analysis of the transparency, data protection, and human oversight measures mandated by the Act to safeguard individuals' rights.

2. Impact on Fundamental Rights:

- Exploration of the potential impact of biometric identification on privacy and fundamental rights, including issues related to bias and discrimination.
- Discussion of the safeguards and measures in place to mitigate these risks and ensure the ethical use of biometric technologies.

3. Implementation and Compliance:

- Overview of the obligations of providers and deployers of high-risk AI systems, including the need for fundamental rights impact assessments and ongoing compliance monitoring.
- Case studies and examples of best practices in implementing biometric identification systems in digital identity wallets.

4. Future Directions and Recommendations:

- Identification of emerging trends and future directions in biometric identification and digital identity systems.
- Recommendations for policymakers, developers, and deployers to enhance the safe and effective use of biometric technologies in digital identity systems.

Biometric Identification and the EU AI Act

Definitions

Biometric Data

Biometric data refers to personal data obtained through specific technical processes related to a natural person's physical, physiological, or behavioral characteristics. Examples include facial images and fingerprints, which uniquely identify individuals. Because of its direct link to personal identity, biometric data is inherently sensitive and carries significant privacy implications if misused. The EU AI Act acknowledges this sensitivity by categorizing biometric data as a special category of personal data, necessitating robust protection measures to safeguard individual privacy and prevent misuse.

Biometric Identification

Biometric identification involves the automated recognition of human features to establish an individual's identity. This process compares a person's biometric data with a database of stored information, distinguishing it from biometric verification, which involves one-to-one comparisons. Biometric identification typically employs one-to-many comparisons, making it a powerful but privacy-sensitive tool. The EU AI Act defines biometric identification as the automated recognition of physical, physiological, or behavioral characteristics, such as facial recognition, to confirm identity by matching biometric data against stored records. While effective for verifying identity, the method raises substantial ethical and legal concerns, particularly around privacy and misuse.

High-Risk AI Systems

High-risk AI systems are those with significant potential to impact health, safety, or fundamental rights. Under the EU AI Act, these systems are classified as high-risk based on their intended use and potential societal impact. Applications such as biometric identification are included due to the grave consequences of errors or misuse in these domains. High-risk AI systems are subject to stringent regulatory measures, including requirements for transparency, robust data protection, and human oversight, to mitigate associated risks and ensure ethical deployment.

Regulatory Framework

Classification of Biometric Identification Systems as High-Risk

The EU AI Act classifies biometric identification systems, particularly those used for remote identification, as high-risk because of their potential impact on fundamental rights, health, and safety. This classification is critical for promoting responsible development and deployment while implementing safeguards to protect individual rights and privacy.

High-Risk Classification Criteria

Remote biometric identification systems, which identify individuals without their active participation, are explicitly categorized as high-risk. These systems often involve comparing biometric data against databases and include applications such as biometric categorization and emotion recognition. Both are deemed high-risk due to their potential to infringe on fundamental rights. Systems are classified as high-risk if they pose significant risks to health, safety, or fundamental rights or if they materially influence decision-making processes. Certain biometric systems used solely for verification purposes, where risks are minimal, may not fall under this classification. However, systems involving profiling or categorization based on sensitive attributes are consistently classified as high-risk.

'High-risk classification central to bias mitigation', Cyber Security Unity

The EU AI Act provides a strong framework for regulating biometric identification, ensuring transparency, data protection, and accountability. Through classifying biometric systems as high-risk, the Act enforces strict compliance to prevent misuse and bias. It promotes secure, innovative AI solutions while safeguarding fundamental rights, fostering public trust, and enhancing security.

> **'EU AI Act Supports responsible AI development'**
>
> *"The EU AI Act sets a new standard for biometric identification, as it enhances security and trust while enforcing transparency, privacy, and accountability to ensure ethical and responsible AI development."*
>
> Lisa Ventura MBA, *Founder,* Cyber Security Unity

Implications of High-Risk Classification

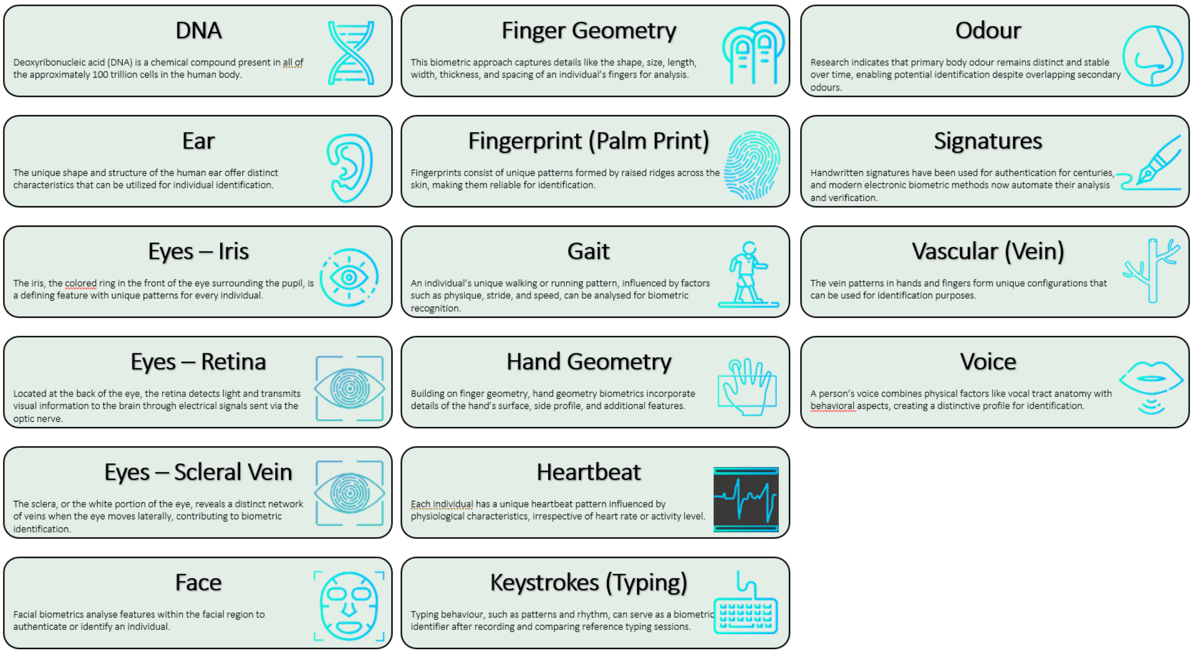
High-risk AI systems must adhere to rigorous regulatory requirements, including transparency, data protection, and human oversight. Providers and deployers are mandated to conduct fundamental rights impact assessments to identify and mitigate risks. These systems must be designed to enable effective human oversight, ensuring that decisions made by AI can be reviewed and overridden when necessary. Transparency is essential to help users understand and properly use system outputs. Additionally, high-risk systems are required to follow strict data governance practices to protect personal data, prevent bias, and ensure compliance with data protection laws. Biometric data, in particular, demands enhanced safeguards to avoid unauthorized use or exploitation.

Deployers of high-risk systems are obligated to work with competent authorities and provide regular reports on their systems' use, fostering accountability and ongoing regulatory oversight. The EU AI Act permits Member States to introduce stricter national laws governing biometric identification systems and explicitly prohibits certain applications, such as real-time remote biometric identification in public spaces for law enforcement, unless strict conditions like prior authorization and fundamental rights assessments are met.

While the high-risk classification imposes additional regulatory burdens, it serves a broader purpose by fostering public trust and promoting responsible AI use. These measures encourage the adoption of trustworthy AI technologies, ensuring innovation aligns with societal values and rights protection. This balance is crucial for building inclusive and ethical digital societies.

Types of Biometrics

The following list from The Biometrics Institute[2] indicates what's captured:



DNA

Deoxyribonucleic acid (DNA) is a chemical compound present in all of the approximately 100 trillion cells in the human body.

Ear

The unique shape and structure of the human ear offer distinct characteristics that can be utilized for individual identification.

Eyes – Iris

The iris, the colored ring in the front of the eye surrounding the pupil, is a defining feature with unique patterns for every individual.

Eyes – Retina

Located at the back of the eye, the retina detects light and transmits visual information to the brain through electrical signals sent via the optic nerve.

Eyes – Scleral Vein

The sclera, or the white portion of the eye, reveals a distinct network of veins when the eye moves laterally, contributing to biometric identification.

Face

Facial biometrics analyse features within the facial region to authenticate or identify an individual.

Finger Geometry

This biometric approach captures details like the shape, size, length, width, thickness, and spacing of an individual's fingers for analysis.

Fingerprint (Palm Print)

Fingerprints consist of unique patterns formed by raised ridges across the skin, making them reliable for identification.

Gait

An individual's unique walking or running pattern, influenced by factors such as physique, stride, and speed, can be analysed for biometric recognition.

Hand Geometry

Building on finger geometry, hand geometry biometrics incorporate details of the hand's surface, side profile, and additional features.

Heartbeat

Each individual has a unique heartbeat pattern influenced by physiological characteristics, irrespective of heart rate or activity level.

Keystrokes (Typing)

Typing behaviour, such as patterns and rhythm, can serve as a biometric identifier after recording and comparing reference typing sessions.

Odour

Research indicates that primary body odour remains distinct and stable over time, enabling potential identification despite overlapping secondary odours.

Signatures

Handwritten signatures have been used for authentication for centuries, and modern electronic biometric methods now automate their analysis and verification.

Vascular (Vein)

The vein patterns in hands and fingers form unique configurations that can be used for identification purposes.

Voice

A person's voice combines physical factors like vocal tract anatomy with behavioral aspects, creating a distinctive profile for identification.

[2] The Biometrics Institute (**2024**), 'Types of Biometrics', accessible at: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/ (last accessed 2nd December 2024)

Requirements for High-Risk AI Systems

Transparency and Information

The EU AI Act mandates stringent transparency requirements for high-risk AI systems to promote their ethical and responsible use. These measures are designed to equip deployers with the necessary tools to understand, interpret, and manage such systems effectively. High-risk AI systems must be developed with transparency in mind, ensuring that deployers can interpret outputs and comply with obligations under the Act. This includes providing clear, accessible, and comprehensive instructions detailing the system's intended purpose, accuracy, robustness, and cybersecurity measures. Additionally, these instructions must outline the system's capabilities and limitations, offering deployers a complete understanding of operational constraints and performance benchmarks.

Performance-related information, such as the system's tested levels of accuracy, robustness, and cybersecurity, must be disclosed. Any circumstances that could impact these metrics, as well as performance variations for specific groups or individuals, must also be explicitly stated. To ensure accountability, human oversight measures must be embedded into the system design, allowing deployers to monitor, interpret, and manage the system's operation. Furthermore, detailed data input specifications, including training, validation, and testing datasets, must be provided, highlighting the system's data requirements and potential limitations.

The Act also requires that deployers be notified of pre-identified changes to the system's performance or functionality, ensuring they remain informed of updates that could affect operations. Logging mechanisms are another critical requirement, enabling deployers to collect, store, and interpret operational data in line with regulatory expectations. These comprehensive transparency measures empower deployers to mitigate risks, uphold fundamental rights, and ensure the responsible use of high-risk AI systems.

Data Protection and Privacy

The EU AI Act establishes a robust framework to safeguard user privacy and protect fundamental rights, particularly for high-risk AI systems that handle sensitive data, such as biometric identifiers. High-risk systems must rely on high-quality datasets that are relevant, representative, and as error-free as possible. Data governance practices must address every stage of data handling, including collection, annotation, and preparation, to minimize bias and ensure appropriateness for the AI system's intended purpose.

To further safeguard fundamental rights, providers may process sensitive personal data, such as biometric information, strictly for bias detection and correction. Such processing must be accompanied by robust safeguards, including strict access controls, advanced security measures, and limitations on data reuse. Transparency also plays a critical role, as systems must be designed to provide deployers with clear instructions and information about capabilities and limitations, enabling them to use the systems responsibly. Human oversight mechanisms are essential to minimize risks to health, safety, and fundamental rights, allowing for effective monitoring and intervention.

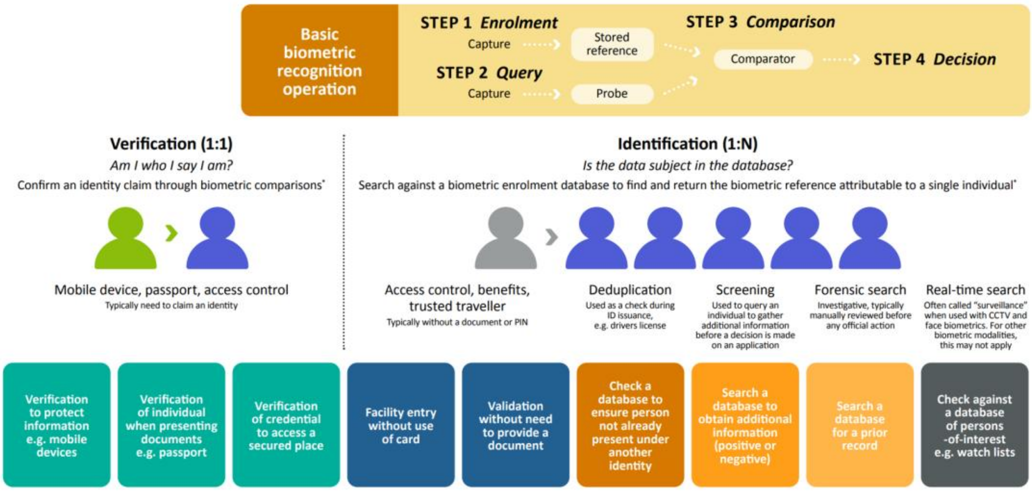
The Act mandates that deployers conduct data protection impact assessments to evaluate and address privacy risks. These assessments must be updated when changes occur in the system's use or context, ensuring ongoing protection of user data. High-risk systems must implement cutting-edge security measures, such as encryption and pseudonymization, to maintain data integrity and confidentiality.

Additionally, providers and deployers are required to maintain operational logs for an appropriate duration to ensure compliance with data protection regulations.

Certain practices, such as real-time remote identification in public spaces for law enforcement, are strictly regulated and permissible only under specific conditions, including prior authorization and the completion of fundamental rights impact assessments. Profiling or categorization based on sensitive attributes is classified as high-risk and subject to strict oversight. These measures collectively ensure that data protection and privacy are prioritized in the design and deployment of high-risk AI systems..

For an infographic on how biometrics work, see **Figure 1** below.

Figure 1: Verification and Identification: Basic Operating Protocols[3]



Basic biometric recognition operation

STEP 1 *Enrolment*
Capture → Stored reference

STEP 2 *Query*
Capture → Probe

STEP 3 *Comparison*
Comparator → STEP 4 *Decision*

Verification (1:1)
Am I who I say I am?
Confirm an identity claim through biometric comparisons*

Mobile device, passport, access control
Typically need to claim an identity

Identification (1:N)
Is the data subject in the database?
Search against a biometric enrolment database to find and return the biometric reference attributable to a single individual*

Access control, benefits, trusted traveller
Typically without a document or PIN

Deduplication
Used as a check during ID issuance, e.g. drivers license

Screening
Used to query an individual to gather additional information before a decision is made on an application

Forensic search
Investigative, typically manually reviewed before any official action

Real-time search
Often called "surveillance" when used with CCTV and face biometrics. For other biometric modalities, this may not apply

Verification to protect information e.g. mobile devices

Verification of individual when presenting documents e.g. passport

Verification of credential to access a secured place

Facility entry without use of card

Validation without need to provide a document

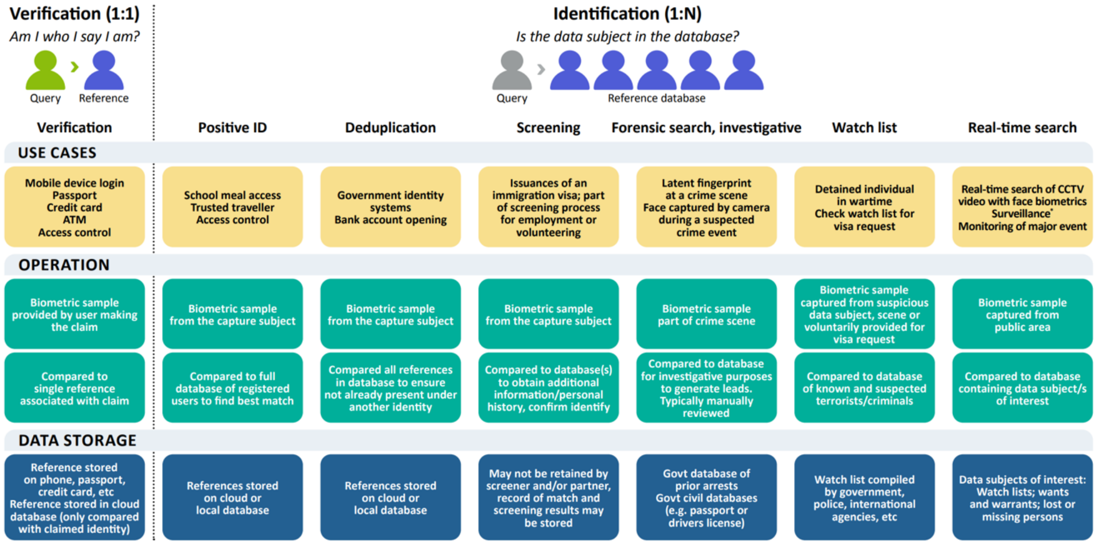
Check a database to ensure person not already present under another identity

Search a database to obtain additional information (positive or negative)

Search a database for a prior record

Check against a database of persons -of-interest e.g. watch lists

Figure 1: Verification and Identification: Use cases, operating models, and data management[3]



Verification (1:1)
Am I who I say I am?
Query › Reference

Identification (1:N)
Is the data subject in the database?
Query › Reference database

	Verification	Positive ID	Deduplication	Screening	Forensic search, investigative	Watch list	Real-time search
USE CASES	Mobile device login Passport Credit card ATM Access control	School meal access Trusted traveller Access control	Government identity systems Bank account opening	Issuances of an immigration visa; part of screening process for employment or volunteering	Latent fingerprint at a crime scene Face captured by camera during a suspected crime event	Detained individual in wartime Check watch list for visa request	Real-time search of CCTV video with face biometrics Surveillance* Monitoring of major event
OPERATION	Biometric sample provided by user making the claim	Biometric sample from the capture subject	Biometric sample from the capture subject	Biometric sample from the capture subject	Biometric sample part of crime scene	Biometric sample captured from suspicious data subject, scene or voluntarily provided for visa request	Biometric sample captured from public area
	Compared to single reference associated with claim	Compared to full database of registered users to find best match	Compared all references in database to ensure not already present under another identity	Compared to database(s) to obtain additional information/personal history, confirm identify	Compared to database for investigative purposes to generate leads. Typically manually reviewed	Compared to database of known and suspected terrorists/criminals	Compared to database containing data subject/s of interest
DATA STORAGE	Reference stored on phone, passport, credit card, etc Reference stored in cloud database (only compared with claimed identity)	References stored on cloud or local database	References stored on cloud or local database	May not be retained by screener and/or partner, record of match and screening results may be stored	Govt database of prior arrests Govt civil databases (e.g. passport or drivers license)	Watch list compiled by government, police, international agencies, etc	Data subjects of interest: Watch lists; wants and warrants; lost or missing persons

[3] The Biometric institute, (2024), 'Verification (1:1) and identification (1:n) explanatory graphics', accessible at: https://www.biometricsinstitute.org/verification-11-and-identification-1n-explanatory-graphics/ (last accessed 2nd December 2024)

Governance and Compliance

National and EU-Level Oversight

The EU AI Act establishes a robust governance framework to ensure the development, deployment, and monitoring of AI systems, particularly those classified as high-risk, in ways that protect public interest and uphold fundamental rights. This framework relies on collaboration between national competent authorities and EU-level bodies, each fulfilling distinct but complementary roles in compliance monitoring and enforcement.

At the national level, competent authorities are tasked with market surveillance and enforcement, ensuring that AI systems within their jurisdictions meet regulatory standards. They focus especially on high-risk systems that pose threats to health, safety, or fundamental rights. These authorities have the power to evaluate AI systems, enforce corrective actions for non-compliance, and even restrict or withdraw non-compliant systems from the market. To promote harmonized enforcement, national authorities must coordinate with related bodies, such as data protection agencies, sharing information and conducting joint investigations when AI systems impact multiple sectors. They are also obligated to notify the European Commission and other Member States of significant findings, especially when issues extend beyond their national borders.

National authorities are further empowered to request and access critical documentation, including technical and training data, to assess compliance. If documentation proves inadequate, they can conduct independent tests to ensure the system adheres to EU standards. They are also responsible for addressing complaints regarding potential violations of the AI Act, investigating concerns raised by stakeholders, and implementing enforcement measures where needed.

EU-level oversight is led by the European Commission, supported by the AI Office, which ensures consistent implementation of the AI Act across Member States. The Commission has exclusive authority over certain aspects, such as supervising general-purpose AI models, while the AI Office provides guidance, fosters cooperation among national authorities, and acts as a hub for information sharing. Through mechanisms like the Union safeguard procedure, the Commission can evaluate and harmonize national measures, requiring Member States to adopt uniform enforcement actions when justified.

Additionally, the Commission and AI Office offer training, resources, and guidance to national authorities, helping them build expertise and adopt best practices for enforcement. They work to establish shared criteria and benchmarks for interpreting and applying the Act consistently across the EU. The EU bodies also engage internationally, cooperating with other countries and organizations to align regulations and address cross-border challenges.

Together, the collaboration between national and EU-level entities ensures that the AI Act is implemented effectively and uniformly, safeguarding fundamental rights while fostering the responsible use of AI technologies.

AI EUROPEAN **ARTIFICIAL**
INTELLIGENCE OFFICE

Database and Registration

The EU AI Act also introduces a comprehensive framework for the registration and oversight of high-risk AI systems, centered around an EU-wide database. This framework enhances transparency, accountability, and compliance by systematically recording and managing information about such systems.

Providers or their authorized representatives must register high-risk AI systems in the EU database before they are placed on the market or deployed. This applies to all systems classified under Annex III of the Act, with limited exceptions. Registration requires providers to submit key details, such as their contact information and a clear description of the system's purpose and fundamental rights impact assessments. Deployers, including public authorities using these systems, must also register their applications and provide relevant operational information.

The database has both public and secure sections to balance transparency and security. High-risk systems used in sensitive areas like law enforcement or border control are stored in a restricted section, accessible only to the European Commission and national authorities. For other systems, publicly accessible information ensures accountability and allows stakeholders to verify compliance. Providers of non-high-risk systems may also voluntarily register, contributing to a comprehensive view of AI usage across the EU.

Serving as a centralized repository, the EU database streamlines the collection, processing, and dissemination of information for regulatory oversight. Its design prioritizes accessibility, offering user-friendly and machine-readable interfaces to ensure stakeholders can easily access relevant data. By maintaining detailed records, the database enhances transparency, supports market surveillance, and ensures compliance with the Act. It allows regulators to track the deployment and operational status of high-risk AI systems, including updates, recalls, or modifications, enabling timely interventions to mitigate risks.

The database also plays a vital role in regulatory compliance by providing a platform for providers and deployers to demonstrate adherence to legal standards. It supports authorities in identifying non-compliance and monitoring the broader impact of AI technologies on health, safety, and fundamental rights. By offering technical and administrative assistance, the Commission helps ensure the seamless operation of this registration process.

In summary, the EU database is a cornerstone of the Act's governance framework. It not only facilitates transparency and accountability but also strengthens the enforcement mechanisms that protect fundamental rights and build trust in AI technologies across the EU..

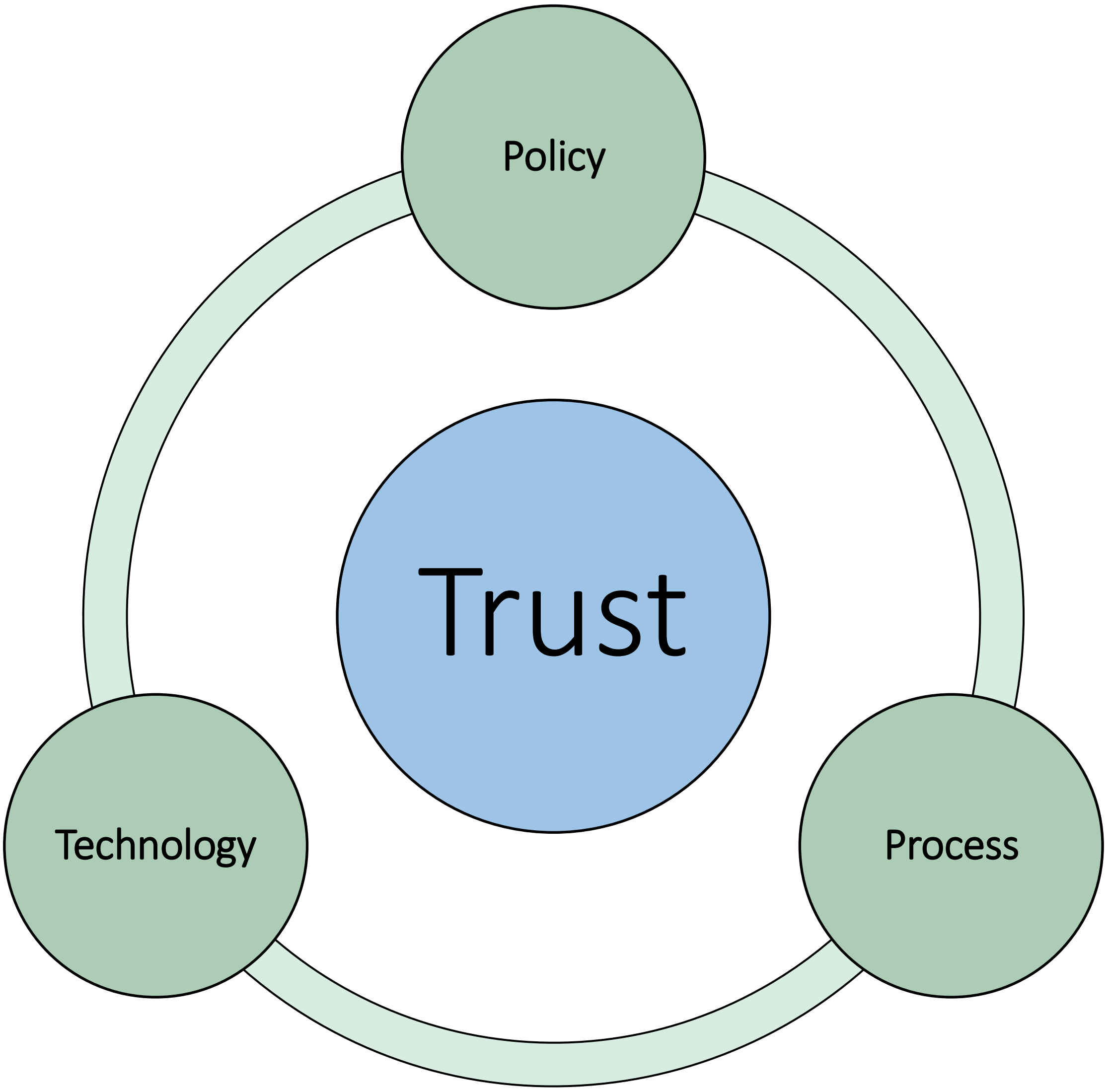
Three Laws of Biometrics

Leveraging the work of The Biometrics Institute[4], which uses Asimov's *Three Laws of Robotics* as its inspiration, firms should use biometrics while remembering the fundamentals of applying the technology responsibly and ethically to align with the EU AI Act.

The three laws of biometrics are:

- POLICY – comes first: Any use of biometrics is proportionate, with basic human rights, ethics and privacy at its heart.
- PROCESS – follows policy: Safeguards are in place to ensure decisions are rigorously reviewed, operations are fair and operators are accountable.
- TECHNOLOGY – guided by policy and process: Know your algorithm, biometric system, data quality and operating environment and mitigate vulnerabilities, limitations and risks.

Figure 2: The Three Laws of Biometrics



[4] The Biometrics Institute (**2024**), 'The Three Laws of Biometrics', accessible at: https://www.biometricsinstitute.org/the-three-laws-of-biometrics/ (last accessed 2nd December 2024)

Challenges and Considerations

Ethical and Legal Concerns

Biometric identification systems, especially those integrated into digital identity wallets, raise complex ethical and legal challenges. These challenges are rooted in privacy concerns, risks of misuse, and implications for fundamental rights. Recognizing these risks, the EU AI Act classifies biometric identification systems as high-risk and mandates stringent regulatory measures to mitigate their potential harm.

‘Biometric identification presents specific regulatory challenges’

“Biometric identification is rapidly becoming integral to digital transactions, with the value of biometrically secured payments projected to surge by over 640%—from $404 billion in 2020 to surpassing $3 trillion by 2025, according to Juniper Research. Yet, this rapid adoption presents specific regulatory challenges under the EU AI Act, which explicitly categorises biometric identification systems as high-risk. Consequently, organizations implementing biometric solutions must integrate AI governance into their operations and management systems to ensure innovation is balanced with regulatory compliance."

Ana Mateu de Ros, *Chief Revenue Officer,* Zertia

Privacy Concerns

The sensitive nature of biometric data, such as facial images and fingerprints, lies at the heart of privacy concerns. As these identifiers are inextricably linked to individual identity, unauthorized access or misuse could result in severe privacy violations. Acknowledging this, the EU AI Act categorizes biometric data as a special category of personal data, requiring robust protections. Securing biometric data is paramount to prevent breaches, unauthorized access, and identity theft.

The Act enforces advanced data governance practices, including pseudonymization, encryption, and access controls, to ensure data integrity and confidentiality. Additionally, informed consent and transparency are critical ethical considerations. High-risk AI systems must operate transparently, with individuals being fully informed about the use of their biometric data and the system’s capabilities and limitations. These measures not only safeguard privacy but also foster trust among users.

Risk of Misuse

Biometric identification systems present significant risks of misuse, particularly in surveillance and profiling. The ability to monitor individuals without their knowledge raises ethical concerns about civil liberties and privacy. To counteract this, the EU AI Act prohibits the use of real-time remote biometric identification in public spaces for law enforcement except under strict conditions. Bias and discrimination are additional challenges, as biometric systems can perpetuate or amplify biases in their training data, resulting in unfair treatment based on race, gender, or other characteristics. To address this, the Act mandates bias detection and correction measures to ensure fairness and non-discrimination. The deployment of such systems also introduces accountability challenges, particularly in cases of harm or misuse. To address this, the Act establishes clear obligations for providers and deployers, emphasizing human oversight and compliance with data protection regulations.

Implications for Fundamental Rights

The deployment of biometric identification systems has significant implications for privacy and autonomy, especially when used without consent or in contexts that encroach on personal freedoms. The EU AI Act emphasizes protecting fundamental rights by requiring comprehensive impact assessments to identify and mitigate potential risks. However, complying with the complex regulatory landscape poses legal challenges for providers and deployers, necessitating adherence to requirements such as transparency, human oversight, and data protection. While biometric identification technologies offer considerable advantages, such as enhanced security and convenience, the Act strives to balance innovation with the safeguarding of fundamental rights to ensure ethical and responsible deployment.

Technological and Operational Challenges

The secure implementation of biometric identification systems under the EU AI Act introduces a range of technological and operational challenges. Addressing these challenges is critical to ensuring system efficacy, security, and compliance with regulatory requirements.

Technological Challenges

Biometric systems face several technological hurdles, starting with the need for high-quality and representative data. Poor data quality can lead to inaccurate identifications, while biased datasets risk perpetuating discrimination. To mitigate this, providers must adopt robust data governance practices, including thorough data collection, cleaning, and validation processes, using diverse datasets to ensure fairness. Additionally, achieving accuracy and robustness is essential. False positives or negatives can undermine system trust, necessitating rigorous testing and validation during development. Cybersecurity threats, such as data breaches, also pose risks to biometric systems, which must implement advanced measures like encryption, access controls, and intrusion detection to protect sensitive data.

‘Biometric ID helps address rising cyber and fraud risks’, Edmund Group

With rising cyber and fraud risks necessitating greater security measures like biometric ID, the EU AI Act’s high-risk classification of biometric ID in digital wallets presents strategic challenges for organisations; requiring a structured gap analysis, enhanced governance frameworks and alignment of internal controls with EU regulatory standards.

‘‘High-risk designation drives complex cross-border compliance risks’

"With evolving cyber and fraud threats driving the need for stronger security measures, classifying biometric ID in digital wallets as high-risk exposes firms to complex cross-border compliance risks."

Elliott Day*, Senior Associate,* Edmund Group

System interoperability represents another challenge, as biometric systems often need to integrate seamlessly with various platforms. Adopting common standards and protocols facilitates compatibility and streamlines operation. Moreover, real-time processing demands advanced computational resources and optimized algorithms, particularly in high-demand environments. To address this, scalable architectures and cutting-edge technologies must be leveraged to ensure performance consistency.

Operational Challenges

Registration is a prerequisite for transparency and control, and the main operational challenge is registering the biometric system as an AI in a registry. Key questions which are answered during the registration process are: who is the provider, who is the deployer, what are the intended uses and what uses, if any, are prohibited. Once this has been accomplished, it will be possible to identify and control adherence to detailed regulatory requirements, including transparency, data protection, and human oversight. Establishing comprehensive compliance frameworks and conducting regular audits are vital for ensuring adherence to these standards. Effective human oversight is another critical factor. Operators must be equipped with the tools and training to interpret system outputs accurately and intervene when necessary. Public trust and acceptance are also essential for successful deployment. Transparent communication about the benefits and safeguards of biometric systems, coupled with robust data protection measures, can build user confidence and promote widespread adoption.

Finally, scalability and resource allocation pose additional operational hurdles. Biometric systems must be designed with modular architectures to accommodate growth and technological advancements while minimizing resource strain. Regular maintenance schedules ensure systems remain functional and up to date. However, these efforts require substantial financial and human resources. Cost-benefit analyses and partnerships can help optimize resource allocation and reduce overall costs. In conclusion, while biometric identification systems offer transformative potential, addressing their ethical, legal, technological, and operational challenges is paramount to ensuring their secure and responsible use under the EU AI Act. These efforts are essential to maintaining public trust, protecting fundamental rights, and fostering innovation in a rapidly evolving technological landscape.

Digital Identity Wallets: Strengthen by robust authentication measures

Digital identity wallets are a transformative innovation designed to securely store, manage, and share personal credentials, offering EU citizens, residents, and businesses a unified digital identity solution.

Envisioned under the European Digital Identity (EUDI) Regulation, these wallets facilitate seamless cross-border access to public and private services while ensuring users retain full control over their personal data. As a core feature, biometric identification plays a critical role in enabling secure authentication. However, given the high-risk classification of biometric technologies under the EU AI Act, stringent safeguards are in place to protect users' fundamental rights and privacy.

Key Features of Digital Identity Wallets

Digital identity wallets serve as a secure, interoperable platform for managing sensitive personal data. These wallets allow users to:

- Securely Store and Share Information: Sensitive documents such as driving licenses, academic credentials, and residency proofs can be stored and shared selectively, enhancing security and privacy.
- Control Data Use: Users share only the necessary information for a specific purpose, limiting overexposure of personal data.
- Sign Documents Electronically: Built-in functionality enables secure electronic signing, reducing reliance on physical paperwork.
- Cross-Border Functionality: Wallets empower individuals to access services and validate identity across EU Member States without physical documents.

This capability responds directly to user demand for secure, unified digital IDs, with 63% of EU citizens expressing the need for a single secure identity solution and 72% seeking greater transparency in data processing practices.

Biometric Identification and High-Risk AI Systems

Biometric identification is fundamental to ensuring secure and efficient authentication in digital identity wallets. By enabling automated recognition of unique physical or behavioral traits such as fingerprints or facial features, biometric systems streamline user experiences while enhancing security.

Under the EU AI Act, biometric systems, particularly those used for remote biometric identification, are classified as high-risk AI applications. This classification underscores the potential for misuse or harm, such as unauthorized surveillance or breaches of privacy. Accordingly, the Act establishes a robust regulatory framework that requires compliance with transparency, accountability, and data protection standards.

EU AI Act Safeguards for Biometric Systems in Digital Identity Wallets

The EU AI Act provides critical safeguards to protect users of biometric identification systems in digital identity wallets:

- Transparency Obligations: Providers must inform users when they are interacting with biometric systems and explain how their data is processed. Clear communication ensures users are aware of and consent to the use of such technologies.
- Privacy Protections: Data minimization principles ensure that only necessary biometric data is collected and processed. These measures align with the General Data Protection Regulation (GDPR), reinforcing users' rights to data privacy.
- Prohibited Practices: The Act explicitly bans certain uses of biometric systems, such as real-time remote biometric identification in public spaces for law enforcement, except under narrowly defined conditions. Although primarily aimed at law enforcement, this prohibition underscores the sensitivity of biometric technologies.
- Accountability Standards: Providers and operators of high-risk systems must implement risk management processes, ensuring that biometric systems are deployed prudently and securely.

‘Digital identity wallets suited to demands of the digital age’, Hande Ocak Başev, WSI London

A secure, transparent, and user-centred digital identity system is one of the key needs of the future. The EU Digital Identity Wallet empowers individuals to manage and protect their identity information, making access to both public and private services easier. An innovative solution tailored to the demands of the digital age.

‘Digital identity wallets protect data privacy’

“Technology should empower individuals. The EU Digital Identity Wallet enables everyone to manage their digital identity securely and offers an innovative solution that protects data privacy."

Hande Ocak Başev, *Managing Partner*, WSI Digital Consulting London & Turkiye

Strengthening Trust and Digital Security

By embedding these safeguards into the operation of biometric systems, the EU AI Act mitigates risks associated with high-risk technologies while reinforcing trust in digital identity wallets. Users are assured that their personal data and privacy are protected, fostering confidence in the system's integrity. Additionally, these protections contribute to the broader goal of inclusive and secure digital ecosystems, where fundamental rights are respected.

Digital identity wallets, supported by biometric identification, promise a more efficient and secure future for personal identification in the EU. However, their success hinges on robust regulatory frameworks like the EU AI Act, which ensures these technologies are developed and deployed responsibly. By safeguarding privacy and transparency, the EU AI Act plays a vital role in protecting users' rights while enabling the adoption of trustworthy AI in digital identity systems. These safeguards not only enhance user confidence but also promote a broader culture of responsible innovation in the digital space.

'Innovation needs to align with privacy, security, and ethical standards'

"As biometric identification becomes integral to digital identity solutions, navigating the regulatory landscape of the EU AI Act is critical to ensure innovation aligns with privacy, security, and ethical standards."

Helen Yu*, CEO,* Tigon Advisory Group

Use Case: Potential, for European Digital Identity[5]

Digital identity wallets are a transformative innovation designed to securely store, manage, and share personal credentials, offering EU citizens, residents, and businesses a unified digital identity solution.

As Europe accelerates its journey toward a comprehensive digital transformation, the concept of digital identity wallets has emerged as a cornerstone of this evolution. The European Digital Identity Wallet initiative, outlined in the eIDAS 2 regulation, envisions a future where citizens can seamlessly and securely manage their digital identities across borders. Key to this initiative is the integration of biometric identification technologies, which promise unparalleled security and user-centric access. However, with the rise of biometric solutions, there is an increased need for robust regulatory frameworks to address associated risks and safeguard personal freedoms. This paper explores the use case of biometric identification in digital identity wallets and its implications under the EU AI Act.

Digital Identity Wallets: A Revolutionary Framework

Digital identity wallets represent a pivotal advancement in the way individuals interact with online services. These wallets serve as centralized tools for securely storing and managing digital identity credentials, enabling users to authenticate their identities and access services across multiple domains. Applications range from eGovernment services to banking, telecommunications, healthcare, and beyond. Key use cases include:

- eGovernment Services: Citizens can use digital identity wallets to authenticate themselves for services like tax filing, voter registration, and obtaining official documents.
- Bank Account Opening: Simplifies the process of opening accounts by securely verifying customer identities, even across borders.
- SIM Card Registration: Enables secure and efficient activation of mobile subscriptions, mitigating fraud.
- Mobile Driving Licences: Provides a digital alternative to physical licences, enhancing portability and convenience.
- Qualified eSignatures: Facilitates legally binding digital signatures for contracts and declarations.
- e-Prescriptions: Allows patients to manage prescriptions digitally, streamlining cross-border healthcare access.

Use Case Analysis: Biometric Identification in Digital Identity Wallets

1. eGovernment Services

Biometric identification enables citizens to authenticate themselves quickly for government services like tax submissions or accessing social benefits. This eliminates the risk of identity fraud and ensures only authorized individuals access sensitive services.

EU AI Act Implications:

- Risk mitigation plans must address potential biases in facial recognition systems, ensuring fair access for diverse demographic groups.

[5] Potential, (2024), 'Building the Future of Digital Identity in Europe', accessible at: https://www.digital-identity-wallet.eu/ (last accessed 2nd December 2024)

- Transparent consent mechanisms must be implemented to align with the GDPR.

2. Bank Account Opening

Biometric systems streamline the verification process for opening bank accounts. Cross-border biometric compatibility allows seamless onboarding for customers relocating within the EU.

EU AI Act Implications:

- Developers must provide assurances that biometric systems used for banking are free from algorithmic discrimination.
- Banks must inform customers of how their biometric data is stored and used, meeting the Act's transparency requirements.

3. SIM Card Registration

Biometric verification during SIM card registration can combat fraud and unauthorized access by ensuring that mobile accounts are tied to verified identities.

EU AI Act Implications:

- Biometric systems must undergo regular audits to ensure compliance with risk management requirements.
- Explicit user consent is critical, with users provided clear options to opt out.

4. Mobile Driving Licences

Biometric-enabled mobile driving licences can be used as secure and portable identity proof for activities like renting cars or proving identity during roadside checks.

EU AI Act Implications:

- Developers must ensure real-time biometric systems for mobile licences comply with restrictions on public use.
- High data security standards must prevent unauthorized access or leaks of sensitive biometric data.

5. Qualified eSignatures

Biometric identifiers like fingerprint scans can authenticate users for creating qualified digital signatures, ensuring legal validity and non-repudiation of signed documents.

EU AI Act Implications:

- Systems must incorporate human oversight mechanisms to handle disputes or incorrect identifications.
- Risk assessments must be documented to comply with high-risk AI obligations.

6. e-Prescriptions

Biometric identification simplifies the management of digital prescriptions, ensuring that only authorized individuals access prescribed medications.

EU AI Act Implications:

- Robust data governance practices must be in place to protect sensitive health-related biometric data.

- Systems must provide users with clear information on data processing to comply with transparency rules.

Challenges and Opportunities

While the EU AI Act provides a robust framework for safeguarding biometric systems, implementing these regulations poses challenges, including:

- Technical Complexity: Ensuring AI systems meet rigorous standards requires advanced expertise and significant investment.
- Cross-Border Harmonization: Aligning diverse national implementations of the EU AI Act and eIDAS 2 regulation is critical for interoperability.
- Public Trust: Building user confidence in biometric systems demands transparent and user-friendly processes.

Opportunities abound as well:

- Innovation: Compliance with the EU AI Act can drive innovation in ethical AI development.
- Global Leadership: Europe's proactive approach sets a global benchmark for AI governance.
- Enhanced Security: Biometric systems, when implemented responsibly, can significantly enhance digital security.

Conclusion

The integration of biometric identification in digital identity wallets marks a transformative step toward a secure and user-centric digital Europe. By addressing the risks associated with biometric systems through the EU AI Act's regulatory safeguards, Europe can lead the way in creating a trustworthy digital ecosystem. As stakeholders collaborate to implement these frameworks, the vision of a seamless, secure, and inclusive digital identity becomes increasingly attainable, paving the way for a digitally empowered future.

Potential
For European Digital Identity

Co-funded by
the European Union

Conclusion

Digital identity wallets represent a transformative innovation, offering EU citizens, residents, and businesses a unified solution for securely storing, managing, and sharing personal credentials. These wallets aim to simplify digital interactions while ensuring robust security and compliance with the EU's regulatory framework.

The EU AI Act emphasizes specific requirements for AI models integrated into systems like digital identity wallets, especially those classified as systemic risk or high-impact capabilities. Providers of general-purpose AI models must maintain comprehensive technical documentation, including details of the model's architecture, training data, and computational resources. Models with systemic risks are subject to additional evaluations, such as adversarial testing, to identify limitations and enhance robustness. Transparency requirements obligate providers to share detailed information with downstream users and make summaries of training content publicly accessible. Governance of these models falls under national authorities, which oversee compliance and encourage the adoption of codes of practice to ensure proper application of the Act. High-risk AI systems must be registered and monitored post-market to ensure ongoing compliance and to assess their impact on fundamental rights.

Implications of the EU AI Act

The focus of the EU AI Act on systemic risk and high-impact AI models has several significant implications:

- Market Dynamics: Stricter regulations for high-impact AI models may raise compliance costs for businesses but contribute to safer and more reliable AI systems, ultimately shaping market behaviours.
- Innovation vs. Regulation: The Act strives to balance innovation with regulation, fostering AI development while safeguarding public interests and fundamental rights.
- Consumer Protection: By addressing systemic risks, the regulation enhances consumer protection, mitigating potential harms from the misuse or malfunction of AI systems.
- Global Influence: The Act's comprehensive framework has the potential to set a global standard, influencing how other regions approach AI governance and regulation.

Recommendations for Stakeholders

To advance the safe and effective use of biometric identification systems in digital identity solutions, the following recommendations are proposed:

Policymakers

- Strengthen Legal Frameworks: Develop clear and enforceable standards for biometric data processing that align with privacy and data protection laws.
- Promote Transparency: Mandate disclosure of information about AI systems, including data sources, model capabilities, and limitations, to ensure informed use.
- Encourage Collaboration: Foster partnerships among governments, industry stakeholders, and academia to create best practices and share knowledge on biometric technologies.

Developers

- Focus on Bias Mitigation: Implement rigorous testing and validation to identify and address biases in biometric systems, ensuring fairness for diverse demographic groups.
- Enhance Security Measures: Prioritize robust security protocols to safeguard biometric data against unauthorized access and misuse.
- Adopt Ethical AI Practices: Incorporate ethical considerations into system design, emphasizing user consent, data minimization, and transparency.

Deployers

- Conduct Impact Assessments: Perform comprehensive evaluations of biometric systems to assess their effects on fundamental rights and societal values.
- Implement Human Oversight: Ensure systems include mechanisms for human oversight, allowing for intervention in the event of errors or unintended consequences.
- Engage with Stakeholders: Involve users, civil society organizations, and other stakeholders in the deployment process to address concerns and increase system acceptance.

By implementing these recommendations, stakeholders can contribute to the responsible development and deployment of biometric identification systems. This approach aligns with the objectives of the EU AI Act to protect public interests, promote innovation, and uphold fundamental rights.

‘ISO/IEC 42001:2023 contains appropriate risk management guidance’, Data Privacy & AI

In general all actors should implement a risk management process for AI based on ISO/IEC42001 point. Actions to address risks and opportunities“, e.g. differentiate acceptable from non-acceptable risks, performing AI risk assessments, conducting AI risk treatment, assessing AI risk impacts. Monitor the AI risks in an iterative way which we know as a continuous improvement process. ISO/IEC 23894:2023 AI Guidance on Risk Management can give the corresponding guidance.

‘Risk management drives Trustworthy AI use’

‘Active risk management is essential for our trustworthy way with AI."

Ina Schöne*, Founder,* Data Privacy and AI

Annex – Third-Party Opinions (Karushkov)

Biometric data and measuring its impact

Upon designing the AI model that shall utilise biometric data, effectuation of an impact assessment test is recommended. Such a test shall focus on compliance check of the AI model and its functionalities - from regulatory perspective, and on reality check - from the perspective of the market and societal sectors in Europe at which the model that utilises biometric data is designed for. You may opt to have a look at our video content dedicated to some regulatory practicalities on this or other technology business matters - http://linkedin.com/in/mitko-karushkov-3533882 , get in touch on tailored advice - at sofia@karushkov.com, or visit our website at www.karushkov.com.

Special, sensitive data as related to high-risk AI models

Biometric data processed solely to identify a human being are seen as special data under the EU legislation and as such, its processing is generally prohibited in Europe. Exceptions to the said prohibition are set, so for anyone who complies to be able to do its business in a legal fashion. And here comes the crossing point with the AI modelling - it is fundamental to understand that irrespective of whether an AI model can be classified as high-risk or no, the mere fact of dealing with biometric data itself already requires attention and relevant compliance steps . You may contact Karushkov Legal Solutions at sofia@karushkov.com for further tailored advice, or visit our website at www.karushkov.com.

About AI & Partners

AI & Partners
Amsterdam – London - Singapore

AI & Partners – 'AI That You Can Trust'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Contacts

Sean Donald John Musch, CEO/Founder, s.musch@ai-and-partners.com

Michael Charles Borrelli, Director, m.borrelli@ai-and-partners.com

Authors

Sean Donald John Musch, CEO/Founder

Michael Charles Borrelli, Director

References

Biometrics Institute, (2024), “Industry Survey”, accessible at: https://www.biometricsinstitute.org/what-is-biometrics/industry-tracker-survey/? (last accessed 29th November 2024)

Biometrics Institute, (2024), “Thought Leadership”, accessible at: https://www.biometricsinstitute.org/thought-leadership-pieces/ (last accessed 29th November 2024)

Biometrics Institute, (2024), “Good practice guidance material”, accessible at: https://www.biometricsinstitute.org/good-practice/ (last accessed 29th November 2024)

European Commission, (2024), “Digital building blocks”, accessible at: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home (last accessed 29th November 2024)

European Parliament and The Council of the European Union, (2014), Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last accessed 29th November 2024)

European Parliament and The Council of the European Union, (2024), 2024/1689 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), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last accessed 29th November 2024)

Acknowledgements

Corporate Partners

We are grateful to our network of corporate partners for their invaluable contributions:

Individual Partners

We are also grateful to our network of individual supporters for their invaluable contributions:

Ana Mateu de Ros, Ana Mateu de Ros has worked for 22 years in marketing positions at various pharmaceutical companies, providing innovative solutions for patients with diverse pathologies. Recognizing the growing importance of artificial intelligence, Ana has decided to make a career change and seize this opportunity to help companies use AI in an ethical and responsible manner. Due to my extensive experience in diverse and dynamic environments, Ana has developed the ability to thrive in rapid-change settings and work effectively within cross-functional teams. Ana is a highly innovative thinker by nature and a creative person, always looking for new and better options. Ana has a passion for science-based brands that can improve patients' lives, and is excited to leverage this passion in the digital world, particularly in the ethical and responsible use of artificial intelligence.

Benjamin Brock, Benjamin Brock is an Artificial Intelligence and Data Science Lead, also at the Edmund Group.

Dr. Meera Sarma, Dr. Meera Sarma, has 20+ years in cybersecurity, specialises in cybercrime, hacking, quantum computing, and education. She holds a PhD in hacker innovation and a degree in Physics and has advised UK Parliament on cybersecurity and quantum safety.

Elliott Day, Elliott Day is a Senior Compliance & Financial Crime Consultant at Edmund Group, a UK consultancy specialising in risk, compliance & financial crime prevention. Benjamin Brock is an Artificial Intelligence and Data Science Lead, also at Edmund Group.

Hande Ocak Başev, Hande Ocak Başev, AI Strategist, Entrepreneur, and President of WSI London, has over 20 years of experience in AI-driven business strategies, management consulting, and digital transformation. She has led 350+ transformation projects and 50+ business development initiatives. As the Founder of Quattro Business Consulting and a member of the WSI Global AI Leadership Board, she guides companies through digital transformation. Having completed AI programs at MIT and Oxford, she is also a Forbes Türkiye AI Columnist, a Global Chamber London Advisory Board Member, and the first woman to serve as CEO and Board Member at Galatasaray Sports Club. Additionally, she leads initiatives promoting women in leadership as Chair of the Strategy Committee at the Women on Boards Association.

Helen Yu, Helen Yu is the founder and CEO of Tigon Advisory. Helen helps tech companies of all sizes multiply their growth opportunities by leveraging AI, cybersecurity, IoT, supply chain, and customer experience. With over two decades of technology industry experience, Helen offers CXO-as-a-service and guidance to organizations through digital transformation, strategic planning, enterprise risk management, go-to-market optimization, and influencer marketing. Helen has worked with enterprise clients such as SAP, Dell Technologies, AT&T, Workday, Intel, IBM, and Microsoft, as well as B2B SaaS, Fintech, Insuretech, and Martech startups. Helen also serves as an independent board director and a venture capital advisor, where she brings a unique perspective on technology thought leadership, cybersecurity risk management, go-to-market strategy, and customer experience. Helen is a certified cybersecurity expert from MIT Sloan School of Management, an MBA from Loyola University of Chicago, and a respected industry thought leader, a Wall Street Journal best selling author, a keynote speaker, and a host of CXO Spice podcast. Helen is passionate about empowering and mentoring the next generation of technology leaders, especially women and minorities.

Ina Schoene, Ina Schoene is Founder of Data Privacy and AI and follows the practice-oriented approach to understand the requirements of AI-Act and the measures to implement this requirements based of the ISO/IEC42001 and additional and guides the companies on the path to get the corresponding certifications. Currently she is in qualification of ISO/IEC42001 Lead Auditor Program for Artificial Intelligence Management systems.

Lisa Ventura MBE, Lisa Ventura MBE is an award-winning cyber security specialist, published writer/author, journalist and keynote speaker. She is the Founder of Cyber Security Unity, a global community organisation that is dedicated to bringing individuals and organisations together who actively work in cyber security to help combat the growing cyber threat.

Mitko Karushkov, Mitko Karushkov has been providing legal, regulatory, compliance, transactional and business solutions to international companies for more than 20 years now. Focused on enterprise companies and their strategic (or daily) operations, Mitko has solved matters related to the digital, tech or electronic assets of such businesses. Active and involved also in bridging between traditional and technology markets, including to the application of the EU DSA, DMA, AI and other regulations. Media, Telecoms, IPRs, Corporate, M&As are also part of the service portfolio of Mitko. For further information: www.karushkov.com.

Neil Oschlag-Michael, Neil Oschlag-Michael is an AI Governance Product Owner and Consultant, specializing in AI and Data Governance, Risk, and Compliance.

Lisa Ventura,

Founder,

Cyber Security Unity

Ina Schöne,

Founder,

Data Privacy and AI

Hande Ocak Başev,

Managing Partner, WSI Digital Consulting London & Turkiye

Elliott Day,

Senior Compliance & Financial Crime Consultant, Edmund Group

Benajmin Brock,

AI and Data Science Lead,

Edmund Group

Mitko Karushkov,

Founder,

Karushkov Legal Solutions

Neil Oschlag-Michael,

AI Governance Product Owner,

2021.AI

Ana Mateu de Ros,

Chief Revenue Officer,

Zertia

Helen Yu,

CEO,

Tigon Advisory Corp.

Important notice

This document has been prepared by AI & Partners B.V. for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of AI & Partners B.V. to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment. Images used throughout the document have either been produced in-house or sourced from publicly available sources (see **References** for details).

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V.