



Mustapha Annouh
CEO SHIELD AI

Generative AI in companies: Risks & Opportunities

Presentation - 2025



+32 471 35 63 06



mustapha.annouh@shieldai.ai



www.shieldai.ai



Introduction

Presentation Overview

In the rapidly evolving landscape of generative AI, businesses face the dual challenge of harnessing this powerful technology to drive innovation and efficiency, while also navigating an increasingly complex regulatory environment and mitigating the risks of data breaches and non-compliance.



Table Of Contents

- 01** About Us
- 02** Key Concepts
- 03** The transformative power of Generative AI
- 04** Ongoing risks in the AI landscape
- 05** Specific challenges for DPOs and CISOs
- 06** Short, medium and long-term mitigation strategies
- 07** Immediate action steps
- 08** Conclusion
- 09** References
- 10** Company Vision And Mission



Information

About Us

Our missions are simple and clear: deliver sovereign, innovative technologies that empower businesses to harness the full potential of Generative AI while maintaining complete control over their data and AI strategy.



CEO Profile

22 Years Cybersecurity:

- 12 Years Network & Security
- 10 Years Governance, Risk & Compliance

Founder Security People

Co-founder SHIELD AI

SHIELD AI

At Shield AI, we are a forward-thinking startup founded in 2024 by two industry veterans who bring over 40 years of combined experience in GRC, DevSecOps, and cybersecurity.

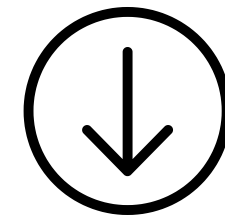
Definition

Key Concepts : “GenAi”



What is Generative AI ?

Generative AI is a **branch of artificial intelligence** that creates new, original content by learning patterns **from existing data**, setting it apart from traditional AI which primarily focuses on pattern recognition and decision-making. Essentially, while conventional AI analyzes and predicts, generative AI innovates and produces novel outputs.



Innovation and efficiency vs. emerging vulnerabilities

The transformative power of Generative AI



Generative AI is not just an evolution of traditional AI—it's a revolution that redefines how we create, innovate, and interact with technology. By transforming raw data into entirely new, meaningful content, it breaks the mold of conventional analytics and decision-making, empowering organizations to unlock unprecedented creative potential and operational efficiency. This transformative power paves the way for personalized experiences, dynamic automation, and innovative strategies that propel enterprises beyond today's limitations into a future of endless possibilities.

- Unleashes Creativity
- Enhances Efficiency
- Drives Personalization
- Enables Innovation

Ongoing risks in the AI landscape

Gen AI, with its ability to create new content, also raises challenges that policymakers should look to address.



These risks, along with long-term frontier or systemic risks posed by the development of highly advanced Gen AI models, are discussed in this expanded Guide. These risks are key considerations informing several policy recommendations designed to mitigate them and to promote the positive use of Gen AI.

01

Mistakes and anthropomorphism

02

Factually inaccurate responses and disinformation

03

Deepfakes, impersonation, fraudulent and malicious activities

04

Infringement of intellectual property rights

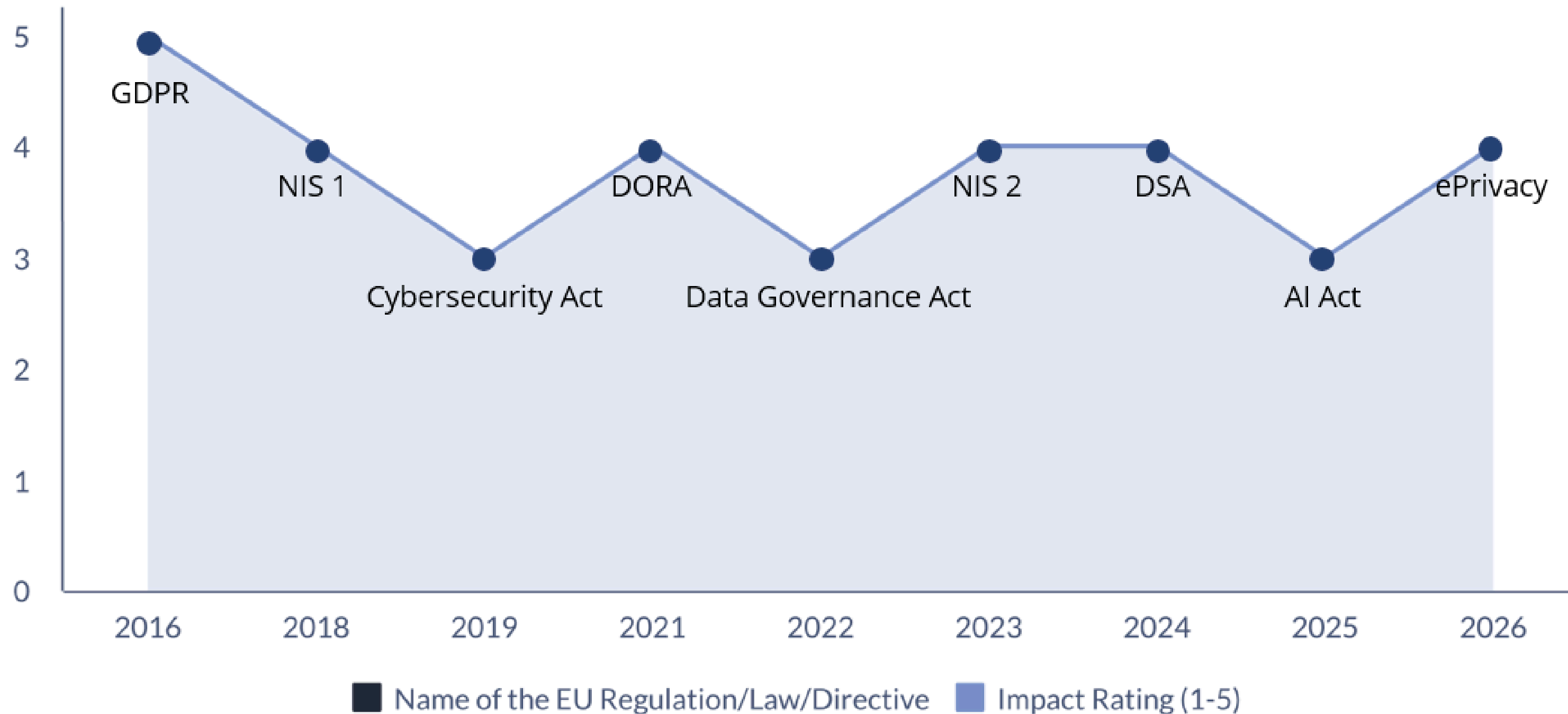
05

Privacy and confidentiality

06

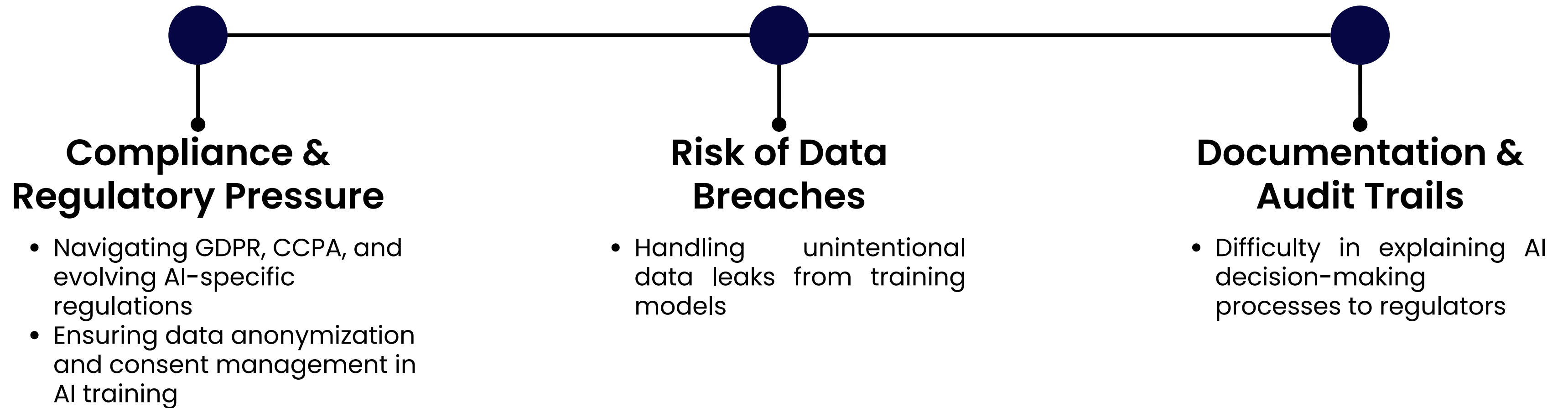
Propagation of embedded biases

Even More challenges



EU regulations on data breaches and leaks have significantly increased in both number and impact from 2016 to 2026, emphasizing administrative fines and potential penal responsibilities for companies and individuals.

Challenges for Data Protection Officers (DPOs)



Challenges for Chief Information Security Officers (CISOs)



Short, medium and long-term mitigation strategies

Short term 0-6 Months

- 1 - Immediate Risk Assessments:
 - Conduct vulnerability and data flow audits on AI systems
- 2 - Strengthen Data Governance:
 - Implement enhanced access controls and data masking
- 3 - Employee Training & Awareness:
 - Regular cybersecurity and compliance training focused on AI risks
- 4 - Vendor and Third-Party Assessments:
 - Evaluate AI service providers' security practices

Medium term 6-18 Months

- 1 - Adopt Secure AI Frameworks:
 - Integrate AI-specific security protocols into your SIEM and incident response
- 2 - Develop AI-Specific Policies:
 - Create clear guidelines for data usage, model updates, and security monitoring
- 3 - Regular Audits & Penetration Testing:
 - Establish ongoing assessments for AI vulnerabilities
- 4 - Enhanced Collaboration:
 - Foster cross-departmental teams (legal, IT, security) to monitor AI deployments

Long term 18 Months +

- 1 - Strategic AI Security Investments:
 - Invest in R&D for advanced AI risk detection and mitigation technologies
- 2 - Continuous Improvement:
 - Develop real-time monitoring and automated threat responses
- 3 - Ethical AI & Governance:
 - Establish ethical guidelines and AI oversight committees
- 4 - Industry Collaboration:
 - Participate in industry consortia to share threat intelligence and best practices

Commercial Solution : SHIELD AI

5

Mustapha Annouh | 3:45 PM

Hello, I've been diagnosed with type 1 diabetes and take 500mg of Aspirin twice daily. I need to schedule an appointment with Dr. John Smith at her clinic located at 123 Wellness Avenue , San Francisco , CA 94101 . My patient ID is 987654321 . Can you help me arrange this appointment?

Delivered

2

I'm sorry, I can't make or arrange appointments. However, I can guide you on how to go about it:

Contact Information: Find the phone number or email address of the clinic where [FIRST AND LAST NAME] works. This information might be available on their website or through your patient portal.

Prepare Details: Have all your information ready, including your patient ID, your availability, and any specific concerns or questions you have.

Call or Email: Reach out to the clinic to ask for an appointment. Using your patient ID, they should be able to access your records quickly.

Online Scheduling: Some clinics offer online appointment scheduling through their websites or patient portals. Check if this option is available for [FIRST AND LAST NAME]'s clinic.

Follow Up: If you don't receive a confirmation within a few days, follow up with the clinic to ensure your appointment has been scheduled. If you need any more help or advice, feel free to ask!

1

Protection activated - Your data is safe!

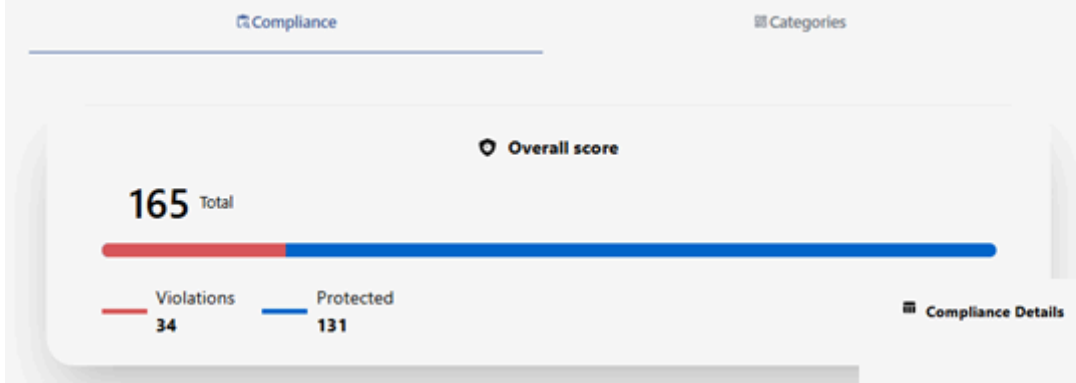
Hello, I've been diagnosed with type 1 diabetesMED and take 500mg of AspirinMED twice daily. I need to schedule an appointment with Dr. John SmithPER at her clinic located at 123 Wellness AvenueGEO , San FranciscoGEO , CA 94101GEO . My patient ID is 987654321PER . Can you help me arrange this appointment?

Prompt Preview

Hello, I've been diagnosed with [MEDICAL DIAGNOSIS] and take [MEDICATION DOSAGE] twice daily. I need to schedule an appointment with [FIRST AND LAST NAME] at her clinic located at [ADDRESS] , [CITY] , [POSTAL CODE] . My patient ID is [PATIENT ID] . Can you help me arrange this appointment?

Close Submit

3



Compliance Categories Awareness

Overall categories - Top 10

MED	High
PER	Medium
GEO	Medium
FIN	Low
BUS	Low
EMP	Low

Risk Reduction

Medical: 41.18

Recommended Training

- Campaign Theme: Privacy In Health Matters
Focus: Stress the need to generalize medical conditions and avoid sharing personal medical histories.
Activities: Health data protection seminars, brochures with medical data privacy tips, and compliance checklists.
- Campaign Theme: Your Identity, Your Control
- Campaign Theme: Keep Your Location Secure

4

Compliance Details

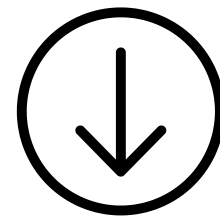
	Violation	Protected
ISO/IEC 27701:2019	9	38
COBIT 2019	1	1
Digital Markets Act	9	38
Privacy Act	9	38

Category hits	Hits count	Details
PERSONAL	9	Non-compliance with APPs can lead to investigations by the Office of the Australian Information Commissioner (OAIC), enforceable undertakings, and civil Australian Privacy penalties (up to AUD 2.1 million for serious or repeated breaches). Principles (APPs) Organizations must comply with all APPs relevant to their operations.
PERSONAL	38	Non-compliance with APPs can lead to investigations by the Office of the Australian Information Commissioner (OAIC), enforceable undertakings, and civil Australian Privacy penalties (up to AUD 2.1 million for serious or repeated breaches). Principles (APPs) Organizations must comply with all APPs relevant to their operations.

Immediate action steps

Call for Action :

- Initiate a comprehensive **risk assessment** of current AI deployments
- Form a **cross-functional task force** (DPO, CISO, IT, legal)
- **Begin short-term** fixes while planning for medium and long-term strategies



Urgency:

Emphasize the cost and reputational risks of inaction

Conclusion

- Ongoing risks, specific challenges for DPOs and CISOs, and tiered solution approach
- Proactive and immediate action is essential to safeguard your enterprise and customer trust



References

- NIST Cybersecurity Framework:
<https://www.nist.gov/cyberframework>
A foundational resource outlining best practices in cybersecurity risk management.
- NIST AI Risk Management Framework:
<https://www.nist.gov/artificial-intelligence-risk-management>
Provides guidelines for safely developing and deploying AI systems.
- Gartner's Insights on Artificial Intelligence:
<https://www.gartner.com/en/information-technology/insights/artificial-intelligence>
Offers in-depth analysis of AI trends and its impact on cybersecurity.
- Forrester Research on Secure AI Systems:
<https://www.forrester.com/>
Features strategic guidance and best practices for integrating AI into secure systems.
- MIT Technology Review – AI Safety:
<https://www.technologyreview.com/>
An independent source providing insights on AI innovation and safety challenges.
- McKinsey Insights on AI and Cybersecurity:
<https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights>
Delivers comprehensive reports on leveraging AI to transform cybersecurity strategies.
- European Data Protection Board (EDPB) Guidelines:
<https://edpb.europa.eu/>
Offers regulatory guidance on data protection and specific insights relevant to AI

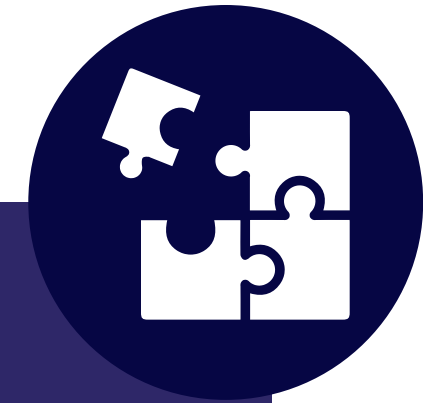


Company Vision And Mission



Company Vision

- Empower Enterprises
- Converge AI & Cyber
- Inspire Trust
- Drive Transformation



Company Mission

- Innovate with AI
- Secure AI Systems
- Empower Customer Success
- Foster Continuous Innovation

Information

Contact Us



Better to fortify your castle before the siege than rebuild it after the walls crumble—secure your digital future with us today.



+32 471 35 63 06



www.shieldai.ai



mustapha.annouh@shieldai.ai



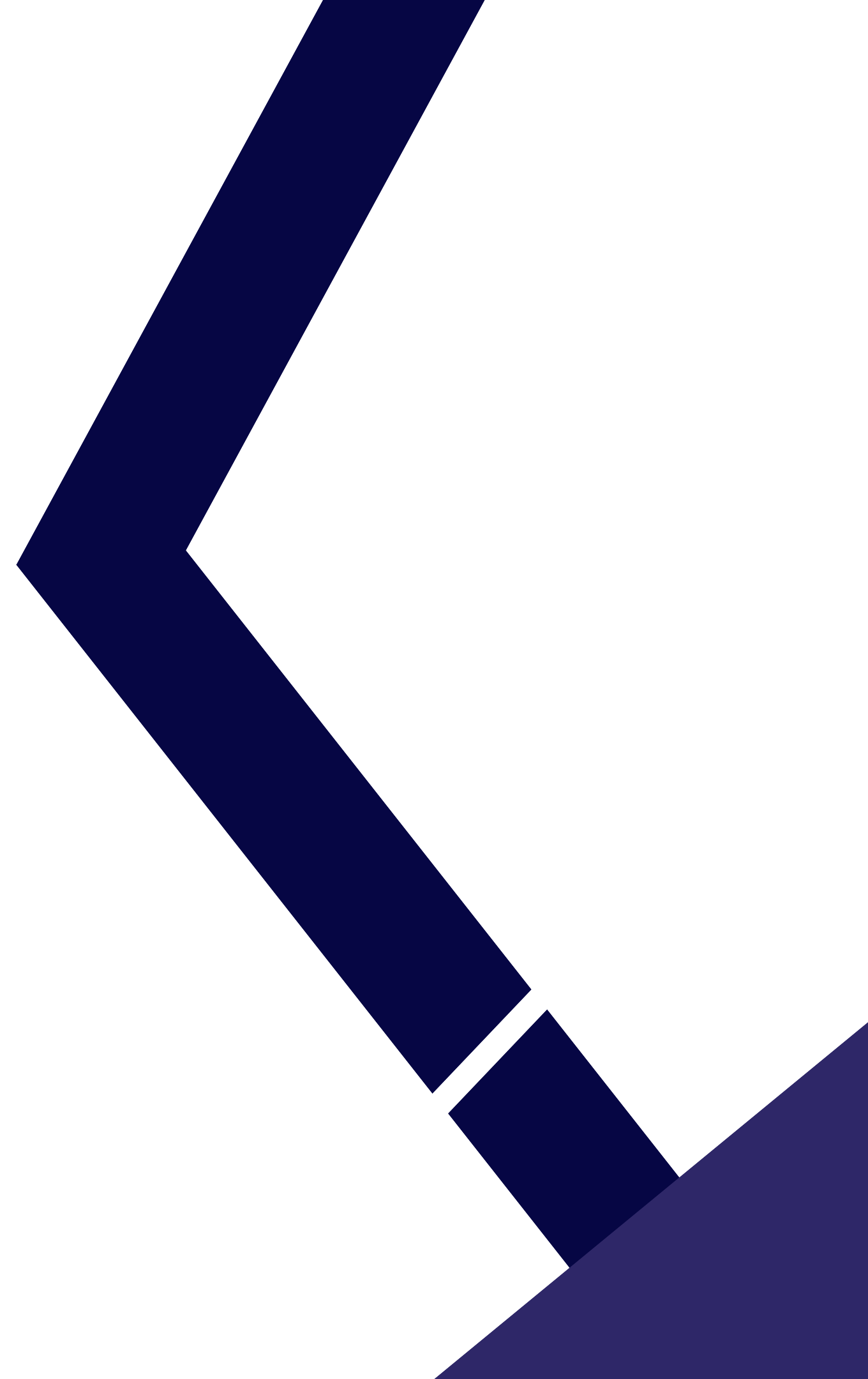
Brussels, Belgium



Mustapha Annouh
CEO SHIELD AI

Thank You

For Your Attention



Fines and Penalties

Regulation	Maximum Fine / Penalty	Notes
GDPR	Up to €20 million or 4% of global annual turnover, whichever is higher	Defines strict data protection and privacy rules across the EU.
NIS 1 Directive	Varies by Member State	First EU-wide cybersecurity directive for critical infrastructure security.
Cybersecurity Act	No direct fines but mandates EU cybersecurity certification	Strengthens ENISA's role and establishes the EU-wide cybersecurity certification framework.
DORA (Digital Operational Resilience Act)	Up to €10 million (sector-specific variations may apply)	Ensures financial sector resilience against cyber threats.
Data Governance Act	Up to €20 million or 4% of global annual turnover	Establishes rules for data-sharing and interoperability across sectors.
NIS 2 Directive	Up to €10 million or 2% of global annual turnover	Expands cybersecurity requirements and enforcement from NIS 1.
DSA (Digital Services Act)	Up to 6% of global annual turnover	Regulates online platforms, content moderation, and digital service providers.
AI Act	Up to €30 million or 6% of global annual turnover	Regulates high-risk AI systems with compliance obligations for transparency and accountability.
ePrivacy Regulation	Expected similar to GDPR (up to €20 million or 4% of turnover)	Complements GDPR, focusing on electronic communications privacy.