AI & Partners

Amsterdam - London - Singapore

EU AI Act

Overseeing Biometric Identification

April 2025

Disclaimer

AI & Partners
Amsterdam - London - Singapore

For more information on this publication, visit https://www.ai-and-partners.com/.

About AI & Partners

'AI That You Can Trust' - Your trusted advisor for EU AI Act Compliance. Unlock the full potential of artificial intelligence while ensuring compliance with the EU AI Act by partnering with AI & Partners, a leading professional services firm. We specialise in providing comprehensive and tailored software solutions for companies subject to the EU AI Act, guiding them through the intricacies of regulatory requirements and enabling responsible and accountable AI practices. At AI & Partners, we understand the challenges and opportunities that the EU AI Act presents for organisations leveraging AI technologies. Our team of seasoned experts combines in-depth knowledge of AI systems, regulatory frameworks, and industry specific requirements to deliver strategic guidance and practical solutions that align with your business objectives.

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

Business Integrity

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.

AI & Partners' publications do not necessarily reflect the opinions of its clients, partners and/or stakeholders.

Contents

AI & Partners
Amsterdam - London - Singapore

Executive Summary

AI & Partners
Amsterdam - London - Singapore

High-Risk Classification

Biometric ID systems are high-risk under the EU AI Act.

Prohibited Practices

Certain uses of biometric ID, like real-time ID in public spaces, are prohibited without specific conditions.

Fundamental Rights Impact Assessment

Deployers must assess and mitigate risks to individuals' fundamental rights.

Compliance and Enforcement

Deployers must cooperate with authorities, submit reports, and inform individuals about high-risk AI use.

Data Governance

High-risk AI systems must follow strict data governance to prevent bias and protect privacy.

Regulating Biometric Identification

The EU AI Act, effective **August 1, 2024**, regulates AI to enhance safety, security, and trust. Biometric identification in EU Digital Identity Wallets is classified as high-risk, requiring transparency, data protection, and oversight. The Act enforces compliance, prohibits misuse, and ensures innovation aligns with fundamental rights and privacy protection.

Introduction

AI & Partners
Amsterdam - London - Singapore

Privacy and Data Protection
Biometric data is inherently sensitive, and its misuse can lead to significant privacy violations.

Bias and Discrimination
Biometric systems can produce biased results, leading to discriminatory effects, particularly concerning age, ethnicity, race, or sex.

Regulatory Compliance
The classification of biometric systems as high-risk under the EU AI Act imposes stringent compliance requirements.

Opportunities

Issues

Enhanced Security
Biometric identification offers a high level of security, reducing the risk of identity theft.

User Convenience
Biometric identification enhances user experience and convenience.

Innovation and Growth
The development of biometric technologies can spur innovation and economic growth,

Facilitating Seamless Access to Services

The EU Digital Identity Wallet enhances security and convenience through biometric identification, classified as high-risk under the EU AI Act. This whitepaper explores regulatory compliance, privacy risks, bias concerns, and ethical safeguards. It provides insights into implementation challenges, best practices, and future recommendations for secure and responsible biometric identity systems.

Types of Biometrics

AI & Partners
Amsterdam - London - Singapore

Covering Full Range of Biometrics

Biometric identification is the automated recognition of individuals based on unique physical, physiological, or behavioural traits, such as facial recognition, fingerprints, iris scans, and voice patterns. Types of biometrics include physiological (fingerprints, facial recognition, iris, DNA) and behavioural (voice recognition, gait analysis, typing patterns), each with distinct applications and security implications.

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

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

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

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

Fingerprint (Palm Print)
Fingerprints consist of unique patterns formed by raised ridges across the skin, making them reliable for identification.

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

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.

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

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

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.

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

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

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.

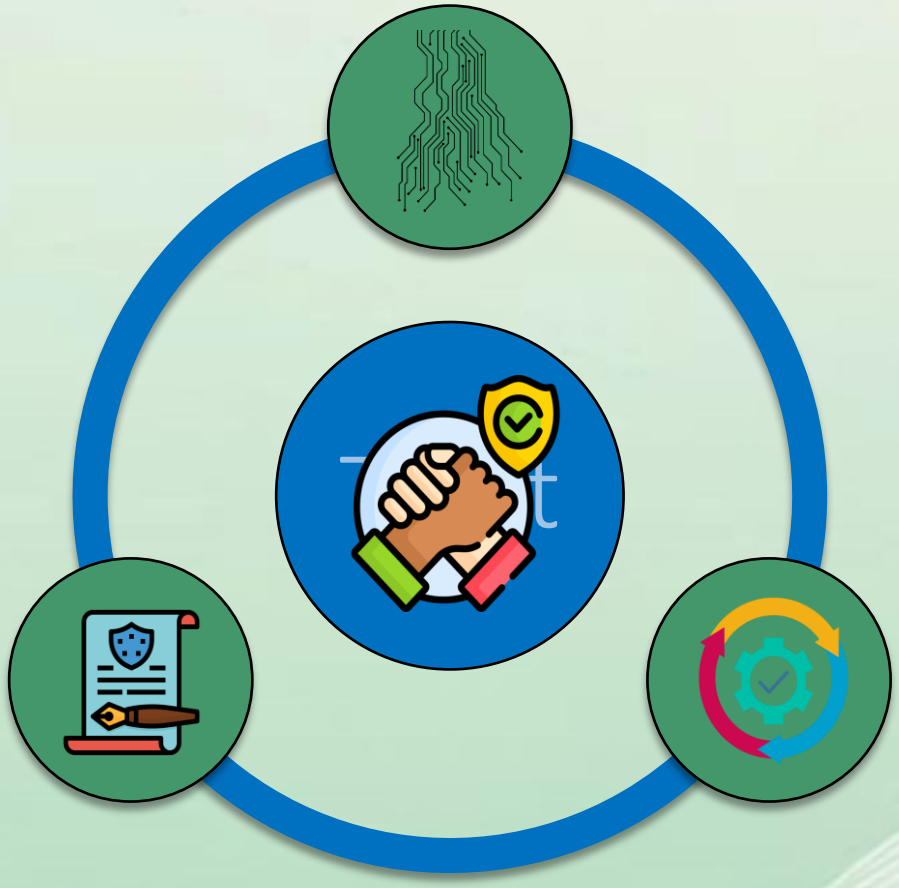
Heartbeat
Each individual has a unique heartbeat pattern influenced by physiological characteristics, irrespective of heart rate or activity level

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

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

Governance and Compliance

AI & Partners
Amsterdam - London - Singapore



Three Laws of Biometrics

Policy

Regulations ensure the ethical and legal use of biometric identification by enforcing transparency, data protection, and oversight. They address privacy concerns, prevent misuse, and establish accountability while balancing security, innovation, and fundamental rights.

Process

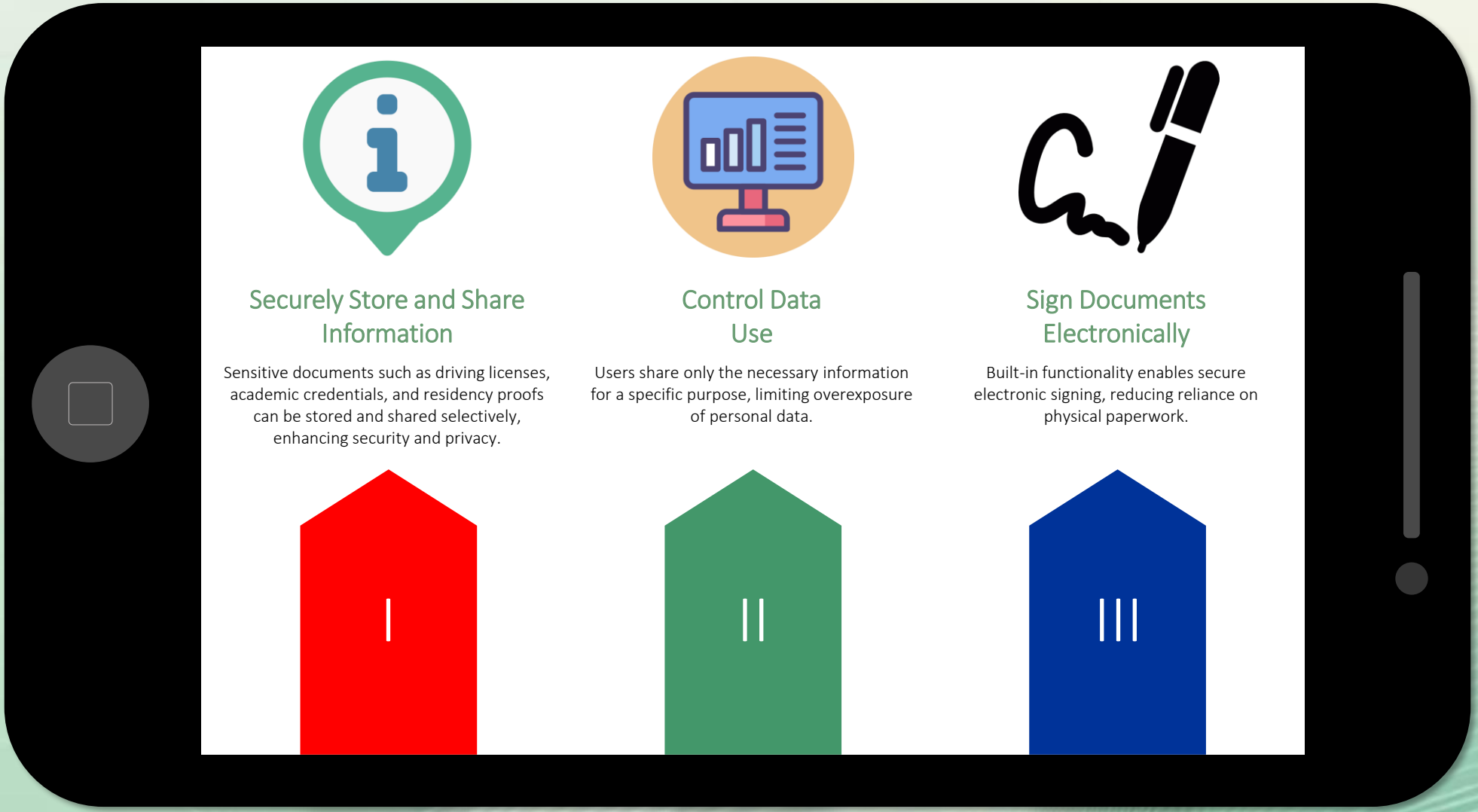
Biometric identification is integrated into authentication systems to enhance security and efficiency. It involves data collection, verification, and compliance with legal frameworks, ensuring transparency, user consent, and safeguards against bias or unauthorized access.

Technology

AI-powered biometric systems analyze physical or behavioral traits for identification. Advanced machine learning improves accuracy, prevents fraud, and ensures interoperability across digital platforms while continuously evolving to meet security and regulatory requirements.

Digital Identity Wallets

AI & Partners
Amsterdam - London - Singapore



Use Case: Potential for European Digital ID

AI & Partners
Amsterdam - London - Singapore

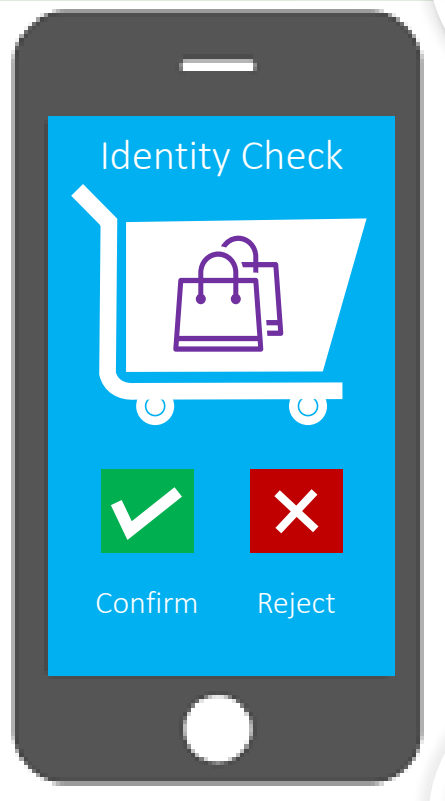
What It Is: Digital identity wallets securely store and manage personal credentials, enabling seamless authentication across various sectors like eGovernment, banking, and healthcare while integrating biometric identification for enhanced security.

Why It Matters: They improve convenience, prevent fraud, and ensure cross-border interoperability while addressing regulatory challenges like privacy, bias, and compliance under the EU AI Act.

How They Use Biometric Identification: Biometric authentication verifies user identities for secure access, enabling fraud-resistant processes in banking, SIM registration, eGovernment services, digital signatures, and e-prescriptions while ensuring data protection and regulatory compliance.

Conclusion

AI & Partners
Amsterdam - London - Singapore



Secure and User-Centric Future: Biometric identification in digital identity wallets enhances security, convenience, and trust, paving the way for a seamless and efficient digital experience across the EU.

Regulatory Compliance is Key: Adhering to the EU AI Act ensures ethical deployment, data protection, and transparency, addressing privacy concerns and fostering public confidence in biometric systems.

Driving Innovation and Leadership: The EU's proactive approach to digital identity and AI governance sets a global standard, promoting responsible innovation while balancing security, privacy, and accessibility.

Appendix – Third-Party Opinions by Karushkov

AI & Partners
Amsterdam - London - Singapore

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.

"Effectuation of an impact assessment test is recommended." Karushkov

KARUSHKOV
LEGAL SOLUTIONS

Feedback from our global network of experts

AI & Partners
Amsterdam - London - Singapore

Biometric Identification and the EU AI Act	Introduction	Conclusion
Regulatory Framework	*Problem Statement: Issues and Opportunities*	*Recommendations for Stakeholders*

'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 MBE, *Founder*, Cyber Security Unity

'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

'Risk management drives Trustworthy AI use'

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

Ina Schöne, *Founder*, Data Privacy and AI

Feedback from our global network of experts

AI & Partners
Amsterdam - London - Singapore

Digital Identity Wallets: Strengthen by robust authentication measures

EU AI Act Safeguards for Biometric Systems in Digital Identity Wallets

'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

Governance and Compliance

Technological and Operational Challenges

'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

EDMUND

Digital Identity Wallets: Strengthen by robust authentication measures

Strengthening Trust and Digital Security

'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 Corp

Feedback from our global network of experts

AI & Partners
Amsterdam - London - Singapore

Challenges and Considerations

Ethical and Legal Concerns

‘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

Thanking Our Corporate Partners

AI & Partners

Amsterdam - London - Singapore

rialto

ACCELERATED IMPACT

CYBERSECURITY UNITY

be safe, be sure, BE SECURE

CYSTEL

DATA PRIVACY & AI

PRE AUDIT SERVICE

WSI

zertia

EDMUND

K. KARUSHKOV LEGAL SOLUTIONS

2021.AI

Tigon Advisory

Start-ups, cure your disconnects.

Thanking Our Individual Partners

AI & Partners

Amsterdam - London - Singapore

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.

Thanking Our Individual Partners

AI & Partners
Amsterdam - London - Singapore

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

Benjamin 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

Thanking Our Individual Partners

AI & Partners
Amsterdam - London - Singapore

Helen Yu,
CEO,
Tigon Advisory Corp.

Utilising top-tier research data

AI & Partners
Amsterdam - London - Singapore

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)

Contact Us

AI & Partners
Amsterdam - London - Singapore

AI & Partners

Amsterdam - London - Singapore

E-mail

contact@ai-and-partners.com

Website

https://www.ai-and-partners.com/

Disclaimer

AI & Partners

Amsterdam - London - Singapore

This Presentation may contain information, text, data, graphics, photographs, videos, sound recordings, illustrations, artwork, names, logos, trade marks, service marks, and information about us, our lines of services, and general information may be provided in the form of documents, podcasts or via an RSS feed ("the Information").

Except where it is otherwise expressly stated, the Information is not intended to, nor does it, constitute legal, accounting, business, financial, tax or other professional advice or services. The Information is provided on an information basis only and should not be relied upon. If you need advice or services on a specific matter, please contact us using the contact details for the relevant consultant or fee earner found on the Presentation.

The Presentation and Information is provided "AS IS" and on an "AS AVAILABLE" basis and we do not guarantee the accuracy, timeliness, completeness, performance or fitness for a particular purpose of the Presentation or any of the Information. We have tried to ensure that all Information provided on the Presentation is correct at the time of publication. No responsibility is accepted by or on behalf of us for any errors, omissions, or inaccurate information on the Presentation. Further, we do not warrant that the Presentation or any of the Information will be uninterrupted or error-free or that any defects will be corrected.

Although we attempt to ensure that the Information contained in this Presentation is accurate and up-to-date, we accept no liability for the results of any action taken on the basis of the Information it contains and all implied warranties, including, but not limited to, the implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy are excluded from these Terms to the extent that they may be excluded as a matter of law.

In no event will we be liable for any loss, including, without limitation, indirect or consequential loss, or any damages arising from loss of use, data or profits, whether in contract, tort or otherwise, arising out of, or in connection with the use of this Presentation or any of the Information.