Deloitte.

Artificial Intelligence Services

Security, ethics and governance for the safety of data and AI

Navigate Tomorrow's Risks Today: AI Governance Solutions for a Secure Future!

2024.

Safeguarding Innovation

***The safe and ethical implementation of AI enables organizations to innovate with confidence***

Embracing digitized ways of working has resulted in many organizations adopting rudimentary artificial agents to automate repetitive processes. To increase the breadth of coverage of these solutions, Artificial Intelligence (AI) is increasingly being employed. However, it brings new risks and governance challenges that continue to act as a barrier to scaling.

To navigate these risks, organizations must understand their current exposure, ensure AI outcomes are validated for both efficacy and ethics, put in place governance that supports the maintenance of these outcomes, and ensure they are ready for crises when they occur.
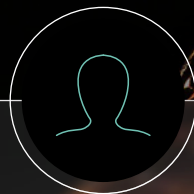
"I need to drive and articulate new AI solutions to our business board, set AI strategy and make technology choices to support it"
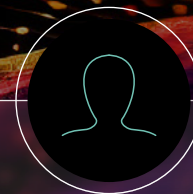
– Chief Information Officer
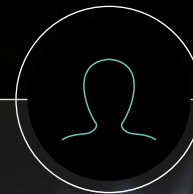
"I need to govern and manage information, and bring innovation to our business model through data processing and data mining"

– Chief Data Officer

"I need to be able to deliver our AI transformation quickly and in a profitable way"

– Chief Innovation Officer

"I need to demonstrate that we have appropriate oversight, compliance and governance in place over our AI"

– Chief Compliance Officer

We understand Your challenges & opportunities

Managing the Digital Transformation Journey

As organisations adopt new technologies and embrace new business models, they also need to evolve their culture, working practices, and organisational structures.

Transforming the business, and the risk and control management functions, in a way that is deliberate and controlled, is critical to achieving the strategic objectives. Failure to do so may lead to unforeseen operational, financial, or customer consequences.

Managing Risk in a Digital organisation

The risk landscape is complex and fast changing. New technologies with additional risks are emerging, and businesses are developing new ways of working, with new digital functions. Operations that were once local, are now global; supply chains are complex and opaque; bad news travels fast through the internet and social media.

These new digitally-driven threats and risks need to be identified, considered, and managed alongside existing risks while tailoring controls specifically for digital initiatives.

Supporting to Adopt Emerging Technologies to Utilize the Maximum out of AI

Digital brings new opportunities to embrace data, tooling, and automation technologies in order to manage business processes efficiently.

The utilization of emerging technologies, such as AI, Cloud Computing, 5G and IoT will help organizations to stay in competition, focus on innovation and deliver accelerated customer value.

The pace of digital adoption is different for all organisations

Market leaders will leverage new digital concepts for risk and control management, and also promote safe adoption across the whole business

Our Data and AI services

At Deloitte, we provide a comprehensive range of customizable data and AI services. Backed by the dedication to technological advancement and extensive industry knowledge, we are equipped with the insights and proficiency to face any scenario.

AI Governance

AI Control Advisory & Risk Management

Trustworthy AI

AI & Data Security

AI Compliance

Service Provider & Third-Party Assessments

Quality Assurance for AI projects

AI Governance

Effective AI governance aims to ensure that AI systems are developed and utilized responsibly, with careful consideration given to potential risks and impacts on individuals, society, and the environment. It involves defining clear guidelines and standards for AI development, promoting transparency and accountability in AI decision-making processes, and addressing issues such as bias, discrimination, and misuse of AI technologies.

We assist our clients in implementing AI governance by conducting thorough risk assessments, developing robust ethical frameworks, establishing transparent data governance protocols, and providing training programs to ensure responsible AI use throughout their organizations. By leveraging our expertise and resources, they can empower businesses to navigate the complexities of AI governance effectively and foster a culture of accountability and trust in their AI initiatives.

We offer the following services for the development and execution of the effective AI Governance model:

- AI Strategy & Roadmap
- Data Governance
- Risk Management
- Impact Assessment
- AI Policy, Standard & Guideline

- Defining Roles & Responsibilities
- Data Ethics
- Regulatory Compliance
- Training & Education
- Stakeholder Engagement
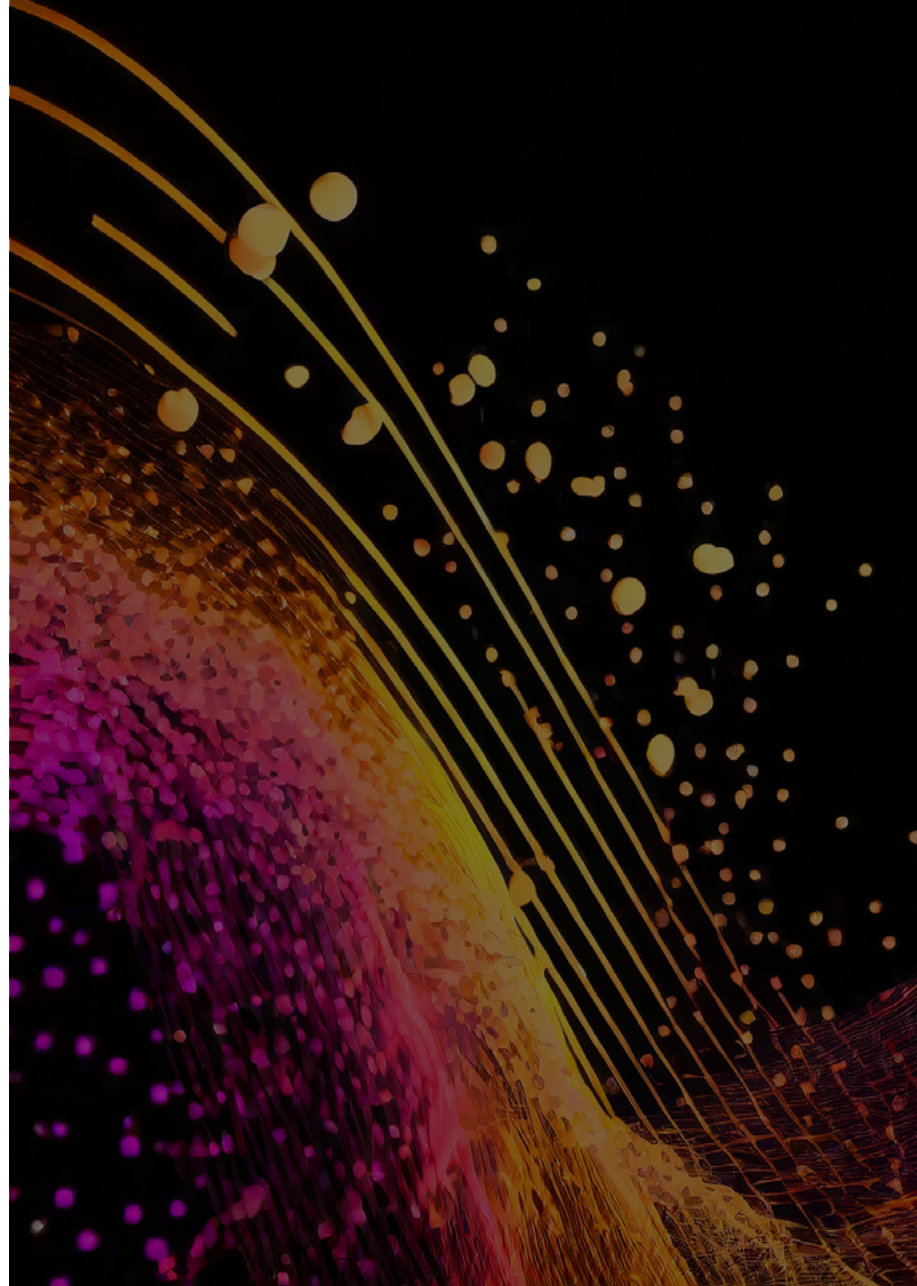
AI Control Advisory & Risk Management

Effective risk management encompasses a set of practices and processes designed to ensure the safe, ethical, and effective deployment of AI technologies within organizations.

Key aspects of AI risk management include:

- Conducting risk assessments to identify potential threats and vulnerabilities in AI systems.

- Analyzing the impact of risks on organizational objectives, stakeholders, and regulatory compliance.

- Developing risk mitigation strategies and controls to address identified risks.

- Implementing monitoring and control mechanisms to track AI performance, detect anomalies, and respond to emerging risks.

- Continuously evaluating and updating risk management processes in response to changes in technology, regulations, or business conditions.

We help our clients in the design and implementation of the following elements to enhance their AI risk management processes:

- Risk Management Framework Development

- Risk Assessment & Analysis

- Control Design and Implementation

- Control Assessment & Security Audit

- Data & AI Maturity Assessment

Trustworthy AI

AI and machine learning are increasingly used to assist and improve business decision making. It is therefore essential that the insights garnered, or decisions made by AI algorithms are fair, ethical, safe and explainable, especially when they affect safety and other important aspects of human life.

Our Trustworthy AI services are designed to ensure the ethical, responsible, and reliable implementation of artificial intelligence technologies. With a focus on transparency, fairness, and accountability, we help organizations navigate the complexities of AI adoption while building trust with stakeholders.

We help professionals to investigate the AI models and provide confidence that the algorithms contained in them perform as expected:

- Trustworthy AI Assessment

- AI Security & Safety

- Explainable AI

- Data Privacy

- Algorithm Assurance

- Bias & Fairness Detection

- Responsibility & Accountability Matrix

AI & Data Security

Security is an important field to implement measures to protect data and AI systems from unauthorized access, breaches, manipulation, and other security threats. This involves safeguarding both the data used to train and operate AI models and the AI systems themselves.

We offer a multifaceted approach to safeguarding data and AI systems against evolving security threats. Our expert team provides tailored consultations and implementation support to ensure that our clients' data and AI infrastructure remain secure and compliant with industry regulations and standards.

We assist to protect valuable assets with a variety of services:

- Secure Architecture Design
- Security Audit
- Secure Cloud Solutions

- Crisis Management
- Business Continuity and Disaster Recovery
- Penetration Testing

AI Compliance

Upcoming and enforced AI regulations and standards are promoting trust and acceptance of AI technologies in society. Showing its compliance is crucial for every organization as it can build trust, credibility, and reputation. When a company demonstrates that it adheres to relevant regulations, ethical standards, and industry best practices, it reassures customers that their rights, privacy, and interests are being respected and protected.

Besides, compliance helps mitigate risks associated with legal and regulatory violations, avoiding potential fines, penalties, and reputational damage.

Our expert team possesses knowledge and experience in a wide range of compliance topics, including:

- EU AI ACT
- EU Ethics Guideline for Trustworthy AI
- ISO 42001 AI Management System
- ISO 38507 AI Governance

- NIST AI Risk Management Framework
- OWASP AI Security and Privacy Guide
- Decrees and Regulations published by the Central Bank of Hungary

Service Provider & Third-Party Assessments

AI technology and business service providers must build trust with their customers and stakeholders fostering long-term relationships and driving sustainable business growth. The best way to achieve this is to obtain assurance from a third-party auditor that can independently assess the provided services and products or prepare the organization for the upcoming challenge.

Independent assessments offer invaluable validation of service providers' adherence to stringent security and operational standards. This assurance not only enhances trust but also demonstrates a commitment to maintaining high levels of data protection and operational excellence.

In an increasingly interconnected and data-driven landscape, third-party assessments services like SOC2 play a crucial role in safeguarding sensitive information and mitigating risk.

Our team is ready to assess service providers and provide professional services for both auditing and advisory urposes, including:

- Service Organization Controls (SOC) 1 reporting
- Service Organization Controls (SOC) 2 reporting
- Vendor Risk Management
- ISO 27001 Information Security Management System

- ISO 22301 Business Continuity Management System
- Cloud Control Matrix
- FedRAMP

Quality Assurance for AI projects

Our expertise ensures that AI systems meet rigorous standards of reliability, accuracy, and performance. By conducting comprehensive testing and validation processes, as an independent QA, we can mitigate the risks associated with AI deployment, such as algorithmic bias, data drift, and unexpected behavior.

Our clients benefit from our specialized knowledge and methodologies, which help identify and rectify issues early in the development lifecycle, saving time and resources in the long run. They can turn to you for assurance that their AI solutions will deliver consistent and trustworthy results, fostering confidence among stakeholders and enhancing the overall success of their AI initiatives.

We help our clients with independent QA throughout the whole AI lifecycle:

- Vendor Selection
- Requirement Specification
- Business & Use-Case Analysis
- Data Quality Assessment

- Model Selection
- Benchmarking
- KPI design
- Post-implementation Review
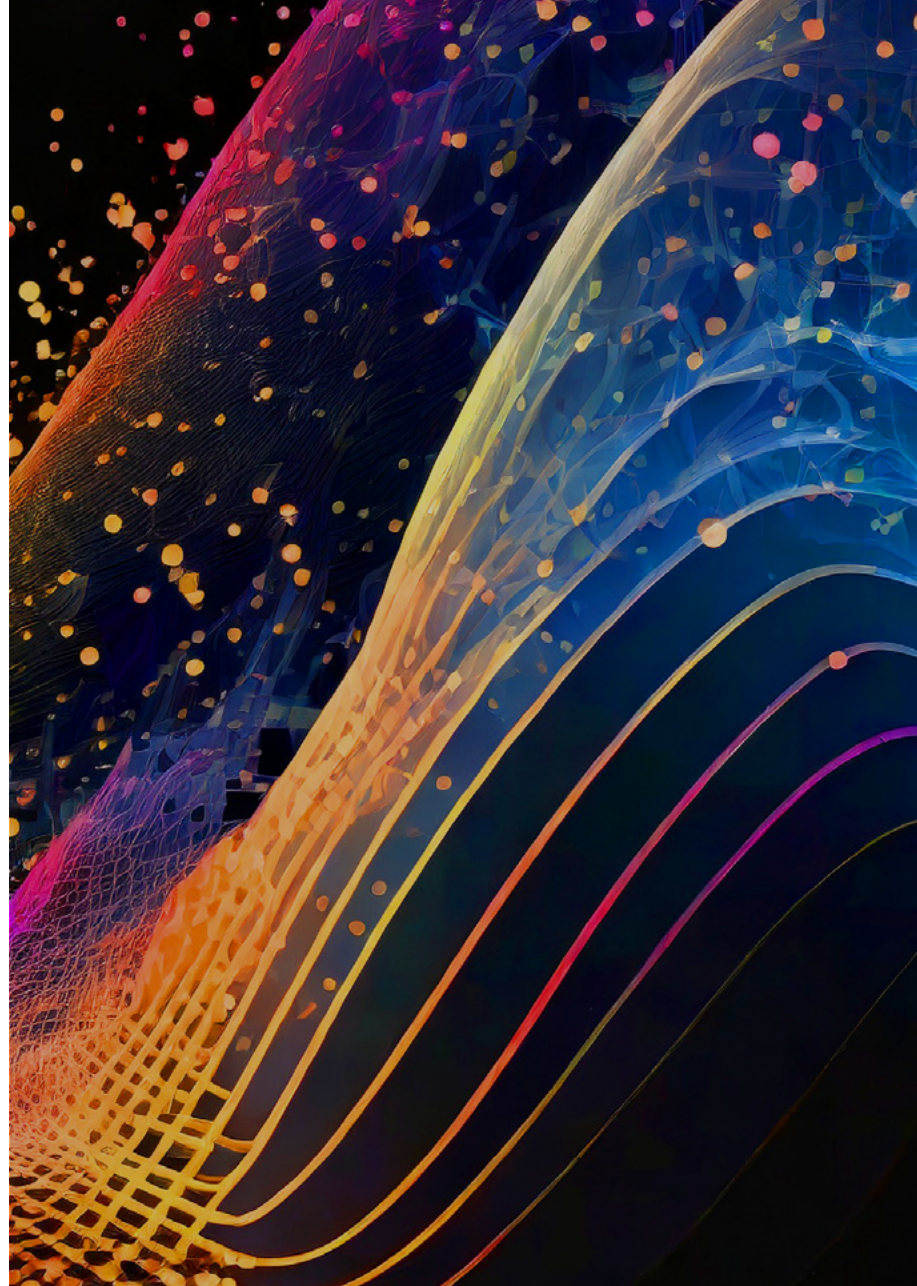
Our Artificial Intelligence Governance Framework

The governance framework, developed by Deloitte CE experts, provides solutions spanning the entire AI lifecycle for all industries, from data management to complete monitoring of AI systems and models.

The framework focuses on industry-leading practices and a strategic approach to seamlessly navigate complex subfields of the AI world, ensuring the deployment of ethical, responsible and safe AI.
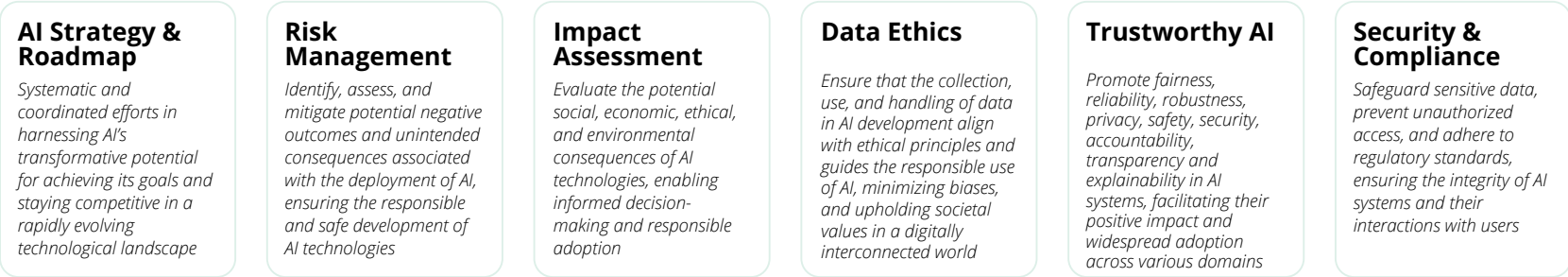
AI Governance Framework

Key elements and objectives

| Data Governance | AI Systems & Processes | Algorithm Assurance | Integration & Development | Interaction & Communication | Performance & Monitoring |

Center-of-Excellence
The organisational structure to provide strategy, governance and management of intelligent automation

Operating Model Components

AI Strategy & Roadmap	**Risk Management**	**Impact Assessment**	**Data Ethics**	**Trustworthy AI**	**Security & Compliance**
Systematic and coordinated efforts in harnessing AI's transformative potential for achieving its goals and staying competitive in a rapidly evolving technological landscape	*Identify, assess, and mitigate potential negative outcomes and unintended consequences associated with the deployment of AI, ensuring the responsible and safe development of AI technologies*	*Evaluate the potential social, economic, ethical, and environmental consequences of AI technologies, enabling informed decision-making and responsible adoption*	*Ensure that the collection, use, and handling of data in AI development align with ethical principles and guides the responsible use of AI, minimizing biases, and upholding societal values in a digitally interconnected world*	*Promote fairness, reliability, robustness, privacy, safety, security, accountability, transparency and explainability in AI systems, facilitating their positive impact and widespread adoption across various domains*	*Safeguard sensitive data, prevent unauthorized access, and adhere to regulatory standards, ensuring the integrity of AI systems and their interactions with users*

AI lifecycle

Planning & Design → Data preprocessing → Model building → Testing & validation → Deployment → Operation & Monitoring

Focus areas

Business objectives | Risk mitigation | Value creation

Deloitte AI risk management framework

Deloitte's unique risk management framework for AI applications incorporates market-leading trends, leading scientifical results, Deloitte's global experience and in-house knowhow, and industry standards throughout the AI development and operations lifecycle.

Deloitte's AI Risk Management Framework provides 6 topics to help mitigate the risks posed by AI systems. Our experts in Hungary have full knowledge of the framework, having participated in its development.

1. DATA GOVERNANCE

1 **Dac** Data Acquisition & collection	5 **Dq** Data quality
2 **Ds** Data storage	6 **Dpr** Data privacy
3 **Dp** Data processing	7 **Dsc** Data security
4 **Di** Data integration	8 **De** Data ethics

2. AI SYSTEMS & PROCESSES

9 **As** AI strategy	13 **Rs** Requirements & specifications
10 **Rr** Roles & responsibilities	14 **Ia** Impact assessment
11 **Au** Acceptable usage	15 **Rm** Risk management
12 **Sda** System design & architecture	16 **Ss** System security

3. ALGORITHM ASSURANCE

17 **Bu** Business & use-case analysis	20 **Et** Evaluation & testing
18 **Mdd** Model design & development	21 **Td** Trustworthy by design
19 **Mtt** Model training, tuning & update	22 **XAI** Explainable & Transparent

4. INTEGRATION & DEVELOPMENT

23 **Cd** Continuous integration & Continuous delivery	26 **Sa** Sandboxing
24 **Sd** Secure development	27 **Ml** MLOps
25 **In** Interoperability	28 **Md** Model deployment

5. INTERACTION & COMMUNICATION

29 **Hi** Human involvement & supervision	32 **Ic** Internal communication
30 **Si** Stakeholder involvement	33 **Ec** External communication
31 **Cc** Communication channels	34 **Us** User support

6. PERFORMANCE & MONITORING

35 **Qa** Quality assurance	39 **Cma** Continuous maintenance
36 **Pr** Performance metrics	40 **Ad** Auditability
37 **Pa** Performance assessment	41 **Ce** Compliance evaluation
38 **Cm** Continuous monitoring	42 **Bd** Bias detection

Latest media appearances, communication and marketing activities

State of AI Hungary Survey: We conducted a detailed analysis study based on in-depth interviews with over 200 decision-makers in Hungary.

State of AI Hungary study, Gen AI, and other AI-related topics media and communication results:

- More than 1000 downloads of the State of AI Hungary study.
- A successful PR conference
- A successful webinar with over 300 applicants.
- Several appearances at in-house client events as presenters.
- More than 5 personal press/radio interviews about the study.
- More than 5 conference appearances as AI expert presenters.
- PR articles featured in approximately 20 online/offline media platforms/magazines.
- Broadcast of 3 AI and Gen AI-related podcast episodes as hosts, featuring conversations with eminent AI leaders in Hungary.
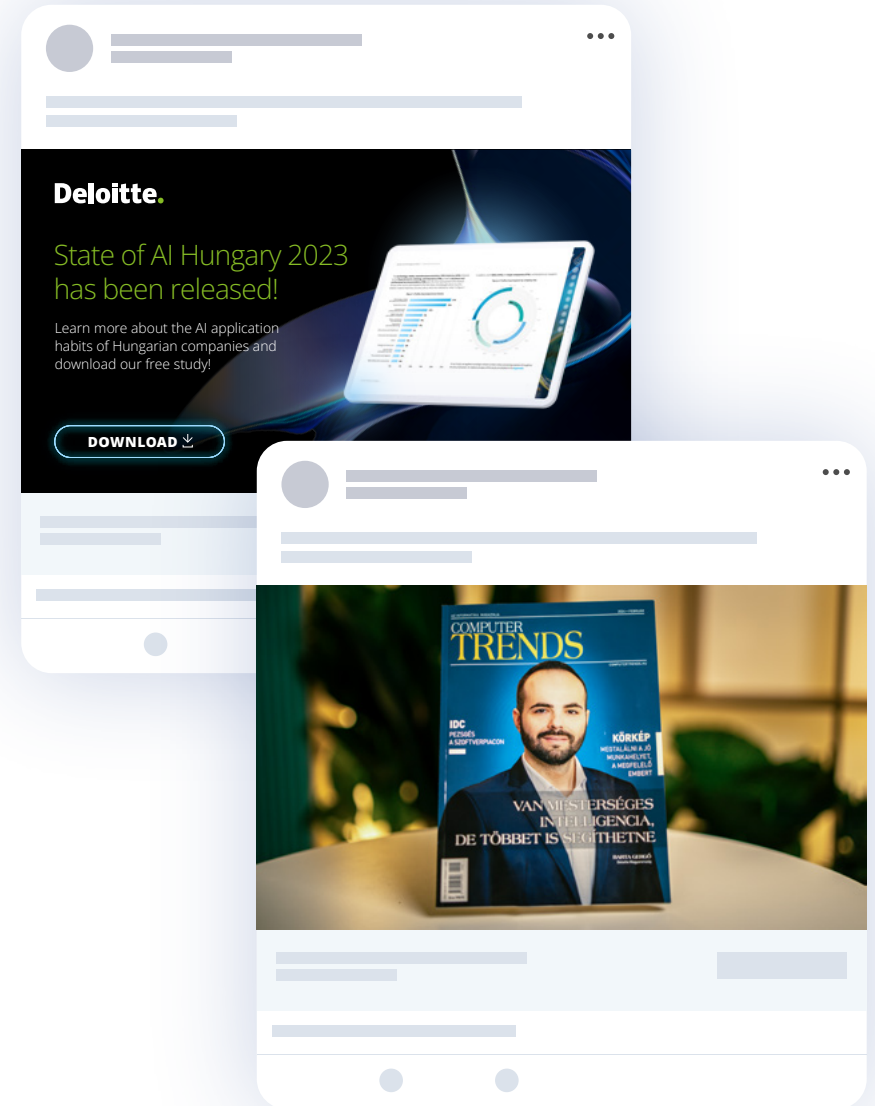
Contact Us

Zoltán Szöllősi
Partner

zszollosi@deloittece.com

+36 20 910 7644

Dr. Gergő Barta
Senior Manager

gbarta@deloittece.com

+36 20 328 1190

Deloitte.