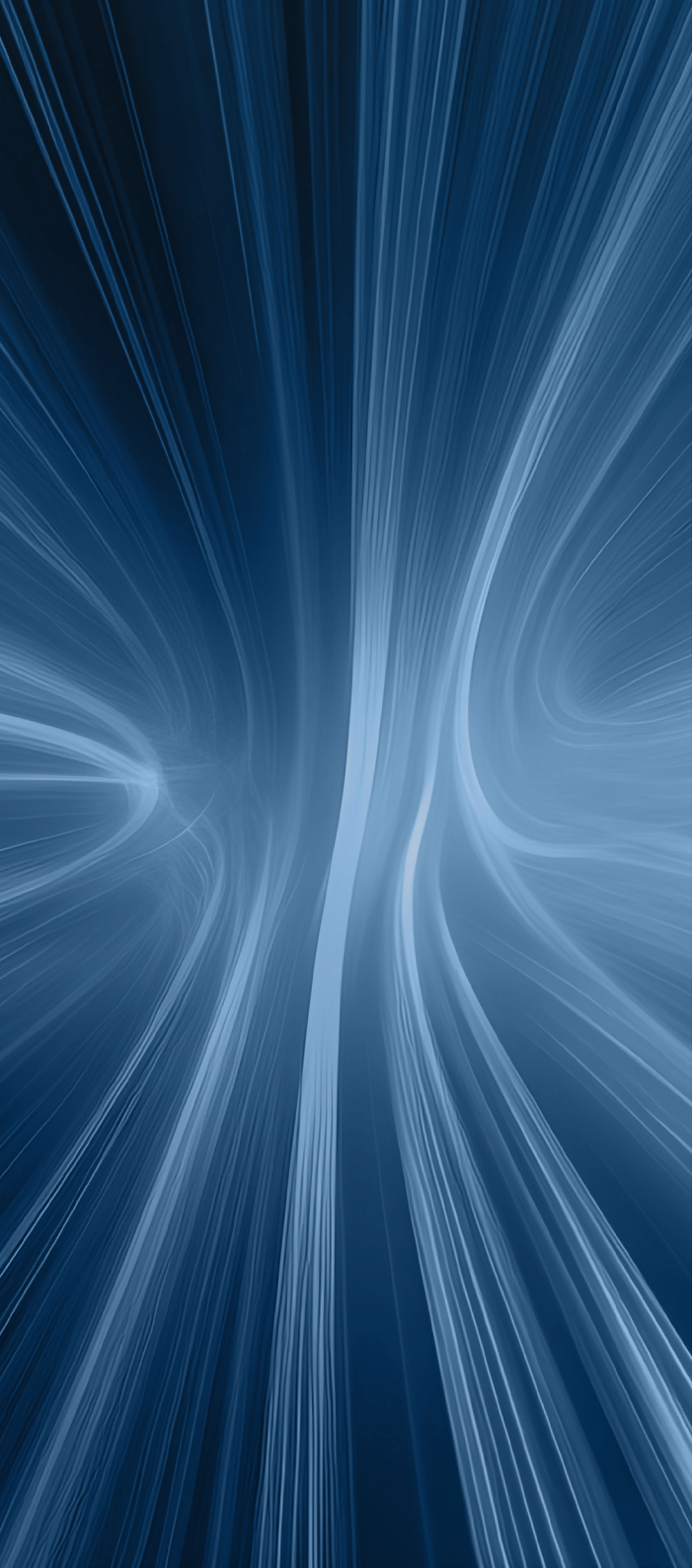
The Intersection of Privacy and AI Governance

By IAPP Research and Insights

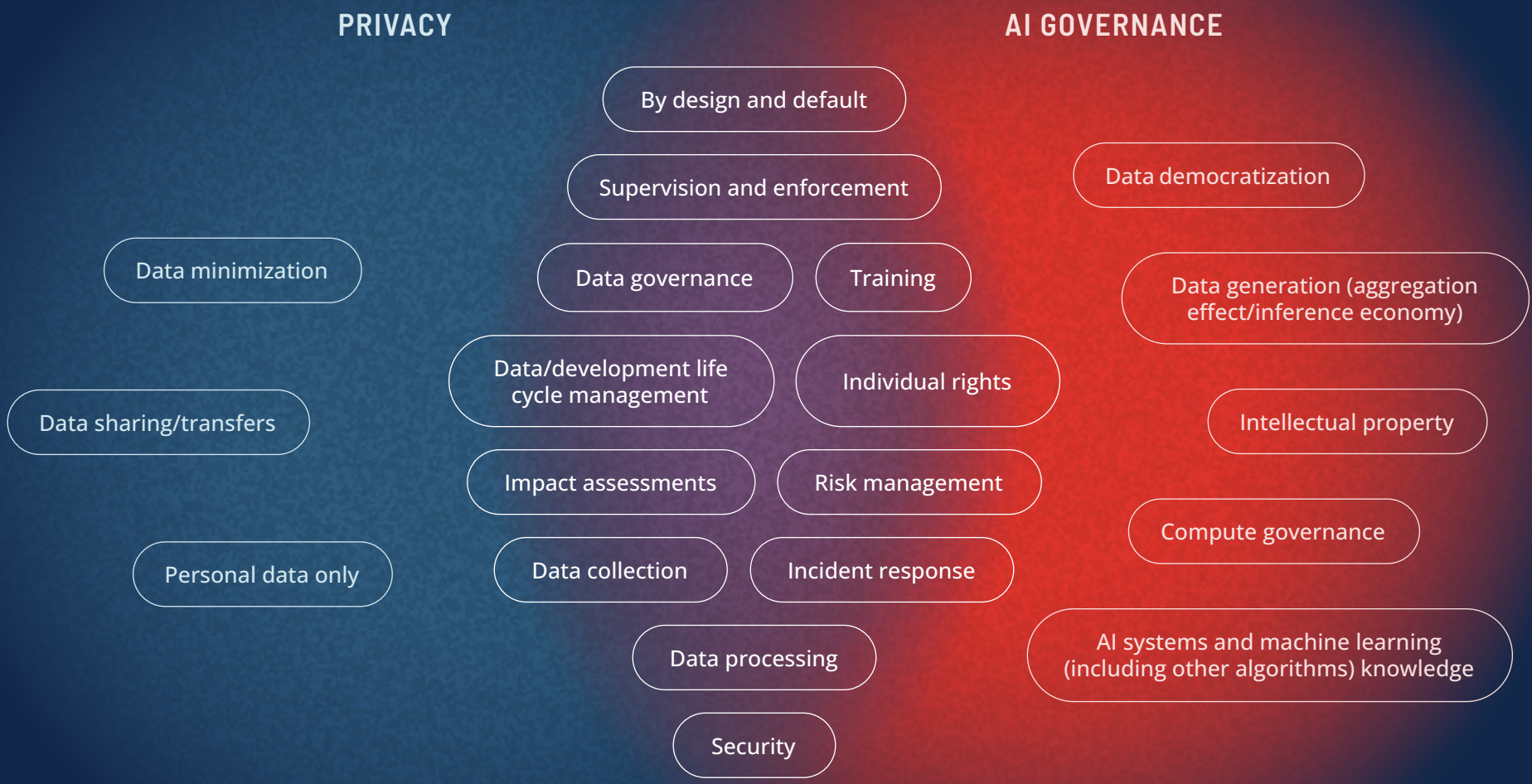


The intersection of privacy and AI governance reveals numerous similarities and differences, providing valuable insights about each area's impact on the other. To better understand such insights, a comparative analysis illustrates that privacy influences AI and vice versa, while highlighting existing gaps or tensions. One notable observation from this analysis is the "shared" terminology between privacy and AI governance. However, disparities and conflicts in term usage demonstrate varied interpretations and meanings. Therefore, focusing on this intersection is crucial not only for comprehending the gaps between terms, e.g., data minimization versus democratization, but also for grasping the convergence of these two fields.

The accompanying Venn diagram is a nonexhaustive illustration of the more important domains shared by and distinct to privacy and AI governance. The center of the diagram does not fully elaborate on all concepts but presents broader, overarching ideas as the concepts are a blend of principles, harms, risks and types of technology. The associated resource table provides a deeper understanding of this intersection by further exploring these specific domains and dissecting them into nuanced principles. Specifically, the table provides a nonexhaustive inventory of IAPP and other relevant resources that deliver valuable insights and knowledge to professionals. For further elaboration on specific terms found within the Venn diagram and resource table, please refer to the IAPP's Key Terms for AI Governance and Glossary of Privacy Terms.

Last updated May 2024.

The Intersection of Privacy and AI Governance



*The concepts that intersect privacy and AI governance are expanded on in the resource table on the following pages and can be clicked to navigate to its location.

BY DESIGN AND DEFAULT

Principle	IAPP resources	Regulatory guidance and other resources
Ethics by design	→ "Ethical AI by design: How responsible AI yields a brighter tomorrow" web conference recording → "Responsible AI: Putting data ethics into action" web conference recording → "AI and ethics: New developments, regulatory considerations and ethical obligations" web conference recording → "Building ethics into privacy frameworks for big data and AI" white paper	→ European Commission's Ethics By Design and Ethics of Use Approaches for AI guidance → UNESCO's Recommendation on the Ethics of AI
Privacy by design/data protection by design (default)	→ Privacy tech and privacy by design topic page → "Strategic Privacy by Design, Second Edition" by R. Jason Cronk, CIPP/US, CIPM, CIPT, FIP → "Cybersecurity Law Fundamentals, Second Edition" by James X. Dempsey and John P. Carlin → IAPP-EY Privacy Governance Report 2023 → Privacy engineering domains chart series → "How to operationalize privacy by design" article → "Privacy by design to evolve beyond compliance and enforce responsible use of data" web conference recording	→ National Institute of Standards and Technology's AI Risk Management Framework Section 3.6 on privacy-enhanced AI → UNESCO's Recommendation on the Ethics of AI, Principle 34 → European Data Protection Board Guidelines 4/2019 on Article 25 Data Protection by Design and by Default → EU General Data Protection Regulation Article 25 and Recital 78 → U.K. Information Commissioner's Office guidance on data protection by design and default → Privacy by design guide from Spain's data protection authority, the Agencia Española de Protección de Datos → Secure Controls Framework's guide to cybersecurity and data privacy by design principles → ICO's "Privacy in the product design lifecycle" article

DATA GOVERNANCE

Principle	IAPP resources	Regulatory guidance and other resources
Nondiscrimination, bias and fairness	→ Privacy and AI Governance Report → "Privacy and responsible AI" article → "The AI Act's debiasing exception to the GDPR" article → "Well-intentioned debiasing methods that hamper AI governance tools" article → "Data bias: AI fairness and the need for diversity in privacy/data/AI governance" web conference recording → "What is the role of privacy professionals in preventing discrimination and ensuring equal treatment?" article → "Utilizing PIAs to limit institutional discrimination and bias" article → "The AI Act's debiasing exception to the GDPR" article → "Antidiscriminatory algorithmic accountability: Transparency by design in AI-powered decision-making" article → "Biased AI systems face the music: Analyzing the FTC's Rite Aid enforcement" article → "Well-intentioned debiasing methods that hamper AI governance tools" article → "Using sensitive data to prevent AI discrimination: Does the EU GDPR need a new exception?" article	→ ICO's guide to U.K. GDPR Article 5 → ICO's "How do we ensure fairness in AI?" article → U.S. Federal Trade Commission's decision that AI developers and companies are accountable for AI being transparent, fair and empirically sound → EU GDPR Article 5, Recital 39 and Recital 60 → NIST's Special Publication 1270 → Joint statement on enforcement efforts against discrimination and bias in automated systems by U.S. federal agencies, namely the Department of Justice, FTC, Equal Employment Opportunity Commission and Consumer Financial Protection Bureau → Organisation for Economic Co-operation and Development's AI Principle 1.2 → UNESCO's Recommendation on the Ethics of AI, Principles 28, 29 and 30 → Singapore's AI Verify principle of ensuring fairness → EU GDPR Article 9 and Recital 51 → ICO's "What about fairness, bias and discrimination?" article → U.S. Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI

DATA GOVERNANCE

Principle	IAPP resources	Regulatory guidance and other resources
Transparency	→ "Privacy and responsible AI" article → "Consumers say trust depends on transparency" article	→ EU GDPR Article 5, Article 12, Recital 39, Recital 58 and Recital 60 → ICO's guide to U.K. GDPR Article 5 → ICO's "How do we ensure transparency in AI?" article → FTC decision that AI developers and companies are accountable for AI being transparent, fair and empirically sound → EU AI Act Chapter 3 and Article 50 → NIST's AI RMF Section 3.4 on accountable and transparent AI → China's Interim Measures for the Management of Generative AI Services, Articles 10 and 11 → Singapore's AI Verify principles of transparency and explainability
Human oversight/accountability	→ Accountability topic page → Privacy and AI Governance Report → "Privacy and responsible AI" article → "Why demonstrable accountability matters" article → "CIPL report explores 'the age of accountability'" article	→ Centre for Information Policy Leadership's organizational accountability resources → CIPL's AI and Data Protection: Delivering Sustainable AI Accountability in Practice report → ICO's Accountability Framework → National Telecommunications and Information Administration's AI Accountability Policy Report → UNESCO's Recommendation on the Ethics of AI, Principles 35 and 36 → OECD's AI Principle 1.5 → Singapore's AI Verify principle of ensuring proper (human) management and oversight of the AI system → European Commission's Guidelines on the Ethics of AI

DATA GOVERNANCE

Principle	IAPP resources	Regulatory guidance and other resources
Explainability/interpretability	→ "The privacy pro's guide to explainability in machine learning" article → "5 things to know about AI model cards" article → "AI governance: What is being governed?" article → "Explaining model disgorgement" article	→ Royal Society's policy briefing on explainable AI → ICO's "Explaining decisions made with AI" white paper → NIST's Four Principles of Explainable AI assessment → NIST's AI RMF Section 3.5 on explainable and interpretable AI

CONSUMER PROTECTION

Principle	IAPP resources	Regulatory guidance and other resources
Individual rights	→ Definitions of the right of access, right to object, right to rectification, right to be forgotten, right to restriction and right to data portability → "Data portability in the EU: An obscure data subject right" article → "Regulating for AI success" article → "The AI Act's debiasing exception to the GDPR" article → "Top 10 operational responses to the GDPR Part 7: Accommodating data subjects' rights" article → "How to comply with the right to erasure" article → "The right to be forgotten: Managing GDPR risk of data erasure for businesses" web conference recording	→ GDPR Articles 12-23 and Recital 59 → ICO's "How do we ensure individual rights in our AI systems?" article → Bird & Bird's guide to subject access, rectification and portability under the GDPR → CIPL's "Data subject rights under the GDPR in a global data driven and connected world" white paper → Ireland's Data Protection Commission guide to access rights and responsibilities under the GDPR

CONSUMER PROTECTION

Principle	IAPP resources	Regulatory guidance and other resources
Supervision and enforcement	→ Enforcement topic page → Global privacy and data protection enforcement database → "AI regulatory enforcement around the world" article → "EDPB coordinated enforcement sheds light on DPO compliance" article → "Evaluating the use of AI in privacy program operations" article → "Practical considerations from EU enforcement" article series, Part 1 and Part 2 → GDPR enforcement priorities infographic	→ GDPR Article 51 and Articles 77-84 → FTC's "AI (and other) companies: Quietly changing your terms of service could be unfair or deceptive" article → European Commission's AI Office → Joint statement on enforcement efforts against discrimination and bias in automated systems by U.S. federal agencies, namely the DOJ, FTC, EEOC and CFPB

RELATING TO DATA AND SECURITY

Principle	IAPP resources	Regulatory guidance and other resources
Data/Development life cycle management	→ "Establishing governance for AI systems" article → "Evaluating the use of AI in privacy program operations" article → "Data life cycle: The privacy path less chosen" web conference recording → "Practical privacy: operationalizing the data governance life cycle" web conference recording → "Privacy Program Management, Third Edition" by Russell Densmore, CIPP/E, CIPP/US, CIPM, CIPT, FIP	→ IBM's overview of AI model life cycle management → NIST's AI RMF AI life cycle → OECD's framework for classifying AI systems → OECD's guidance on the AI system life cycle → U.S. General Services Administration's guide to understanding and managing the AI life cycle

RELATING TO DATA AND SECURITY

Principle	IAPP resources	Regulatory guidance and other resources
Training	→ Training overview → "IAPP releases AI Governance Professional training course" article → "Building a privacy layer for AI" article → "Proposed data provenance standards aim to enhance trustworthiness of AI training data" article → "Privacy attacks on AI systems: A current concern for organizations" article → "AI beyond the hype: Focus on the data" article → "Training AI on personal data scraped from the web" article → "6 ways privacy awareness training will transform your staff" white paper → "Must-have privacy training features for your team" white paper	→ EU GDPR Article 39 and Recital 97
Data collection	→ Privacy and Consumer Trust Report → "Training AI on personal data scraped from the web" article → "Privacy and responsible AI" article → "How existing data privacy laws may already regulate data-related aspects of AI" article → "Most consumers want data privacy and will act to defend it" article → "No AI without IP" video conference recording	→ EU GDPR Article 13, Article 14 and Article 22 → IBM's report on data quality, AI performance and trust → ICO's joint statement on web scraping in conjunction with other international data protection and privacy authorities → International Organization for Standardization's ISO 8000
Data processing	→ "How existing data privacy laws may already regulate data-related aspects of AI" article	→ EU GDPR Article 5, Article 6, Recital 39 and Recital 40 → Harvard Kennedy School Carr Center for Human Rights Policy's "The Ethical Use of Personal Data to Build AI Technologies" discussion paper

RELATING TO DATA AND SECURITY

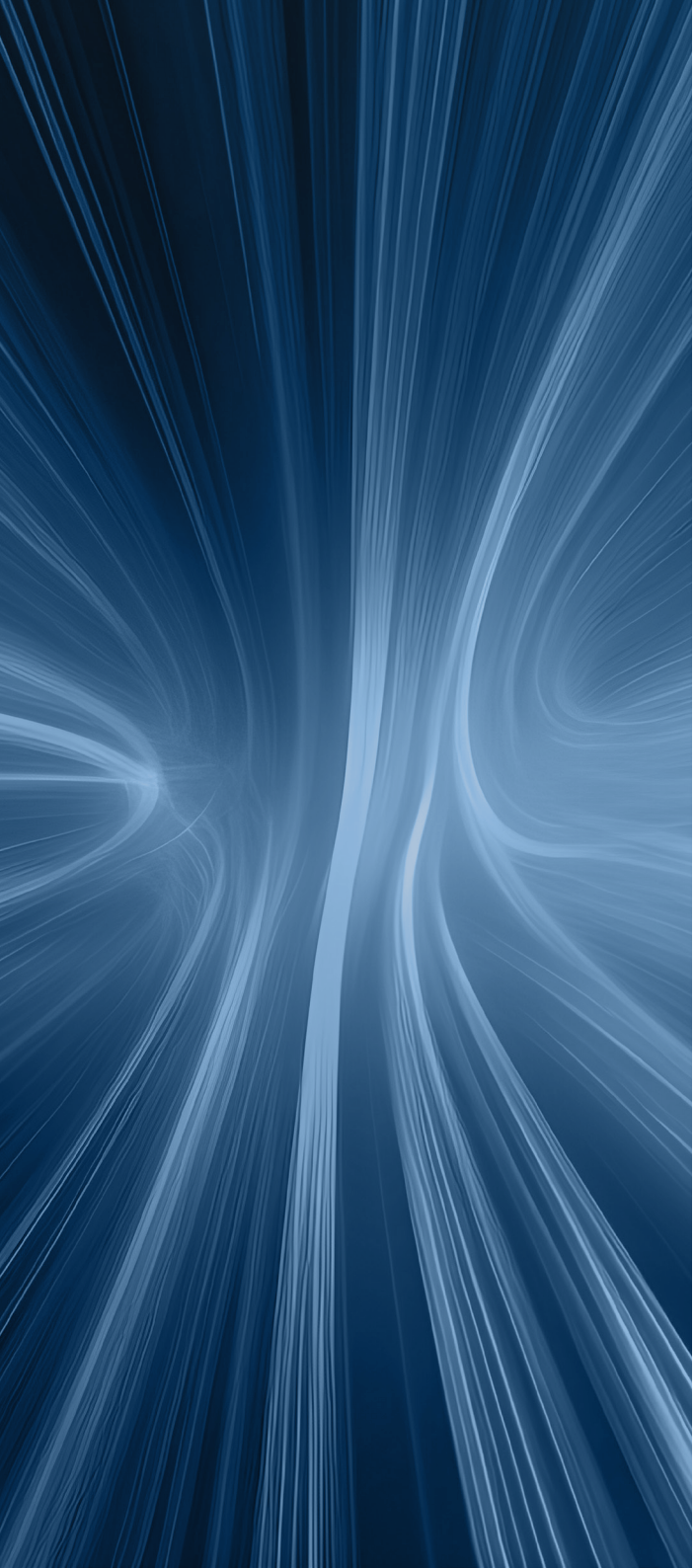
Principle	IAPP resources	Regulatory guidance and other resources
Impact assessments	→ Privacy and AI Governance Report → Data protection and privacy impact assessment topic page → Privacy impact assessments definition → "How privacy professionals can assess risks in AI, algorithms and automated decision-making systems" article → "Assessing risk: Determining the appropriate risk flags for your privacy risk assessments" article	→ EU GDPR Article 35, Recital 76, Recital 77, Recital 84 and Recital 90 → U.S. Chief Information Officers Council's algorithmic impact assessment tool → U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology's and Office for Civil Rights' security risk assessment tool → EU AI Act Chapter 3 on high-risk AI systems → UNESCO's policy area on ethical impact assessments
Incident response	→ Incident and breach management topic page → "Benchmarking your privacy incident management program" article series → "How to evaluate a privacy-incident response program" article → "AI incident response plans: Not just for security anymore" article → "Beyond data breach: Why every incident matters" article	→ EU GDPR Article 33, Article 34 and Recital 86 → EU AI Act Article 73

RELATING TO DATA AND SECURITY

Principle	IAPP resources	Regulatory guidance and other resources
Risk management	→ Incident and breach management topic page → Privacy Risk Study 2023 → "The skill set needed to implement a privacy risk management framework" white paper → "Shaping the future: A dynamic taxonomy for AI privacy risks" article → "Third-party liability and product liability for AI systems" article → "Performant risk mitigation for AI and LLMs" article → "What AI can learn from privacy: Recommendations for AI governance" web conference recording → "3 steps to elevating your third-party risk management process" web conference recording → "Managing privacy in the era of generative AI" web conference recording	→ EU GDPR Article 35, Article 36 and Recital 78 → Deloitte's survey on global risk management → NIST's AI RMF → NTIA's press release on audits and auditors for high-risk AI systems → Canada's Bill C-27 → EU AI Act

RELATING TO DATA AND SECURITY

Principle	IAPP resources	Regulatory guidance and other resources
Security	→ Incident and breach management topic page → Privacy and Consumer Trust Report → "From silo to synergy between cybersecurity and privacy in Europe" web conference recording → "Building the next generation of security and privacy professionals" white paper	→ EU GDPR Article 32, Recital 83, Recital 85 and Recital 86 → BakerMcKenzie's Global Privacy and Security Handbook → ICO's "How should we assess security and data minimisation in AI?" article → U.S. Executive Order on the Safe, Secure and Trustworthy Development and Use of AI → Joint guidelines for secure AI system development by the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, U.K. National Cyber Security Centre, and other international partners → CISA's "Software must be secure by design, and AI is no exception" article → U.K. Department for Digital, Culture, Media and Sport's "Exploring organisational experiences of cyber security breaches" white paper → EU NIS2 Directive → EU AI Act's specific security requirements for high-risk AI systems and general-purpose AI models → NIST's AI RMF Section 3.3 on secure and resilient AI → NIST's Cybersecurity Framework → Singapore's AI Verify principle of ensuring safety and resilience of the AI system



Contact

Joe Jones
IAPP Research and Insights Director
jjones@iapp.org

Uzma Chaudhry
IAPP AI Governance Center Fellow
uchaudhry@iapp.org

Ashley Casovan
IAPP AI Governance Center Managing Director
acasovan@iapp.org

For further inquiries, please reach out to research@iapp.org.

Follow the IAPP on social media

Published May 2024.