EVERSHEDS SUTHERLAND

Updata

Protecting your interests

Your quarterly Data, Privacy and Cybersecurity update

EVERSHEDS SUTHERLAND

Updata

Your quarterly Data, Privacy and Cybersecurity update

Edition 29

Connect

Welcome to the latest edition of Updata!

This edition covers **July to September 2025** and is full of newsworthy items, including on the following topics:

- **Artificial Intelligence (AI)** – see our Global AI Regulatory Update (August 2025), the EU's consultation on its draft AI Act transparency provision guidelines and code of practice, the final version of the EU's GPAI Code of Practice, in the US California's Transparency in Frontier AI Act, NIST's concept paper on securing AI systems as well as the Italian implementation of the EU AI Act and the Dutch DPA's report on AI and algorithms
- **Smart data laws** – see EU Data Act and local legislation requirements, the EDPB's statement on data sharing under the Data Act, progress on the phased commencement of the UK's Data (Use and Access) Act 2025 and the UK government's response to its data intermediaries consultation
- **Data security** – an uptick in regulatory scrutiny of security practices, as well as new incident reporting guidance in Italy, China and Hong Kong, notable fines in Italy and Spain, the UK's proposed ban on ransomware payments, new ICO encryption guidance and NCSC guidance on AI and cyberthreats as well as a plethora of regulatory reports highlighting rising cyber threats in Lithuania and Singapore
- **Regulatory scrutiny over data sharing practices** – including in the Netherlands a financial institution being ordered to disclose its data sharing practices to data subjects and in the US the Health and Human Services being sued for sharing sensitive health data with the Department of Homeland Security
- **Children and data** – such as the European Commission's newly published guidelines and prototype age verification app to help service providers comply with the DSA, the Bulgarian DPA's recommendations on school and nursery CCTV, the EDPB's opinion on the interplay between the DSA and GDPR and NationalDataSecurityStandardsSystem2025e, China's draft requirements on protection of personal information for minors' products and services and in the UK DSIT's Final Statement of Strategic Priorities for Online Safety
- **Health and biometric data** – interesting developments in the United States including California's new Privacy Health Data Location and Research Act, amendments to Virginia's Consumer Protection Act and Colorado's Privacy Act, new guidance in Germany on employee health data, and in Portugal a new working group for defining health data retention periods, enforcement action against an employer in Slovakia, and regulatory reports highlighting biometrics as an area of focus in Italy, the Netherlands and the UK

Don't forget to check out our other recent updates:

- Webinar: Preparing for the EU Data Act: What you need to know
- Article: US midyear roundup of privacy and cybersecurity regulation, enforcement, and litigation
- Webinar and Guide: Understanding the UK Data (Use and Access) Act 2025 and Guide to the UK's Data (Use and Access) Act 2025

Michael Bahar
Co-Lead of Global Cybersecurity and Data Privacy

Paula Barrett
Co-Lead of Global Cybersecurity and Data Privacy

Rachel Reid
Head of Artificial Intelligence, US

Co-Lead of Global Cybersecurity and Data Privacy

Updates by region

General EU and International

ECJ confirms pseudonymous data is not always personal data

In its September 4, 2025 judgment in *Case C-413/23 P European Data Protection Supervisor v Single Resolution Board*, the ECJ ruled, among other things, that pseudonymised data will not, in all cases and for every person, be regarded as personal data.

Facts

The Single Resolution Board (SRB) (the EU's central resolution body for failing banks) conducted a consultation process which involved shareholders and creditors submitting their comments along with certain supporting documentation (including proof of identity and proof of ownership of capital instruments). Each comment was allocated an alphanumeric code and separated from the personal information of its author. The comments and the alphanumeric codes were shared with a third party audit firm to be examined. The audit firm was not given the data required to link any comment to its individual author.

Affected shareholders and creditors lodged a complaint against the SRB, alleging infringement of the transparency obligations contained in the EU Institutions General Data Protection Regulation 2018/1725 (EU Institutions GDPR). The European Data Protection Supervisor (EDPS) agreed and issued a reprimand.

The SRB asked the EDPS to review its decision, contesting that the information it shared with the audit firm was not personal data because the audit firm did not have the requisite data key to attribute the comments to their authors. The EDPS subsequently adopted a revised decision and decided not to use its corrective powers but recommended the SRB amend its consultation privacy notice to include all potential recipients of the data. The SRB brought an action with the EU General Court to annul the EDPS' revised decision. The General Court ruled in favour of the SRB and annulled the EDPS's decision. The EDPS appealed to the ECJ.

Ruling

The ECJ ruled that:

- personal opinions are necessarily closely linked to – and therefore "relate to" – the person expressing the opinion
- pseudonymised data will not, in all cases and for every person, be regarded personal data – pseudonymised data is not personal data where pseudonymisation effectively prevents the data subject from being identified
- for the purposes of complying with the notice provision requirements of the GDPR, the identifiability of the data subject must be assessed at the time of collection of the data and from the point of view of the controller

Impact: Although this case related specifically to facts governed by the EU Institutions GDPR, the provisions relating to the definition of personal data contained in the GDPR and the EU Institutions GDPR are the same and are interpreted in the same way. So the judgment is relevant to organisations processing personal data subject to the GDPR.

The judgment confirms the "relative" nature of personal data. The ECJ also did not discuss specifically how its interpretation should be applied to recipients of data acting as a *processor* on behalf of the disclosing controller (as opposed to a separate controller). It's also unclear how the judgment will be interpreted for the purposes of intra-group data sharing of pseudonymous data.

In terms of practical steps to take, organisations should revisit records of processing activities to establish data flows within and outside organisations and review privacy notices to ensure that pseudonymisation activities and recipients of such data are properly documented. Where pseudonymisation is being carried out, organisations should ensure that technical and organisational measures are taken to ensure its robustness, i.e. that the data cannot be attributed to an identifiable person. This will be key if asserting that such data is not personal data in a recipient's hands.

Contact a specialist in our International team

EU-US Data Privacy Framework remains valid

On September 3, 2025 the General Court of the EU rejected a challenge brought by Philippe Latombe against the European Commission's adequacy decision for the EU-US Data Privacy Framework (DBF), finding that the US framework offers "*substantially equivalent*" protection to EU standards. The decision confirms that the DPF remains a valid transfer mechanism and provides legal certainty for transatlantic data transfers.

Impact: For further information, see our Flash update from **Paula Barrett**, **Caroline Lyannaz** and **Clemence de Chanaud**.

Contact a specialist in our International team

EDPB publishes opinion on interplay between DSA and GDPR

On September 12, 2025 the European Data Protection Board (EDPB) released draft guidelines on the interplay between the DSA and the GDPR, for consultation.

By way of reminder, the Digital Services Act (DSA) applies to online intermediary services and aims to create a safer online environment.

DSA provisions which relate to the GDPR, include among others: (i) content moderation; (ii) notice-and-action systems that help individuals or entities report illegal content; (iii) recommender systems used by online platforms to automatically present specific content to the users of the platform with a certain relative order or prominence; (iv) provisions to ensure a high level of privacy, safety, and security of minors and prohibiting that profile-based advertising using their data is presented to them; (v) transparency of advertising by online platforms; (vi) prohibition of profiling-based advertising using special categories of data.

The guidelines clarify how both regulations should be interpreted and applied consistently. The guidelines emphasise the need for legal certainty and coherent application by supervisory authorities, to protect individuals' rights and avoid regulatory inconsistencies.

Cooperation between digital services and data protection authorities is essential for effective enforcement and to prevent gaps or overlaps in regulation.

The EDPB also took the opportunity to note it is working with other regulators across the cross-regulatory landscape, including with the European Commission to develop joint guidelines on the interplay between the Digital Markets Act and the GDPR, as well as on joint guidelines on the interplay between the AI Act and EU data protection laws.

Impact: The consultation ends on October 31, 2025. Interested organisations should consider responding.

Contact a specialist in our International team

EU Data Act and local legislation requirements

The EU Data Act is entering into force in September 2025 and while the regulation sets a directly applicable legal framework across all Member States, certain aspects require national legislative action to ensure full and consistent implementation.

In this post, we break down what EU Member States must cover in their local legislation, what flexibility they have, and how businesses should prepare.

The Data Act contains several areas that require Member States (MS) to complement the regulation with national laws & regulations. These cover:

- **penalties** – effective, proportionate and dissuasive penalties should be set MS level with national authorities designated responsible for monitoring and compliance. These regimes should be notified to the European Commission by 12 September and MS are encouraged to follow European Data Innovation Board (EDIB) recommendations to mitigate fragmentation
- **competent authorities** – these should be appointed to oversee the regulation on matters such as fair data access obligations between businesses, handling user access rights and overseeing the switching of cloud service and interoperability obligations
- **dispute resolution mechanisms** – the Data Act encourages out of court resolution mechanisms so MS may offer the option to engage in Alternative Dispute Resolution (ADR) by establishing certified bodies

Due to these aspects where local variations may arise, businesses operating in multiple MS should:

- start monitoring national legislative developments
- identify which national bodies will oversee enforcement in your key markets
- prepare for differences in sanctions and supervisory approaches across jurisdictions

Beyond compliance, the Data Act presents a strategic opportunity to unlock value from data assets. Companies can leverage new access rights to improve product development, negotiate better supplier terms, and enhance customer experience. Sector-specific readiness is key: manufacturers of connected products must prepare for user access and cloud switching obligations, while healthcare and energy providers should anticipate public emergency data access requests.

Impact: For further information on this see: The EU Data Act & Local Legislation… What the EU Member States need to cover in local legislation?

You may also be interested in: EU Data Act – An overview.

Contact a specialist in our International team

Consultation on guidelines and code of practice on transparency provisions of EU AI Act

On September 4, 2025 the European Commission launched a consultation on guidelines and a code of practice on the AI transparency provisions under Article 50 of the EU AI Act.

These provisions apply from August 2, 2026 and are intended to ensure that people are aware that they are interacting with or being exposed to AI. They require deployers and providers of certain AI systems to inform people when they interact with an AI system or view AI generated or manipulated content.

Under the AI Act the European Commission is required to issue guidelines on the practical implementation of these obligations, and the EU AI Office is required to facilitate the development of codes of practice on implementation of the obligations relating to detection and labelling of AI generated or manipulated content.

Responses to the consultation are sought from stakeholders, including providers and deployers of interactive and generative AI systems or biometric categorisation and emotion recognition systems, private and public sector users of such AI systems, academia and research institutions, civil society organisations, governments, supervisory authorities and the general public.

Alongside the consultation, the European Commission has opened a call for expressions of interest to participate in the process of creating the code of practice.

Impact: The consultation and the call for expressions of interest closed on October 2, 2025.

Contact a specialist in our International team

Call for evidence on Chips Act 2.0

On September 5, 2025 the European Commission launched a call for evidence in connection with its review and proposed revision of the Chips Act to create "Chips Act 2.0".

The Chips Act is intended to support and enhance semiconductor tech manufacture and investment in the EU and to pre-empt chip crises and shortages. Whilst considering the Chips Act to be fit for purpose, the Commission states that "*further steps are necessary to strengthen the EU's role in a wide selection of chips technologies and the full semiconductor value chain including materials, equipment, design and manufacturing*".

The two key objectives of Chips Act 2.0 are to:

- reduce EU dependency on third countries for supply of semiconductor chips, in particular by increasing EU manufacturing capacity for advanced semiconductors for critical sectors such as defence, security, automotive, space and high-performance computing
- improve EU insight into the global semiconductor ecosystem including supply chains and key market actors, to facilitate security of supply and crisis management

Impact: Interested parties are invited to share their views by November 28, 2025. Suppliers and users in this sector should consider responding to help shape policy in this area.

Contact a specialist in our International team

Call for evidence on simplification of data, cybersecurity and AI rules

On September 16, 2025 the European Commission launched a call for evidence on how to simplify its legislation in relation to data, cybersecurity and AI, as part of the forthcoming Digital Omnibus. This is part of the EU drive to reduce administrative burdens and compliance costs for business, and follows consultations on the Data Union Strategy, the Cybersecurity Act and the Apply AI Strategy.

Impact: Responses were due by October 14, 2025 and the EU Commission plans to adopt the Digital Omnibus in the last quarter of 2025.

Contact a specialist in our International team

European Commission consultation on revised Technology Transfer Block Exemption Regulation

On September 11, 2025 the European Commission launched a consultation on its draft Technology Transfer Block Exemption Regulation (TTBER), and accompanying guidelines, that are intended to replace the existing TTBER when it expires on April 30, 2026.

The TTBER exempts technology transfer agreements (under which one party permits another to use its technology rights to produce goods or services) that meet certain conditions from the Article 101 prohibition on anti-competitive agreements.

The main changes that the European Commission proposes to make to the existing TTBER and guidelines include:

- new definitions of active and passive sales to reflect the corresponding definitions in the Vertical Agreements Block Exemption Regulation
- greater clarity on market share thresholds and an extension of the grace period for continued application of the TTBER when market shares increase during the term of an agreement
- guidance to provide for increased transparency on the technology rights included in technology pools
- new guidance on the competitive assessment of licensing negotiation groups
- new guidance on data licencing

Impact: Consultation closes on October 23, 2025. Businesses operating in the EU that engage in licensing industrial property rights should consider responding to share their views on the proposed changes.

Contact a specialist in our International team

Opportunity to feedback on EU Digital Markets Act

On August 26, 2025 the European Commission opened a consultation as part of its first review of the effectiveness of the Digital Markets Act in achieving its objectives of "*ensuring contestable and fair digital markets and on its readiness to face emerging challenges*".

Impact: Open until September 24, 2025, views were sought on whether the aims of the DMA are being met (particularly with regard to SMEs and end users) and included an AI questionnaire on the implications of the DMA on that sector.

Contact a specialist in our International team

Digital Services Act decision

On September 10, 2025 the General Court of the EU held that the European Commission must adopt a delegated act specifying the method for calculating the average monthly service recipients of online platforms under the Digital Services Act.

Contact a specialist in our International team

Global AI Regulatory Update

In our quarterly global AI bulletin, we look at:

- Asia

  Hong Kong: effects of unsupervised AI-use risk on data privacy and security; new article published on creating an internal generative AI policy

  Singapore: new initiatives and tools launched for AI and data protection

- Europe – proposal to adhere to the Convention on AI; Commission launches AI tools for researchers and industry; General-Purpose AI Code of Practice published; guidelines for providers of general-purpose AI models published; European Commission publishes GPAI Training Data Summary Template; European Commission allegedly withdraws AI liability and patents proposal
- UK – regulators guide firms on responsible AI use; compliant use of AI in advertising – the UK's stance; Ofcom's updates on online safety and AI; AI tools set to transform UK audit practices; howz can tech firms help users spot deepfakes?; Compute Roadmap – advancing AI in the UK; Government report on the impact of social media algorithms and generative AI (GenAI)
- US – Department of Commerce renames and reforms AI Safety Institute; Senate decides not to impose AI law moratorium; White House issues AI Action Plan and executive orders; California regulates business use of automated decision-making technology; Colorado to convene special legislative session to consider implementation changes to pioneering AI law; National Institute of Standards and Technology is developing resources to meet demand for additional AI guidance; lawmakers in Texas enact the Texas Responsible Artificial Intelligence Governance Act
- Global – harmonized AI standards to reduce fragmented global rules

In addition see Unlocking the benefits of AI adoption in the UK public sector: the evolving landscape – where we review recent AI-focussed private sector partnerships entered into by the UK government, evolving policy initiatives and their wider impact on public sector customers and suppliers.

Contact a specialist in our International team

Global legal risks for data centers

As data centers become the backbone of the global digital economy, their legal and environmental footprint is drawing unprecedented scrutiny. This is no longer a niche infrastructure issue, it's a strategic legal priority. International courts are redefining States' environmental obligations under international law, with the anticipation that regulatory frameworks will in time shift in response as well. These new developments confirm that environmental law obligations are increasingly becoming legally actionable. Businesses must now reassess how they invest, operate, and protect their interests in this space. From energy and water consumption to treaty protections and dispute resolution, the legal risks are growing. These converging pressures are reshaping the risk landscape for data center investments and demand careful consideration at the highest strategic level.

Impact: To read more see: Global Legal Risks for Data Centers

With thanks to Wesley Pydiamah and Dimitrios Papageorgiou

Contact a specialist in our International team

Progress report on establishing pan European systemic cyber incident coordination framework

The European Systemic Risk Board (ESRB) has been reviewing the implementation of its recommendations by EU authorities of a pan-European systemic cyber incident coordination framework (EU-SCICF) under the Digital and Operational Resilience Act (DORA).

It had previously recommended that authorities should prepare to develop an EU-wide response to major cross-border cyber threats affecting the financial sector. In its report (published on August 12, 2025 but written in December 2024) it concludes that overall compliance with this recommendation is good but two points for improvement are identified for authorities to ensure appropriate resource is in place and for the EU-SCICF to be operational from January 2025 and further developed in a "timely manner". The ESRB will continue to monitor progress of the transition from concept to practice and encourages more investment in resource and IT to aid this process.

Contact a specialist in our International team

Dubai Introduces AI Transparency Framework

The Dubai Future Foundation has unveiled the **Human-Machine Collaboration Classification (HMC)** system to enhance clarity around AI involvement in research and design – learn more from our Linked In post

Contact a specialist in our International team

ENISA technical guidance on NIS2 implementing regulation compliance

On June 26, 2025 the European Union Agency for Cybersecurity (ENISA) published technical guidance to help organisations in the digital infrastructure, ICT service management and digital provider sectors implement cybersecurity measures to comply with the NIS2 Directive, as defined in the Commission Implementing Regulation 2024/2690.

NIS2 is designed to help organisations protect themselves against cyber threats and to ensure that the EU's critical infrastructure is more secure and robust. It applies to entities operating in sectors that are critical to society and economy, including health, energy, transport, waste, digital services and ICT service management. The implementing regulation sets out the technical and methodological cybersecurity risk-management measures which in-scope organisations are required to take, as well as what constitutes a "significant" cybersecurity incident that needs to be reported to national authorities.

Impact: This new technical guidance is essential reading for all in-scope organisations, namely domain name system service providers, top-level domain name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers and managed security service providers, providers of online marketplaces, online search engines and social networking services platforms and trust service providers. It includes guidance on what to consider when implementing a requirement, the types of evidence that demonstrate a requirement is in place, and mapping against industry good practice, European and international standards, and national frameworks. However, it is guidance only and is not legally binding.

Contact a specialist in our International team

Joint Action to strengthen navigation resilience for critical infrastructure

On July 10, 2025 the UK and France announced a new partnership to enhance the resilience of Positioning, Navigation and Timing (PNT) systems used across critical national infrastructure. The agreement responds to growing concerns around signal jamming and interference, tactics increasingly seen in state-led cyber and electronic warfare. Experts from both countries will work together on developing navigation and timing systems that are less vulnerable to disruption.

This collaboration forms part of a broader UK–France strategic tech relationship, which also includes long-standing cooperation on AI governance, research, and infrastructure. The agreement is expected to accelerate joint R&D, public-private investment, and procurement activity related to resilient PNT systems. Businesses operating in defence tech, AI, telecoms, and infrastructure services should monitor potential contracting and cross-border collaboration opportunities.

Contact a specialist in our International team

European Commission proposes to conclude and sign UN Convention against Cybercrime

On July 16, 2025 the European Commission proposed to sign and conclude the United Nations Convention against Cybercrime to help in the international fight against online crime and to facilitate access to digital evidence on serious crimes.

Among the reasons cited by the Commission for the proposals, are that the Convention:

- enables cooperation with countries not party to the Budapest Convention, closing gaps that cybercriminals exploit as safe havens
- establishes mechanisms for extradition, mutual legal assistance, and cross-border access to electronic evidence, streamlining responses to cybercrime
- addresses modern cyber offences such as online child sexual abuse, grooming, and non-consensual sharing of intimate images

- includes provisions to ensure respect for human rights, including data protection and privacy, aligning with EU legal standards

The Council will now discuss and decide on the adoption of the proposed decisions to enable the EU to sign and conclude the Convention. The conclusion of the Convention will also require the consent of the European Parliament.

Contact a specialist in our International team

European Commission releases draft EU-UK adequacy decision for transfers of personal data

On July 22, 2025 the European Commission launched the formal process to renew the free flow of personal data from the EEA to the UK, by releasing two draft adequacy decisions under the GDPR and the Law Enforcement Directive. The Commission's decision follows its conclusion that the UK's legal framework continues to provide data protection safeguards essentially equivalent to those provided by the EU.

The draft decisions have been sent to the European Data Protection Board (EDPB) for its opinion. Before adopting the decisions, the Commission will also seek approval from a committee composed of representatives of the EU Member States. The European Parliament also has a right of scrutiny over adequacy decisions.

On June 24, 2025 the Commission extended the 2021 GDPR and LED adequacy decisions by six months, until December 27, 2025, to allow time for the Commission to assess the UK's Data Use and Access Act.

Once approved, the adequacy decisions will enable organisations to transfer personal data from the EEA to the UK without needing to put in place an appropriate safeguard such as standard contractual clauses and without needing to conduct a transfer impact assessment.

Contact a specialist in our International team

Developments regarding GDPR simplification proposals

On July 3, 2025 the EDPB adopted the Helsinki Statement setting out new initiatives to enable more straightforward GDPR compliance, improve dialogue between stakeholders, strengthen consistency and develop cross-regulatory cooperation in the new digital regulatory landscape.

The initiatives include new tools to help make GDPR application easier including: a suite of templates for organisations building on national guidance; a common template for data breach notifications for data protection authorities, in support of a possible cross-regulatory European notification solution; and easy to use resources, such as checklists, how-tos and FAQs, to help organisations understand their key obligations.

The EDPB also committed to enhance consistency of the application and enforcement of the GDPR by DPAs, including: collating the positions taken on priority issues in national guidance, decisions and court judgments, to produce 'case law'-style publications to help organisations understand concrete positions taken by DPAs; regular follow-ups on guidelines to ensure effectiveness and consistent application; continued efforts to align national and EDPB guidance where inconsistencies are identified; greater harmonisation of enforcement; and when strategic cross-border topics arise, prioritising the preparation of EU positions to ensure consistency by design.

On July 9, 2025 the EDPB and European Data Protection Supervisor published Joint Opinion 01/2025 on the Proposal for a Regulation on simplification measures for SMEs and SMCs, in particular the record-keeping obligation under Art. 30(5) GDPR. We commented on the GDPR simplification measures in our June edition. The proposals look to remove the Article 30 recordkeeping obligation SMEs/SMCs employing fewer than 750 persons, and which do not engage in processing activities likely to result in a high risk to individuals. The joint opinion provides broad support for the proposals, and includes a number of recommendations for the co-legislators, including to clarify in the recitals that, where the Article 30(5) GDPR derogation applies, a record of processing would only be mandatory for those processing activities 'likely to result in a high risk'.

Contact a specialist in our International team

Commission seeks comments on key EU data legislation

On July 1, 2025 the European Commission opened a number of surveys to garner comments on three EU data regulations: the Free Flow of Non-Personal Data Regulation (FFDR), Open Data Directive (ODD), and Data Governance Act (DGA).

The consultations explored:

- how clearly and effectively the FFDR is applied in practice, and whether it successfully removes barriers to the free movement of non-personal data across EU borders by eliminating unjustified data localisation requirements
- in the context of the ODD, how public sector data is being reused, the impact on innovation and the economy, and whether legal or technical barriers remain
- how well the DGA supports trusted data sharing, including the role of data intermediaries, data altruism, and safeguards for international data transfers – researchers, data analysts, and industry professionals were invited to participate

The consultations ended on July 25, 2025.

Contact a specialist in our International team

EDPB adopts statement on Data Act's data sharing MCTs

On July 8, 2025 the EDPB adopted a statement providing non-exhaustive and high level comments on the European Commission's Recommendation on draft non-binding model contractual terms (MCTs) on data sharing under the Data Act (version of May 22, 2025).

The EDPB makes the following recommendations to the Commission:

- clarify the application of the MCTs to contractual parties of different "standing" (e.g. natural persons which may or not be data subjects for the purposes of the GDPR), and consider the development of different MCTs depending on whether the user is or is not the data subject
- restrict compensation mechanisms in the annexes II and III to the use of non-personal data, in accordance with Articles 4(13) Data Act
- include definitions section to clarify the meaning of particular concepts such as 'consumption data', and to cross-reference to ensure the information boxes signpost to supporting statutory references in the Data Act and GDPR for legal coherence
- make it more explicit in the MCTs that existing data protection and privacy laws including the GDPR and ePrivacy Directive shall prevail over the contractual terms in case of conflict
- make it clear in the information boxes that the contracting parties may need to take certain additional steps to ensure compliance with the GDPR
- amend the MCTs to address consumer vulnerability and the power asymmetries, which emerge in the digital economy, and amend the penalties to ensure proportionality and so as not to infringe on the rights of data subjects

Contact a specialist in our International team

AI – final Code of Practice and guidelines for general-purpose AI

On July 10, 2025 the European Commission published the final version of the General-Purpose AI GPAI Code of Practice (Code).

The Code (which is split into three chapters covering Transparency; Copyright; and Safety and Security) is designed to help industry comply with the EU AI Act provisions on GPAI ahead of binding obligations entering into force on August 2, 2025. A FAQ is also available to support understanding covering:

- what the Code is – a voluntary tool designed to help providers of GPAI models demonstrate compliance with the EU AI Act
- its benefits – all providers of GPAI models in the EU are invited to comply with the Code which aims to provide a "simple and transparent way" to demonstrate compliance with the EU AI Act. It does not go beyond the requirements set out in law
- next steps – Member States and the EU Commission will assess the adequacy of the Code (developed by experts at the AI Office engaging with stakeholders). It will need to be approved and undergo an "adequacy assessment" to confirm alignment with the EU AI Act. This is unlikely to happen before August 2, 2025. Therefore, the EU Commission has granted a grace period to signatories of the Code. They will be assumed to be acting in good faith and not face enforcement action until August 2, 2026. Any providers with GPAI already on the EU market have until August 2, 2027 to comply. The Commission is also considering allowing companies to sign selected parts of the Code to attract more signatories

- review process – the Code will be reviewed at least every 2 years (this may adjust to align with technological developments)

On July 18, 2025 the European Commission published the guidelines on the scope of obligations for providers of gpAI under the AI Act.

The purpose of this guidance is to ensure legal certainty for stakeholders throughout the AI value chain by clearly outlining when and how they must meet these obligations. They focus on four key topics of:

- what a gpAI model is
- who the 'provider' is (the developer/commissioner of the model who "places it" on the EU market – the guidance explains the scope of the "placing it" requirement)
- exemptions (certain exemptions for models released under free / open source licences for example); and
- enforcement obligations (the Commission will take action from August 2, 2026 and use the first year to work with notifying providers of gpAI on their adherence to the Act and Code)

A FAQ has been developed to support the guidelines which covers:

- the legal obligations on providers from August 2, 2025:
  - maintaining technical documentation on the model
  - providing information to downstream AI system providers so they understand the capabilities and limitations of the model
  - implementing a Union compliant copyright policy
  - publishing a sufficiently detailed summary of the content used for training the model
  - appointing an EU representative (if providers are based outside the EU)
- the additional obligations for providers of gpAI models which pose "systematic risks" (i.e. risk of large scale harm) and when a model is classed as such
- when a gpAI model is subject to regulation – the scope and thresholds need to be applied to each gpAI model to see if they apply. The modification of gpAI models will not always trigger compliance (to allow scope for innovation)

Providers are required to comply with their gpAI obligations in the AI Act from August 2, 2025. In-scope providers planning to place GPAI on the EU market from next month should review the Code to understand the practical steps they can take to ease their compliance with the forthcoming law.

The guidelines themselves are not legally binding but indicate the approach the Commission takes to interpreting and enforcing the Act. They provide clarification of key concepts in the AI Act, including the ways in which the Code can be used to demonstrate compliance with the legislation.

With these guidelines, providers of gpAI can check whether their interpretation of the law aligns with the Commissions, make decisions on whether their gpAI products need notification to the Commission and understand the scope of their obligations under the EU AI Act. The guidance should be read in tandem with the Code to enable maximum understanding and compliance.

On July 25, 2025 the EU Commission published a template for the summary of gpAI model training content under the EU Act.

Contact a specialist in our International team

EU Parliament study on AI and civil liability

The EU debate on whether to legislate specifically for liability for loss and damage caused by AI continued this month.

On July 24, 2025 the European Parliament published a study on AI and civil liability. This argues against withdrawal of the proposed AI Liability Directive (AILD), on the basis that failure to legislate at an EU level will result in fragmented and piecemeal national legislation. However, the study does not advocate passing the AILD in its current form, but recommends transforming it into a strict liability regime for high-risk AI.

Contact a specialist in our International team

EU: protecting minors and consumers – the Digital Services Act and Digital Fairness Act

On July 14, 2025 the European Commission published guidelines and a prototype age verification app to assist online service providers in complying with their obligations under the Digital Services Act (DSA).

The guidelines were developed following extensive stakeholder consultation and outline key "*appropriate and proportionate*" measures to protect children from online risks like grooming, harmful content, addictive behaviours, cyberbullying, and exploitative commercial practices. They adopt a risk based approach and will be used by the Commission to assess online platforms' compliance with DSA obligations. Good practice recommendations include:

- default "private" settings for minors' accounts so their personal data is hidden
- empowering children to block and mute users and control their feeds of recommendations – providers have a role to play in modifying their recommender systems to aid this and improve moderation and reporting tools
- disabling features which encourage excessive use or unwanted spending and prohibiting the ability to share minor content posted online
- the use of age assurance methods. An EU Age Verification Solution is under development to align Member States approach on this (developed from the European Digital Identity Wallet framework)

Impact: All platforms which are accessible to minors are recommended to review and comply with the guidelines which, whilst voluntary, will be an aid to demonstrating compliance with the DSA (note small and micro enterprises are exempted from the DSA requirements but good practice would be to adopt the recommended measures as far as practicable). The age verification solution has been specifically designed for developers and service providers looking to integrate age checks on their online services (and uses open source software). As a pilot, engagement with this product is encouraged as it enters the 'testing phase'.

These measures are the particular focus of the European Council (Danish presidency) who presented their priorities last week to MEPs. They stressed the need for continued focus on the creation of a safe environment for children, a firm enforcement of the DSA and stronger regulation to address age verification, addictive designs and profiling – using the upcoming Digital Fairness Act (DFA' in this regard.

The DFA is currently the subject of a European Commission consultation and call for evidence with views sought (until October 9, 2025) on proposed legislation to "*tackle unethical techniques and commercial practices related to manipulative interface design (dark patterns), misleading marketing by social media influencers, addictive design of digital products and online profiling, especially where consumer vulnerabilities are exploited for commercial purposes*". The aim is to fill the digital gap in current consumer protection laws. Businesses who engage with consumers online should consider responding with an early opportunity to shape the approach to proposed regulation in this area.

There will be further focus on these topics in the autumn and towards the end of the year. The approach of the Danish presidency indicates they wish to tighten the loopholes without over regulation.

Contact a specialist in our International team

EU action against cyber bullying

On July 22, 2025 the European Commission opened a consultation on the action plan against cyberbullying. Feedback is invited until September 29, 2025 on the plan which aims to "*make the online experience safer and healthier for minors and youth, targeting in particular members of vulnerable groups, and ensure a more consistent and effective approach to tackling cyberbullying across the EU*."

This is in advance of the Commission's planned adoption of the measures in early 2026.

Contact a specialist in our International team

EU Quantum Strategy

On July 2, 2025 the European Commission adopted its Quantum Strategy, which aims to make the EU a global leader in quantum by 2030. It says "*the Quantum Europe Strategy aims to turn Europe into a quantum powerhouse by fostering a resilient, sovereign quantum ecosystem, that fuels startup growth and transforms breakthrough science into market-ready applications, while maintaining its scientific leadership*".

The strategy comprises five pillars: research and innovation; quantum infrastructures, strengthening the quantum ecosystem, space and dual-use quantum tech (security and defence); and quantum skills.

Contact a specialist in our International team

With special thanks to our authors **Lizzie Charlton**, **Sara Ellis** and **Angela Kindness**.

Austria

Austrian Parliament passes the Resilience of Critical Entities Act (RKEG)

On September 24, 2025, the Austrian National Council passed the Resilience of Critical Entities Act (RKEG) to implement the EU CER Directive. The RKEG introduces new minimum standards for protecting essential services.

The RKEG identifies 11 critical sectors (energy, public transport, finance, digital infrastructure, food supply etc.) and requires organizations in these sectors to conduct regular risk assessments, develop resilience plans and report security incidents to the authorities within 24 hours. The RKEG focusses on physical resilience and complements the NIS2 Directive's obligations on digital resilience, which has not yet been implemented in Austria.

Impact: The RKEG will come into effect in early 2026.

Affected infrastructure operators will face significant compliance obligations to bolster their resilience. They must integrate rigorous risk management and emergency planning into their operations.

Non-compliance may result in substantial penalties, with fines of up to EUR 100,000 or EUR 500,000, underscoring the high priority placed on protecting critical infrastructure.

Contact a specialist in Austria

Vienna higher regional Court rules against marketing emails to abandoned cart customers

It is common for online shops to send email reminders to users who add items to their shopping carts but do not complete the purchase.

The Vienna Higher Regional Court (OLG Wien) has confirmed that sending such unsolicited "cart abandonment" reminder emails to potential customers without their consent is unlawful. An exemption may apply only if the recipient is an existing customer of the shop.

Impact: This case highlights that, in Austria, direct marketing emails require either prior consent or a legitimate interest based on an existing customer relationship. Businesses cannot contact potential customers who abandoned an order for marketing purposes without obtaining consent.

E-commerce companies should therefore ensure their marketing practices are either consent-based or supported by an ongoing customer relationship. Consent must be obtained through a clear, affirmative action (e.g., an opt-in checkbox).

Contact a specialist in Austria

Federal Administrative Court confirms GDPR compliance of employment service algorithm due to human oversight

On September 1, 2025 the Austrian Federal Administrative Court (BVwG) ruled that the Austrian Public Employment Service's (AMS) algorithm does not violate Article 22 of the GDPR.

The court found that AMS caseworkers were always substantively involved in each decision and could override the algorithm's results when necessary. Therefore, the decisions were not "exclusively" automated.

Impact: The ruling overturns the previous decision of the data protection authority and clarifies that algorithm-based decision-making is permissible, provided that each case undergoes meaningful human review.

Companies using algorithms or AI tools for decision-making should note that a merely theoretical human veto is insufficient. There must be genuine, substantial human involvement and the ability to alter automated outcomes to avoid an unlawful fully automated decision.

Contact a specialist in Austria

Freedom of Information Act (IFG) enters into force, ending official secrecy

On September 1, 2025, Austria's new Freedom of Information Act (IFG) came into effect.

The reform abolishes the longstanding principle of *Amtsgeheimnis* (official secrecy) and introduces a transparency regime. Public authorities are now required to proactively publish information of general interest. In addition, the IFG grants individuals the right to access information held by public sector bodies.

Impact: The obligations under the IFG primarily affect the public sector. Government bodies (and certain state-controlled entities) must establish processes for handling information requests and routinely disclose data, increasing public oversight.

Private entities may be indirectly impacted, as government bodies could be required to disclose records relating to them (e.g., contracts, permits). However, the IFG provides exemptions for specific areas where confidentiality remains necessary, such as personal data, national security, and trade secrets.

Contact a specialist in Austria

Belgium

Belgian DPA restricts the unlawful use of CCTV in student housing

On September 04, 2025, the Belgian data protection authority (DPA) directed a student housing owner to discontinue the use of four surveillance cameras, delete the images obtained from them, and pay fines totalling EUR 9,700.

The property owner had installed CCTV cameras in communal areas and at the building entrance. Since 2018, these cameras had recorded motion-triggered footage, which was available for real-time access via smartphone and was also stored on a PC. A student tenant regarded this surveillance as disproportionate and, following unsuccessful mediation and an information request, submitted a complaint to the DPA, which determined that the surveillance constituted a violation of the principles of lawfulness and data minimisation. The decision is only available in Dutch.

Impact: Organisations using CCTV to monitor their premises should take into account both the GDPR and the Belgian CCTV Act, and be aware that that the DPA will be watching too.

Contact a specialist in Belgium

Bulgaria

Data Protection Commission (DPC) issues guidance on GDPR-compliant access to school surveillance footage

The Bulgarian Data Protection Commission adopted recommendations addressed to schools and kindergartens concerning the lawful granting of access to video recordings from their surveillance systems. The recommendations clarify how to balance the rights of children, parents and other data subjects under GDPR when video surveillance captures images (and possibly audio) in educational institutions.

They highlight that parents have the right to:

- find out whether recordings exist concerning their child
- receive information about processing (including the purpose, categories of personal data processed, recipients, and storage period) and
- to access the recordings themselves

Schools and kindergartens are the controllers of personal data in these cases, and the rights of third parties who may also be captured must be safeguarded. To avoid harming others' rights, data controllers should use technical measures such as blurring or masking faces of other persons in the recordings. The recommendations further suggest options for complying with an access request in a way that protects the rights of all physical persons involved.

Impact: For information only at this stage

Contact a specialist in Bulgaria

New guidelines on the use of dashcams in private vehicles

In August 2025, the Data Protection Commission adopted Guidelines on the use of dashcams (video recorders) in private vehicles. Dashcams typically capture forward-facing footage of the road and may also record passengers inside the vehicle, meaning their use can involve the processing of personal data. The Guidelines emphasise the following key points:

- If the dashcam is used purely for personal or domestic purposes, data protection law may not apply due to the "household/personal or domestic activities" exemption. However, if the recordings capture public spaces, passengers, or are used in a professional, commercial, or non-personal context, the user becomes a data controller and must comply with GDPR obligations.
- When a dashcam user qualifies as a data controller, they must meet applicable obligations under data protection law, including:
  - **Transparency** – the vehicle should display a visible notice (e.g., sticker or sign) indicating that recording is taking place
  - **Purpose and storage limitation** – recordings should only be retained for as long as necessary for the specific purpose and
  - **Data subject rights** – individuals whose images or audio are recorded have rights under GDPR, including access to their personal data
- Publishing recordings (e.g. on social media) constitutes further processing and increases the privacy risks for those recorded. Such publications generally cannot rely on the personal/domestic exemption.

Impact: For information only at this stage.

Contact a specialist in Bulgaria

China

Administrative Measures for the Reporting of National Cybersecurity Incidents

《国家网络安全事件报告管理办法》

On September 11, 2025, the Cyberspace Administration of China (CAC) issued the "Administrative Measures for the Reporting of National Cybersecurity Incidents" (Measures) to guide network operators building, operating, or using networks to provide services in China, on cybersecurity incident (Incident) reporting.

The Measures outline the following:

- Classification: Incidents are classified as Particularly Major, Major, Significant, or General Incidents, based on factors such as the scale of important data or personal information affected, economic loss, etc
- Reporting channels: Network operators shall report Incidents via designated channels (12387 hotline, website, email, fax, etc.)
- Reporting timeframe: For Significant or higher Incidents, network operators shall report to the provincial-level CAC within four hours. The timeframes are shortened to two hours for network operators affiliated with central and state government departments (or their directly affiliated units) and one hour for critical information infrastructure operators.
- Reporting particulars: Particulars such as information of the network operator, affected systems/facilities, the Incident, remedial measures, causes, projected and new developments shall be reported. Suspected cybercrimes shall be reported to the public security authority
- Resolution reporting: Within 30 days of resolution, network operators shall submit a full analysis covering causes, emergency response, resulting harm, accountability, corrective actions, and lessons learnt

Impact: Given that the Measures are due to take effect, relevant network operators should align their internal Incident reporting guidelines with the requirements set out in the Measures. In particular, they should establish a classification system to categorize Incidents based on the matrix of factors specified in the Measures, update their response policies accordingly, and adhere to the revised policies. In the unfortunate event of an Incident, where a network operator has implemented reasonable and necessary measures to effectively mitigate the harm, lighter penalties might be imposed.

Contact a specialist in China

National Data Security Standards System (2025 Edition) (Draft for Comments)

《数据安全国家标准体系（2025版）（征求意见稿）》

On August 15, 2025, the National Technical Committee 260 on Cybersecurity of Standardization Administration of China (TC260) issued the "National Data Security Standards System (2025 Edition) (Draft for Comments)" (Data Security System) for consultation.

The Data Security System covers the entire data processing lifecycle (from collection to deletion), targeting data-related organizations, products, services, systems, technologies, management practices, and activities, organizing existing standards into six categories:

- Basic standards: Terminology and general rules for data classification and graded protection.
- Technology and products: Frameworks, specifications, and guidelines for classification and grading, security protection, shared security, backup, recovery, and deletion, etc.
- Management: Requirements, methods, and guidelines for data processing and export, data security operations, and data security organization and personnel.
- Evaluation and certification: Standards for testing and evaluation, supervision and inspection, and security certification activities, in data security risk assessment, capability evaluation, management certification, and assessment institutions.
- Products and services: Security requirements and guidelines targeting data services, data system components, electronic products, network platform services, and others (e.g. data centres and cloud computing services).
- Industries and applications: Standards for key industries (e.g. government, healthcare, telecom, and automotive), and emerging technologies (e.g. AI and drones)

Impact: The Data Security System is published to supplement existing legislation such as the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, etc. It helpfully categorizes existing data security standards to facilitate reference by enterprises engaged in data-related business activities, and foreshadows that standards and guidelines would be developed to address key data security issues and context-specific characteristics, and enhance the effectiveness in applying relevant standards.

Contact a specialist in China

National Personal Information Protection Standards System (2025 edition) (Draft for Comments)

《个人信息保护国家标准体系（2025版）（征求意见稿）》

On August 15, 2025, the National Technical Committee 260 on Cybersecurity of Standardization Administration of China (TC260) issued the "National Personal Information Protection Standards System (2025 Edition) (Draft for Comments)" (PIP System) for consultation.

The PIP System covers the entire personal information (PI) processing lifecycle (from collection to deletion) to protect PI rights, e.g. the rights to be informed, to decide, and to restrict or deny processing, organizing existing standards into six categories:

- **Basic standards:** Terminology and general rules in PI processing security and sensitive PI protection.
- **Technology:** Frameworks, specifications, and guidelines for de-identification, anonymization, and privacy design and engineering.
- **Management and rights safeguards:** Requirements, methods, and guidelines for PI processors, protection officers, emergency response, and rights safeguards (e.g. processing rules, notice and consent, automated decision-making, data subject rights, and minors' protection).
- **Evaluation and certification:** Standards for impact assessments, compliance audits, application testing, and data export certification.
- **Products and services:** Requirements and guidelines targeting the mobile application ecosystem, cloud computing services, online platform services, smart terminals, offline consumption scenarios, etc.
- **Industries and applications:** Standards for key industries (e.g. education, healthcare and public health, culture, tourism, and housing and urban-rural development), and emerging technology (e.g. AI and biometric information protection).

Impact: The PIP System is published to supplement existing legislation such as the Cybersecurity Law, the Personal Information Protection Law, the Regulations on Network Data Security Management, etc. It helpfully categorizes existing PI protection standards to facilitate reference by enterprises engaged in PI-related business activities, and foreshadows that standards and guidelines would be developed to address key PI protection issues and context-specific characteristics, or enhance the effectiveness in applying relevant standards.

Contact a specialist in China

Data Security Technology – Personal Information Protection Requirements for Minors' Products and Services (Draft for Comments)

《数据安全技术 未成年人产品和服务个人信息保护要求（征求意见稿）》

On July 29, 2025, the National Technical Committee 260 on Cybersecurity of Standardization Administration of China (TC260) issued the "Data Security Technology – Personal Information Protection Requirements for Minors' Products and Services (Draft for Comments)" (Draft Requirements) for consultation.

The Draft Requirements outline principles and standards for personal information protection (PIP) in products and services for minors, including requirements for personal information (PI) processing, security protection, and safety in emerging technologies and applications. They establish a three-tier PIP classification system comprising:

- **Basic protection:** applicable to all products/services for protecting PI security and rights of minors
- **Enhanced interaction:** adding PIP prompts/options to help minors understand PIP rules and rights, thereby better adapting to cyberspace
- **Age-appropriate optimisation:** balancing guardian oversight with minors' autonomy, enhancing minors' judgment and control in cyberspace

Providers such as smart terminal product manufacturers, developers of online protection software for minors, and online (platform) service providers shall select applicable requirements based on relevant forms, functions and target users, and justify any inapplicability. The Draft Requirements are also applicable to regulators, third-party testing organisations, and guardians.

The Draft Requirements also outline standards for minor user identification, PI processing and security protection, special protection requirements for minors, and age-appropriate optimisation.

Impact: The Draft Requirements aim to supplement existing legislation such as the Law on the Protection of Minors, the Personal Information Protection Law, and the Regulations on the Protection of Minors Online. Once finalized and implemented, the Requirements would provide a more comprehensive regulatory framework in minor-specific PIP.

Going forward, relevant providers of products and services for minors are encouraged to look out for the finalised Requirements and align their development and operation processes accordingly and update internal protocols or policies as needed.

Contact a specialist in China

Cybersecurity Technology – Technical Requirements for Minors Mode in Mobile Internet (Draft for Comments)

《网络安全技术 移动互联网未成年人模式技术要求（征求意见稿）》

On July 29, 2025, the National Technical Committee 260 on Cybersecurity of Standardization Administration of China (TC260) issued the "Cybersecurity Technology – Technical Requirements for Minors Mode in Mobile Internet (Draft for Comments)" (Draft Requirements) for consultation.

The Draft Requirements detail the technical requirements for minors mode across mobile smart terminals (Terminals), mobile internet applications (Apps), app distribution platforms (Platforms), and hardware-software interaction. Key specifications include:

- **Terminals:** One-click activation or deactivation of minors-mode, parental controls over app access (including downloads), and managements of minors' account and usage time.
- **Apps:** Functional requirements for managing access, usage time, minors' accounts, addiction prevention, consumption, external links and downloads. Apps shall also offer age-appropriate contents with appropriate tagging, moderation, and penalties, and tailor different service offerings to minors.
- **Platforms:** Automatic detection of minors-mode, designated minors zone with specified categories of age-rated apps, and parental approvals for downloads outside the minors zone.
- **Hardware-software interaction:** Seamless operation across Terminals, Apps, and Platforms, with stringent requirements (including parent authentications where applicable) for configuration changes or personal information handling.

The Draft Requirements also serve as guidance for regulators and third-party testing organisations.

Impact: The Draft Requirements aim to supplement existing legislation such as the Law on the Protection of Minors and the Regulations on the Protection of Minors Online. Once finalized and implemented, the Requirements would better regulate the development of minors-mode and more comprehensively address risks such as exposure to illegal or harmful contents, online addiction, induced consumption, and infringement of personal information rights, thereby safeguarding minors' rights and interests online.

Going forward, relevant Terminals, Apps, and Platforms are encouraged to look out for the finalised measures and adjust the minors-mode setting in alignment with the Requirements accordingly.

Contact a specialist in China

Practical Guide to Cybersecurity Standards – Safety Requirements for Triggering Shake-to-Open Advertisements

《网络安全标准实践指南——摇一摇广告触发行为安全要求》

On July 22, 2025, the National Technical Committee 260 on Cybersecurity of Standardization Administration of China (TC260) issued the "Practical Guide to Cybersecurity Standards – Safety Requirements for Triggering Shake-to-Open Advertisements" (Guide) to address issues with unintended redirections caused by shake-to-open advertisements (shake ads) on mobile smart terminals, regulating shake ads' display and triggering.

The Guide outlines the principles for protecting individual rights and interests associated with shake ads, and safety requirements for application operators (App Operators) and third-party advertising software development kit operators (SDK Operators).

Specifically:

- SDK Operators shall clearly guide users with prominent icons, animations, or text, and inform users of the outcomes of their actions
- Ads interfaces shall include a one-click close button, and apps must offer a convenient way for disabling shake ads
- SDK Operators shall set an appropriate sensitivity threshold (to be tested by App Operators) to prevent accidental triggering from normal device movements
- SDK Operators shall provide App Operators with configurable parameters for enabling/disabling the shake ads feature
- App Operators providing shake ads directly are subject to the same requirements as SDK Operators

The Guide also serves as guidance for assessment agencies or other personal information processors including mobile smart terminals.

Impact: Before the Guide was introduced, mainstream mobile phone systems, manufacturers, and leading applications have already implemented various measures to address inappropriate behaviours associated with shake ads. The implementation of the Guide will likely accelerate industry-wide standardization, helping to further curb disruptive advertising practices and enhance user experience.

Going forward, personal information processors (especially App Operators and SDK Operators) should align their internal policies with the requirements as set out in the Guide.

Contact a specialist in China

Data Security Technology – Technical Requirements of Electronic product Information Erasure

《数据安全技术 电子产品信息清除技术要求（征求意见稿）》

On July 14, 2025, the Office of the Central Cyberspace Affairs Commission published the "Data Security Technology – Technical Requirements of Electronic Product Information Erasure (Draft for Comments)" (Draft Technical Requirements) for consultation.

China hosts one of the world's largest second-hand electronics market, but second-hand electronic products (notably smart phones and tablets) are often sold to third parties without the previous owner's personal information being completely erased. These Draft Technical Requirements aim to address this issue by mandating that all electronic product manufacturers and relevant electronics recycling business operators comply with certain information erasure requirements.

In particular, the Draft Technical Requirements clearly outline:

- The scope of information to be removed (including applications, photos, videos etc.) and applicable technical requirements
- The information erasure requirements applicable to relevant electronics recycling business operators when recycling electronic products
- The methods for verifying whether information has been sufficiently erased

The Draft Technical Requirements also mandate that electronic product manufacturers provide a function for users to clear all user information at the tap of a button.

Impact: Once the Draft Requirements are finalized and implemented, enterprises engaged in the second-hand trade of electronics should ensure that any second-hand electronic products being sold or traded have had their information erased or cleared to the standard required by the Technical Requirements.

Contact a specialist in China

Cybersecurity Techniques – Incident Investigation Principles and Processes (Draft for Comments)

《网络安全技术 事件调查原则和过程（征求意见稿）》

On July 14, 2025, the National Technical Committee 260 on Cybersecurity of Standardization Administration of China (TC260) issued the draft national standard, "Cybersecurity Techniques – Incident Investigation Principles and Processes (Draft for Comments)" (Draft Standard) for consultation.

The Draft Standard outlines legal principles and procedures for investigating cybersecurity incidents (Incidents) involving digital evidence in binary form. It would guide organizations and personnel involved in the investigation in selecting appropriate tools, techniques, and methods across various scenarios.

It defines five processes:

- **Preparation:** An optional process to optimize digital evidence's value and the relevant organization's cybersecurity posture while minimizing cost and business impacts, through planning, implementing, and assessing digital evidence handling processes before and during Incidents.
- **Initialization:** Incident detection, initial response, planning, and preparation
- **Acquisition:** Physical investigation of objects containing potential digital evidence, covering identification, collection, acquisition, transfer, storage and preservation of such evidence.
- **Investigation:** Examining and analyzing potential digital evidence, interpreting digital evidence, reporting, presentation, and concluding the investigation
- **Parallel:** To ensure evidence admissibility, this process occurs concurrently with other processes, covering authorization, documentation, information flow management, chain of custody and digital evidence preservations, and coordination between physical and digital investigations

Impact: National standards have been available in incident management, incident description and exchange formats, emergency drills, and incident classification and grading, but not in incident investigations. The Draft Standard aims to standardize and ensure consistency of the Incident investigation process.

The Draft Standard applies to investigations including but not limited to unauthorized access, data destruction, system crashes, or enterprise cybersecurity violations. Once finalized and implemented, the Standard would guide various organizations in conducting Incident investigations. Organizations are also recommended to familiarize themselves with the Draft Standard, ang align their internal investigation policies on Incidents with the relevant requirements.

Contact a specialist in China

France

New Council of AI and Digital Affairs

The French government has officially change the "Conseil national du Numérique" into the "Conseil de l'intelligence artificielle et du numérique". This change, enacted by a decree published on September 6, 2025, represents a fundamental realignment of France's primary digital policy advisory body.

The decree modifies the council's missions, composition and operating methods to place a clear and strategic priority on Artificial intelligence.

More information can be found here.

Impact: This move centralizes high-level strategic thinking on AI and positions the new entity as the government's key advisory body for navigating its complexities. The timing is significant, as it coincides with the implementation of the EU Data Act.

Contact a specialist in France

Germany

North Rhine-Westphalia Data Protection Authority (LDI NRW) imposes €35,000 fine on recruitment agency

On September 12, 2025, the North Rhine-Westphalia Data Protection Authority (LDI NRW) announced a fine of over €35,000 against a Düsseldorf-based recruitment agency for persistent violations of data protection rights. The company repeatedly ignored job seekers' requests for information and deletion of their personal data and failed to respond to official inquiries from the LDI NRW. Despite claiming to have deleted data, the agency continued to send marketing newsletters to affected individuals. The LDI NRW emphasized that companies are legally obliged to cooperate with supervisory bodies and respect the rights of data subjects. The case highlights the regulator's commitment to enforcing compliance and addressing blatant disregard for GDPR obligations.

Impact: The decision underscores the importance of responding promptly to data subject requests and cooperating with supervisory authorities. Non-compliance can result in significant financial penalties and reputational damage.

Contact a specialist in Germany

Federal Ministry for Digital and State Modernization (BMDS) launches consultation on AI Market Surveillance and Innovation Promotion Act (KI-MIG)

On September 12, 2025, the Federal Ministry for Digital and State Modernization (BMDS) launched the consultation process for the draft AI Market Surveillance and Innovation Promotion Act (KI-MIG), which implements the European Artificial Intelligence Act (AI Act) in Germany. The draft law designates the Federal Network Agency (BNetzA) as the central market surveillance authority and notifying authority for AI systems. It also establishes a Coordination and Competence Center (KoKIVO) at BNetzA and introduces an AI Service Desk to support market participants. The law aims to create an innovation-friendly and streamlined governance structure, leveraging existing supervisory frameworks and avoiding duplicate structures. The consultation invites feedback from federal states and associations on the proposed framework.

Impact: Organizations developing or deploying AI systems in Germany should closely monitor the legislative process. The final requirements and actions will become clear once the law is adopted.

Contact a specialist in Germany

Hamburg Data Protection Commissioner publishes "The Bridge Blueprint" on aligning the General Data Protection Regulation (GDPR) and Artificial Intelligence Act (AI Act)

On September 10, 2025, the Hamburg Data Protection Commissioner (HmbBfDI) published the draft discussion paper "The Bridge Blueprint", which aims to provide practical guidance for harmonizing compliance with the GDPR and the AI Act. The paper addresses the legal uncertainty faced by organizations deploying AI systems that process personal data and proposes a framework for interpreting GDPR principles in the context of AI regulation. The guidance emphasizes that data minimization should be balanced with the need for sufficient data to ensure fairness, accuracy, and safety in AI systems. It also highlights the importance of integrating data protection and ethical safeguards into the design and deployment of high-risk AI systems. The HmbBfDI invites feedback from stakeholders to further develop the blueprint.

Impact: Organizations developing or deploying AI systems in Germany should review the discussion paper and consider submitting feedback before November 15 2025. The blueprint provides a practical approach to reconciling GDPR and AI Act requirements, but further guidance and legal certainty will depend on stakeholders' input and future regulatory developments.

Contact a specialist in Germany

Regional Court of Lübeck referral to the Court of Justice of the European Union (CJEU) on data transfer to credit agencies

On September 9, 2025, the Regional Court of Lübeck referred questions to the Court of Justice of the European Union (CJEU) regarding the lawfulness of transferring customer data from mobile phone providers to credit agencies such as Schufa without consent. The case concerns a provider that shared personal data (name, birth date, address, contract date, and contract number) with Schufa, which later used the data for credit scoring. The clarification sought is on whether Article 6(1)(f) of the GDPR applies to mass data transfers, whether the use of data for profiling makes the transfer unlawful, and iii) whether data subjects can claim damages even if they were informed but not asked for consent. Full details are available in the official press release.

Impact: The CJEU's decision will clarify the scope (applicability) of Article 6(1)(f) GDPR and could significantly impact data-sharing practices with credit agencies.

Contact a specialist in Germany

Independent German Federal and State Data Protection Supervisory Authorities (DSK) published guidance on data transfers for scientific research

In September 2025, the Independent German Federal and State Data Protection Supervisory Authorities (DSK) published an orientation paper addressing the requirements for transferring personal data to third countries in the context of scientific and medical research. The guidance clarifies the legal bases for such transfers, including the use of "broad consent" as described in Recital 33 GDPR. The paper provides practical recommendations for research institutions, including the need for clear documentation, risk assessments, and the implementation of appropriate safeguards when transferring data outside the EU. The orientation paper also discusses the limitations and requirements for using broad consent and highlights the importance of transparency and accountability in research data transfers.

Impact: Research institutions and organizations involved in scientific and medical research should review the DSK guidance and ensure that all international data transfers are documented and compliant with GDPR requirements. The orientation paper provides a checklist for lawful transfers, including the use of broad consent, and highlights the need for ongoing risk assessments and transparency. Further regulatory developments may follow as the debate on GDPR reform continues.

Contact a specialist in Germany

High Regional Court Munich on disclosure obligations for e-mail hosting services under the Telecommunications-Telemedia Data Protection Act (TDDDG)

On August 26, 2025, the High Regional Court Munich issued a decision regarding the disclosure obligations of e-mail hosting services under Section 21 Telecommunications-Telemedia Data Protection Act (TDDDG). The case concerned a car manufacturer seeking user data from an e-mail hosting provider after receiving only e-mail addresses from a platform operator in connection with allegedly unlawful reviews. The court found that e-mail hosting services qualify as interpersonal communication services regulated by telecommunications law, not as providers of digital services under Section 21 TDDDG. Therefore, the provider was not required to disclose user data under this provision.

Impact: The decision clarifies that e-mail hosting services are not subject to disclosure obligations under Sec. 21 TDDDG, limiting the scope of data access for rights holders. Further developments may arise if the Federal Court of Justice reviews the case.

Contact a specialist in Germany

District Court Berlin clarifies hosting provider liability under the Digital Services Act (DSA)

On August 7, 2025, the District Court Berlin (LG Berlin) ruled that a hosting provider only gains knowledge of content that violates personal rights in a reasonable manner if the affected person uses the appropriate notice-and-action procedure under Article 16 Digital Services Act (DSA) established by the provider. In the case, a restaurant sought an injunction against the platform operator acting as a hosting provider to stop the publication of third-party star ratings of its business. The court found that informal notifications, such as e-mails, do not meet the DSA requirements. The platform had provided a structured, easily accessible reporting mechanism as required by the DSA, but the claimant did not use it. As a result, the court held that the platform could not be deemed to have obtained actual knowledge of the allegedly unlawful content.

Impact: The decision confirms that organizations and individuals seeking removal of unlawful content must use the platform's official reporting tools under Article 16 DSA. Informal notifications are insufficient.

Contact a specialist in Germany

German Association for Data Protection and Data Security (GDD) published guidance papers on data processing roles and data processing agreements

In August 2025, the German Association for Data Protection and Data Security (GDD) published two practical guidance papers: one on distinguishing between controller-to-processor relationship and joint controllership, and another on best practices for terminating data processing agreements. The first paper provides criteria for identifying whether a relationship qualifies as controller-to-processor relationship or as joint controllership. Key factors include the existence of instructions, the determination of purposes and means, and the core activity of data processing. The second paper offers recommendations for the proper termination of data processing agreements, emphasizing the obligations of both controllers and processors to ensure the secure deletion or return of personal data. The guidance highlights the importance of clear contractual arrangements and documentation to minimize liability risks.

Impact: The GDD guidance provides practical checklists for the determination of the data processing roles and the termination of the data processing agreements.

Contact a specialist in Germany

Supervisory Authority for Baden-Württemberg updates ONKIDA 2.0 – AI & data protection navigator

In August 2025, the Supervisory Authority for Baden-Württemberg published an updated version of its "Orientation Navigator for AI & Data Protection" (ONKIDA) to help controllers and processors locate authoritative guidance on ten core GDPR topics for AI use cases. The ONKIDA maps issues such as purpose limitation, data minimization, data subject rights, and deletion to exact passages across leading sources, and links directly to the original documents.

Impact: ONKIDA 2.0 offers a curated "one-stop" entry point to supervisory guidance that organizations can use to: (i) select a lawful basis for AI training/use; (ii) scope DPIAs and risk assessments (including TIAs for international transfers); (iii) implement TOMs aligned to AI development phases; and (iv) operationalize transparency and data subject rights for LLMs and other AI systems. Teams deploying AI in the EU should incorporate ONKIDA into project checklists and policy updates as they prepare for AI Act implementation alongside ongoing GDPR compliance.

Contact a specialist in Germany

Data Protection Commissioner for North Rhine-Westphalia (LDI NRW) issues guidance on employee health data

On July 17, 2025, the Data Protection Commissioner for North Rhine-Westphalia (LDI NRW) published guidance on the processing of health data in cases of continued illness in employment relationships. The guidance clarifies that employers may only process health data if it is necessary to fulfil legal obligations, such as verifying entitlement to continued remuneration under the Continuation of Remuneration Act (Entgeltfortzahlungsgesetz). The legal basis for processing such sensitive data is Sec. 26(3) Federal Data Protection Act (BDSG) in conjunction with Art. 9(2)(b) and Art. 6(1)(b) GDPR. Employers must not request more information than necessary and should only process health data when there is a concrete reason to suspect a continued illness, not merely based on general suspicion. The guidance emphasizes the need for strict data minimization and confidentiality.

Impact: Employers should review their procedures for handling health data in cases of continued illness. Only data strictly necessary for verifying entitlement to continued remuneration may be processed, and only when there is a concrete reason to suspect a continued illness. Failure to comply with these requirements may result in regulatory action.

Contact a specialist in Germany

District Court Cologne allows German government to continue Facebook Fanpage

On July 17, 2025, the District Court Cologne ruled that the Press and Information Office of the German government may continue operating its Facebook Fanpage for public relations purposes. The court overturned an order by the Federal Commissioner for Data Protection and Freedom of Information (BfDI), who had prohibited the Fanpage due to alleged violations of the GDPR, particularly regarding the use of cookies and the lack of valid user consent. The court found that only Meta (formerly Facebook) is responsible for obtaining user consent for cookies placed when visiting the Fanpage. The role of the Press and Information Office of the German government is limited to operating the page and does not extend to controlling cookie placement or data processing parameters. Meta and the government are not joint controllers for the contested data processing. The court allowed an appeal.

Impact: Companies operating social media pages should note that, according to this judgement, responsibility for obtaining user consent for cookies lies with the platform provider. However, further legal clarification may follow if the case is appealed.

Contact a specialist in Germany

Hong Kong

2025 Policy Address promotes AI Adoption

On September 17, 2025, the Chief Executive of the Hong Kong Government released his 2025 Policy Address, which emphasized that AI development must be steered by safety and driven by application.

The Government will promote AI applications in government services, and some departments will develop their own AI solutions.

On the business front, the Hong Kong Monetary Authority (HKMA), in collaboration with Cyberport, has expanded their AI Sandbox initiative to promote AI applications to more financial institutions. Additionally, the HKMA is developing an AI model evaluation approach to step up testing on the system security of financial institutions. The Department of Justice will also establish an inter-departmental working group to review the legislation needed to support a wider application of AI.

Impact: The growing interest in AI adoption across industries is expected to accelerate. Organizations are recommended to continue monitoring evolving regulatory frameworks to ensure readiness and compliance.

Contact a specialist in Hong Kong

PCPD issues 10 Practical Tips for the Safe Use of AI Chatbots amid rising privacy risks

On August 4, 2025, the Privacy Commissioner for Personal Data (PCPD) issued ten practical tips to help users safeguard personal data when using AI chatbots, following reports of a large-scale generative AI platform exposing user chat histories to online search engines.

The tips are grouped into three categories as follows:

1. **Before use:** Users are advised to read privacy policies, beware of fake Apps and phishing websites posing as known AI chatbots, and adjust settings to prevent their chat history from being stored or used for model training
2. **During interaction with AI chatbots:** Users should avoid sharing personal data, correct / remove inaccurate personal data, guard against cybersecurity threats, and delete outdated conversations from their chat history
3. **Safe and responsible use of AI chatbots:** Users are reminded to use the information provided by AI chatbots carefully, refrain from sharing confidential information, and ensure students receive proper guidance when using AI chatbots

Impact: The PCPD's publication highlights growing regulatory attention on the data risks linked to the use of generative AI platforms. To minimize security risks, organizations are recommended to implement these safety tips and remind users of the same before deploying or allowing the use of AI chatbots in the workplace.

Contact a specialist in Hong Kong

Asia-Pacific Privacy Authorities launch Anonymisation Guide to strengthen AI and data security

On July 31, 2025, the Privacy Commissioner for Personal Data, Hong Kong (PCPD) and the Personal Data Protection Bureau, Macao (PDPB), in collaboration with seven Asia-Pacific privacy authorities, jointly released the "Guide to Getting Started with Anonymisation" at the 63rd Asia Pacific Privacy Authorities (APPA) Forum.

The guide sets out five key practical steps for organizations to anonymize personal data:

1. Identify the nature of the data in question, including direct identifiers and indirect identifiers
2. Remove direct identifiers from the dataset
3. Apply anonymization techniques to indirect identifiers to prevent others from identifying an individual by combining the indirect identifiers with other data
4. Assess re-identification risks, and determine whether the anonymization is sufficient based on the assessment result and
5. Manage residual risks by implementing corresponding risk mitigation measures, such as restricting the use of the data for intended purposes and access by intended personnel

Impact: The guide outlines recommended steps for anonymizing personal data, helping organizations mitigate re-identification risks and demonstrate compliance maturity.

Contact a specialist in Hong Kong

Hong Kong's financial regulators launch Anti-Scam Consumer Protection Charter 3.0 to combat digital fraud

On July 9, 2025, Hong Kong's financial regulators, including the Hong Kong Monetary Authority (HKMA), the Securities and Futures Commission (SFC), the Insurance Authority (IA), and the Mandatory Provident Fund Schemes Authority (MPFA), jointly launched the Anti-Scam Consumer Protection Charter 3.0 (Charter 3.0), in collaboration with major technology and telecommunications firms.

Charter 3.0 aims to create a safer online environment and improve fraud detection and prevention. It outlines six key principles: (1) enabling user reporting of scams, (2) establishing direct reporting channels for regulators, (3) verifying advertisers, (4) implementing internal monitoring of financial content, (5) enforcing platform terms of service, and (6) promoting public awareness through joint campaigns.

Participation is voluntary and non-legally binding, and actions are intended to be applied on a proportionate basis as appropriate. Notable participants include global tech firms and major telecom providers in Hong Kong.

Impact: For information only at this stage.

Contact a specialist in Hong Kong

PCPD advocates for stronger Personal Data Privacy protection

The Office of the Privacy Commissioner for Personal Data (PCPD) has called for stronger protection of personal data privacy following its intervention in eight data security incidents across various sectors.

To address challenges relating to personal data security, the PCPD issued six key recommendations to organizations of all sectors:

1. Incorporate privacy protection into core values, appoint responsible managers, and publicly demonstrate leadership commitment
2. Enhance employee awareness and capabilities through role-specific training, risk education and scenario drills
3. Develop clear work guidelines, using checklists or flowcharts tailored to job functions, and reinforce them regularly via internal communications
4. Adopt technical safeguards, such as encrypted email systems and auto-filling of correct email recipients to minimise risk of errors
5. Monitor and assess compliance, including regular or surprise inspections and feedback collection for continuous improvement
6. Develop a comprehensive data breach response plan to ensure swift and effective incident management

Impact: To strengthen the protection of personal data privacy, organizations are recommended to implement the PCPD's proposals which represent best practice, particularly in the event of a data security incident.

Contact a specialist in Hong Kong

Hungary

The NAIH's investigation into the lawfulness of personal data processing by Városi Kurír

On August 11, 2025, the Hungarian Data Protection Authority (NAIH) published its report concerning the Városi Kurír news website, following a citizen's complaint regarding the publication of personal data in an article.

NAIH examined whether Városi Kurír provided prior notice and had a lawful basis for processing the personal data.

Firstly, NAIH determined that Városi Kurír qualifies as an independent data controller, even though the article in question was a republished summary of content from other news outlets. The act of republishing constituted a separate data processing activity, making the website responsible for ensuring the legality of the data handling.

Secondly, NAIH determined that although not a public figure, the complainant's alleged conduct at a festival transformed the incident into a matter of public interest.

NAIH concluded however that Városi Kurír did not specify the purpose or legal basis for the data processing. No documentation was provided to demonstrate either the complainant's consent, or an assessment of legitimate interest.

Although journalistic activity may rely on legitimate interest as the legal basis of data handling, this requires a proper balancing test, which was not conducted by Városi Kurír. Consequently, the data processing violated principles of lawfulness, fairness, transparency and accountability.

Impact: NAIH's investigation into the Városi Kurír online news portal carries significant legal implications for data controllers, particularly in the media sector.

Contact a specialist in Hungary

Italy

Italy becomes the first EU country to adopt a national AI law, complementing the EU AI Act

On September 17, 2025, the Italian Senate definitively approved Bill No. 1146-B, then published in the Italian official Journal as Law 132/2025, the first national law within the European Union to complement Regulation (EU) 2024/1689 (AI Act), introducing provisions tailored specifically to Italy.

The new Italian AI Law establishes fundamental principles, areas of application, national strategies, safeguards, and liability frameworks concerning artificial intelligence. The Italian AI Law focuses on areas deemed particularly significant, including healthcare, scientific research, employment, intellectual professions, justice, public administration, copyright, and criminal law. Meanwhile, Agenzia per l'Italia digitale (AgID) has been appointed as the notifying and accrediting authority, while Agenzia per la cybersicurezza nazionale (ACN) has been appointed as the supervisory body responsible for enforcing AI-related regulations and imposing sanctions for non-compliance.

Future developments are anticipated soon as several implementing acts are expected, and the Italian Government has been provided with specific delegated legislative powers. The Italian AI Law will enter into force on October 10, 2025.

Impact: Following the entry into force of the Italian AI Law, professionals and companies operating in specific sectors must align their AI governance and usage with both the AI Act and the new national requirements.

Specifically, companies should update their internal policies to reflect transparency, security, and human oversight principles, and their privacy information notices for any case of AI usage, along with a review of the their processing activities impacted by AI. They will also need to engage with AgID and ACN as the relevant authorities going forward. Given the expected implementing acts, legal developments must also be monitored.

Contact a specialist in Italy

Italian judge sanctions the unverified and misleading use of generative AI in a legal proceeding

On September 16, 2025, an Italian Court issued ruling 1018/2025, sanctioning the unverified use of generative AI in legal proceedings. The case involved a lawyer who submitted a procedural document opposing a payment order, relying entirely on AI-generated content that included misleading and unfounded arguments. The court determined that the lawyer acted in bad faith, or at the very least, with gross negligence, and, under Article 96(3) of the Italian Code of Civil Procedure, imposed a financial penalty on the claimant, in addition to ordering compensation to each opposing party.

Impact: This ruling marks the first time an Italian judicial authority has formally sanctioned the unverified use of AI in the courtroom.

Lawyers must always critically review AI generated content before using it in formal or legal contexts

Contact a specialist in Italy

ACN publishes guidance document on security measures and incident reporting under NIS2

The Italian National Cybersecurity Agency (ACN) has published a guidance document outlining the security measures to be adopted, and the categories of incidents that must be reported by essential and important entities under Italy's implementation of the NIS2 Directive.

Impact: The guidance document should be considered by entities falling within the scope of NIS2, considering the progressive applicability of the underlying requirements in Italy.

Contact a specialist in Italy

Italian Supreme Court rules on a case involving an employer's access to the emails of former employees

On June 11, 2025, the Italian Supreme Court confirmed a decision of the Court of Appeal which found that a company violated the privacy rights of its former employees by accessing their email accounts. Any data acquired through such access was therefore unusable as evidence.

The company had sued its former employees, alleging unfaithful behaviour during their employment. The court of first instance found in the company's favour but the Court of Appeal overruled the decision. The company then appealed to the Supreme Court which confirmed the Court of Appeal's judgement.

The confirmed decision stated that since the emails retrieved by the employer were obtained from personal accounts included in the company server, although after the employment relationship ended, . The act of accessing the password protected email accounts amounted to the criminal offences of abusive access and violation of correspondence.

Impact: Although this is a decision on a specific case, it highlights the need for utmost care in regulating the usage of company devices, especially concerning controls which can be performed. This judgement demonstrates how compliance with data protection and employment laws is essential in the context of employment, and the mere defensive needs of employers cannot justify any intrusive access to employees' emails.

Contact a specialist in Italy

Decree expands the list of cybersecurity incidents that must be reported to the CSIRT.

On August 1, 2025, the Decree of the President of the Council of Ministers No. 111/2025 (**"Decree"**), was published in the Italian Official Journal. The Decree updates the list of cybersecurity incidents that must be reported to the National Computer Security Incident Response Team (**"CSIRT"**) by entities falling within the scope of the National Cybersecurity Perimeter (Perimeter). The Perimeter, established by Decree-Law No. 105/2019 (converted into Law No. 133/2019), constitutes the national security framework aimed at enhancing digital resilience through specific obligations, including the prompt notification to CSIRT of any incident that may compromise the confidentiality, integrity, or availability of digital infrastructures.

The Decree identifies six macro-categories of reportable incidents: Initial Exploitation, Fault, Establish Persistence, Lateral Movement, Actions on Objectives, and unauthorised access or abuse of privileges. The latter also encompasses access by authorized personnel when performed anomalously or outside the scope of assigned duties, as detected through qualitative indicators (e.g., unusual access times, hidden command-line usage) or quantitative indicators (e.g., excessive data queries).

The Decree entered into force on August 16, 2025.

Impact: The Decree expands the scope of the Perimeter and reinforces notification obligations to enhance national cybersecurity. Its purpose is to strengthen the detection of insider threats and credential-based intrusions, thereby anticipating cyber attacks and incidents.

For this reason, entities falling within the Perimeter should review and update their incident management protocols, implement processes to monitor authorized personnel activities (such as log retention), and properly train authorized personnel to raise awareness regarding their roles and responsibilities.

Contact a specialist in Italy

The IDPA plans inspections across high-risk sectors

On August 4, 2025, the Italian Data Protection Authority (IDPA) published by resolution its inspection programme for the July–December 2025 timeframe. IDPA will carry out at least 35 inspections targeting key areas of data protection. These include: recent data breaches involving sensitive public databases; insurance data processing for pricing estimates; use of whistleblowing platforms; data handling in local public transport systems; biometric identification in banking services; statistical data processing related to pathology registries; management of personal data in electronic health records; and unlawful telemarketing practices in the energy sector. Additional inspections may be launched independently or in response to complaints.

Impact: Companies, especially those operating in the sectors that will be targeted by IDPA, must ensure that their data processing activities are fully compliant with GDPR and national privacy legislation and should be aware of IDPA investigation activity.

Contact a specialist in Italy

IDPA issues its Annual Report

On July 15, 2025, the Italian Data Protection Authority (IDPA) presented its Annual Report at the Chamber of Deputies. The Annual Report analyses IDPA's activities, highlighting its major interventions, its issued measures, its performed investigations, the amount of fines imposed and the data breaches received, alongside topics of interest.

Among the notable topics the Annual Report considers are: AI; biometrics and facial recognition; online protection of minors and age verification; employment; consumer protection and unlawful marketing; and digital transformation.

Impact: The IDPA's Annual Report is always a good insight into the authority's trends, past activities, and priorities, and is an important reference for operators.

Contact a specialist in Italy

The IDPA fines an insurance company for several data protection breaches

In October 2024, the client of an insurance company submitted a complaint to the Italian Data Protection Authority (IDPA), alleging that the company unlawfully disclosed her personal data to an unauthorised third party. Between 2021 and 2023, the company responded to information requests that appeared legitimate (including handwritten signatures and detailed personal data) by sending sensitive documents to an email address that the claimant later confirmed she had never used or created. The company suspended communications and initiated an internal investigation on September 22, 2024.

On July 10, 2025, IDPA concluded that the company violated key principles of the GDPR, specifically those concerning lawfulness and data security (Art. 5(1)(a) and (f)). The company explained that the complainant had not provided any email address to them, and that the operator relied on the genuineness of the requests received from the third party address, considering the presence of unambiguous and detailed elements relating to the client and the handwritten signature. Nonetheless, these explanations were found to be insufficient. As a result, IDPA declared the data processing unlawful and imposed an administrative fine, under Article 83 of the GDPR, for €80,000 along with corrective measures to ensure proper identity verification in future communications.

Impact: This decision underscores the critical importance of verifying the authenticity of communication channels before disclosing personal data. It is no longer sufficient to rely on superficial indicators such as signatures or detailed personal information. Organizations must implement robust identity verification procedures and ensure that any email address used for communication has been explicitly confirmed by the data subject.

Contact a specialist in Italy

Lithuania

Lithuanian Data Protection Authority reports stronger oversight in 2024

On August 8, 2025, the Lithuanian Data Protection Authority (VDAI) and the Office of the Inspector of Journalist Ethics (competent authority for supervising personal data processing when it is carried out for journalistic, academic, artistic or literary purposes) published their review of personal data protection supervision in Lithuania for 2024. The report highlights increased public engagement, regulatory activity and international cooperation in the field of data protection.

Some key developments include a 15% rise in complaints to VDAI compared to 2023, with the most frequent issues related to direct marketing, data disclosure, video surveillance and access rights. Public awareness of GDPR continues to grow, with 86% of surveyed Lithuanians now familiar with the regulation. In terms of enforcement, VDAI most frequently issued orders requiring data controllers/data processors to bring data processing activities into compliance with GDPR provisions, reflecting VDAI's focus on corrective guidance and compliance support.

Impact: For information only.

Contact a specialist in Lithuania

Cybersecurity incidents dominate Lithuania's data breach landscape in H1 2025

On July 30, 2025, the Lithuanian Data Protection Authority (VDAI) published its semi-annual report on personal data breaches in Lithuania. Between January and June, VDAI received 116 breach notifications, affecting 168 822 data subjects. Most incidents (86%) involved breaches of confidentiality.

Cybersecurity incidents accounted for 32% of all breaches, including ransomware, unauthorized access, Brute Force attacks. These events disproportionately impacted individuals, representing 81% of all affected data subjects. In any case, human error still remains the leading cause of breaches (57%).

Impact: The report reveals a critical need for organisations in Lithuania to strengthen cybersecurity defences and reduce human error through training and awareness. Companies must prioritize GDPR compliance and invest in robust data protection, as well as cybersecurity protection strategies to mitigate future breaches. Failure to act could result in legal consequences, loss of consumer trust and operational disruptions.

Contact a specialist in Lithuania

Netherlands

Dutch Council of State (ABRvS) upholds 50% of initial regulatory fine imposed on company which required submission of ID when submitting data subject requests

On September 24, 2025, the ABRvS ruled that an initial fine imposed by the Dutch Data Protection Authority (DDPA) is to be reduced by 50%. Initially the company in question was fined €525,000 for requiring individuals to upload a full copy of their ID when submitting access or erasure requests. The DDPA argued that requesting more information than is necessary was contrary to the principle of data minimization as laid down in Article 5(1)(c) GDPR.

Contrary to the decision from the lower court, the ABRvS found that the DDPA was justified in issuing the fine, but lowered the fine based on the fact that:

- the impact was limited to a small number of cases;
- the IDs were only briefly retained (one month) and the policy was amended in practice; and
- there is no proof the policy had the aim of discouraging the submission of data subject requests.

Impact: Data controllers should assess alternative, less privacy-intrusive options when verifying identity as part of data subject requests. While a copy of an ID may be reasonable in some cases, it must be proportionate and compliant with Article 5(1)(c) GDPR. It is recommended to consider alternative verification methods and document the rationale.

Contact a specialist in the Netherlands

Dutch Data Protection Authority (DDPA) publishes 2024 Privacy Complaints Report

On September 23, 2025, the DDPA published its '2024 Privacy Complaints Report' (the Report), detailing the types of complaints it received and how they were handled. The Report offers insights into the regulator's enforcement priorities and recurring GDPR issues.

Impact: Organizations should review and analyze complaint trends to identify and remedy common compliance gaps. By doing so, the risk of enforcement can be mitigated.

Contact a specialist in the Netherlands

Dutch Court of Appeal ruling on duty to investigate and notify data subject of third party recipients receiving their personal data before actioning a request for erasure

On September 23, 2025, the Dutch Court of Appeal ruled that data controllers had a duty to investigate and notify data subjects of third party recipients receiving their personal data before actioning a request for erasure under Article 17 GDPR, unless this is deemed impossible or if disproportionate efforts would be involved. The court stated that:

- The obligation to notify recipients of data erasure applies to all recipients, not just data processors, and includes any party to whom personal data was disclosed
- Although data controllers must maintain a record of categories of recipients (Article 30 GDPR), they are not required to track disclosures at the individual or file level, meaning the controller was not obligated to keep a separate register of specific disclosures
- Before destroying personal data following a request for erasure, the data controller should have assessed whether personal data had been shared with third party recipients and notified the data subject of recipients accordingly – failure to do so breaches GDPR obligations
- However, the obligation to notify all recipients does not apply if this proves to be impossible or requires disproportionate effort (Article 19 GDPR)

For more information, see the Court of Appeal's judgement.

Impact: This ruling reinforces the need for data controllers to proactively assess and document data disclosures before actioning a request for erasure of personal data. Failure to do so may result in GDPR violations. Organizations should review notification procedures and ensure traceability of data sharing to meet their Article 19 obligations effectively.

Contact a specialist in the Netherlands

District Court orders financial institution to disclose to data subject what personal data is shared with third party recipients

On September 5, 2025, the District Court ordered a financial institution to provide a detailed overview of third parties with whom the data subject's personal data had been shared. The court found sufficient evidence that the financial institution had shared the data subject's personal data with specific entities.

The financial institution must provide an overview of the data subject's personal data shared with the data protection officer, the recipient's email provider, IT service providers, and the group entities of the financial institution.

Impact: Data controllers should ensure they can identify and provide disclosures to data recipients under Articles 13 and 15 GDPR. It is recommended to maintain accurate records of data processing and to specifically identify and map disclosures of personal data to processors and third parties.

Contact a specialist in the Netherlands

District Court finds that trustees in bankruptcy are data controllers

On August 7, 2025, the District Court confirmed that a trustee in bankruptcy (the Trustee) was rightfully fined by the Dutch Data Protection Authority (DDPA) for violations under GDPR, but reduced the fine from €148,750 to €58,000 due to mitigating factors.

The court found that the Trustee can be deemed a data controller under GDPR, as he had access to and influence over personal data contained on data carriers as part of the estate in bankruptcy. The violation under GDPR can be attributed to the Trustee, but to a lesser extent than the DDPA had determined. Although the Trustee failed to verify the deletion of personal data on the data carriers, he had taken mitigating measures to remove such data, which justified a further reduction of the fine.

Impact: This case highlights the importance of verifying GDPR roles and responsibilities; protection of personal data through appropriate technical and organisational measures; and data deletion procedures during asset disposal. Although partial compliance with GDPR obligations may reduce penalties by the DDPA, failure to ensure complete compliance may still result in significant fines. Organizations should document all steps taken (including security measures) to protect personal data, in particular during data asset disposal or transitions.

Contact a specialist in the Netherlands

Dutch Data Protection Authority (DDPA) publishes guidance on meaningful human intervention in algorithmic decision-making

On July 23, 2025, the DDPA published guidelines for human intervention to support meaningful human oversight in algorithmic decision-making. This document is intended as a tool for those within an organization who design and implement human intervention, referred to as "designers". It also provides guidelines for those who carry out human intervention, referred to as "assessors". This tool is based on European Data Protection Board (EDPB) guidelines, the experience of DDPA staff, academic research, and case law.

Impact: Organizations using algorithmic decision-making should review their internal processes and design. Ideally, an organization should have a clearly described process for meaningful human intervention, and the involved employees can explain this well.

Contact a specialist in the Netherlands

Dutch Data Protection Authority (DDPA) publishes report on AI and algorithms

On July 15, 2025, the DDPA published 'Report AI & Algorithms Netherlands July 2025' (the Report). The Report highlights regulation on the use of biometric data and examines AI systems used for emotion recognition based on biometrics, explaining both risks and ethical issues, including issues relating to the AI Act and GDPR.

For more information, see the DDPA's news article about the Report.

Impact: Companies should evaluate their use of AI for the purpose of emotional recognition from both an AI Act and GDPR perspective.

Contact a specialist in the Netherlands

Dutch Data Protection Authority (DDPA) approves protocol for shared blacklisting at ports, airports and sensitive logistics locations

On July 14, 2025, the DDPA approved a protocol enabling ports, airports and other sensitive logistics sites to share criminal data from blacklists under strict safeguards. Organizations that operate in accordance with the terms of this protocol will receive a license from the DDPA to lawfully share information about such individuals.

Impact: Qualifying companies may apply for a license if they adhere to the requirements under the protocol (e.g. limited access, objection and appeal mechanisms, and retention limits).

Contact a specialist in the Netherlands

Dutch Data Protection Authority (DDPA) guidance: algorithms processing personal data can be registered as part of the Register of Processing Activities (RoPA)

On July 11, 2025, the DDPA published practical guidelines for setting up and maintaining an "algorithm registry". Algorithms used for high risk personal data processing activities can be registered as part of the RoPA to meet regulatory requirements.

Impact: To help meet the requirements in setting up and completing an algorithm register, if applicable, algorithms can be included as part of the RoPA.

Contact a specialist in the Netherlands

Dutch Data Protection Authority (DDPA) orders Tax Administration to stop or replace use of non-compliant IT applications

On July 10, 2025, the DDPA ordered the Tax Administration to completely phase out two IT applications and adapt four others due to privacy non-compliance, including processing of personal data leading to discriminatory practices.

Impact: Companies should ensure they have a documented lawful basis for processing special category and criminal data; actively prevent discriminatory practices in their IT systems; prevent unrestricted data exports from IT applications; and comply with all legally required notifications.

Contact a specialist in the Netherlands

Dutch Data Protection Authority (DDPA) issues fine for unlawful use of cameras capturing footage of public areas

On July 8, 2025, the DDPA fined a foundation €500 for using cameras in a Dutch village to livestream public spaces, capturing identifiable people and homes, without a valid legal basis. Under normal circumstances, this violation would justify a basic fine of €525,000. However, the DDPA took into account the very limited financial capacity of the foundation and reduced the amount to €500. Additionally, the DDPA imposed an order subjecting the foundation to a penalty for further non-compliance. For further information, see the DDPA's decision.

Impact: Even small-scale CCTV/cameras require a lawful basis, and transparency and data minimization must be ensured. Companies are recommended to audit their use of cameras aimed at public spaces; consider blurring certain video footage and camera angles; and limit their retention periods.

Contact a specialist in the Netherlands

Dutch Data Protection Authority (DDPA) publishes 2024 Data Breach Report

On July 3, 2025, the DDPA published its '2024 Data Breach Report' (the Report). In summary, the Report states that:

- The DDPA focuses on data breaches with the highest risks to data subjects
- Data subjects must be informed about what has happened, what to watch out for and how to protect themselves; and
- The DDPA investigated 28 serious breaches in 2024, often caused by poor basic security measures.

Impact: Organizations should prioritize basic cybersecurity controls against ransomware and data theft (e.g. segmentation and back-ups); prepare and raise awareness in breach communications; and evaluate notification decision trees.

Contact a specialist in the Netherlands

Portugal

Network and Information Directive 2 (NIS2) Transposition Approved

On September 19, 2025, the transposition of NIS 2 was finally approved in Portugal, after delays due to government elections.

Impact: The law transposing the Directive will be published in the Diário da República (Official Gazette). More details to follow.

Contact a specialist in Portugal

Despacho n.º 10918/2025/Order No. 10918/2025: Provision to create a working group responsible for defining retention periods for health-related data

On September 16, 2025, an Order was published providing for the creation of a working group to analyze and propose requirements for defining the retention periods for health data stored in information systems. These systems are managed by the Shared Services of the Ministry of Health (SPMS) and used in primary and hospital health care for recording clinical processes and administrative acts.

Impact: For information only at this stage. This working group will be composed of representatives from various entities, for example the General Secretariat of the Ministry of Health and the Directorate-General for Health. The group will work for 1 year, with the possibility of an extension for a further 6 months.

Contact a specialist in Portugal

Opinion no. 2025/53 issued by the Portuguese Data Protection Authority (CNPD) regarding the implementation of Regulation 2022/2065 (the Digital Services Act)

On September 16, 2025, the CNPD issued a new Opinion regarding Draft Law No. 25/XVII/1.ª which aims to implement Regulation 2022/2065 (the Digital Services Act).

The CNPD is the National Supervisory Authority for the purposes of the GDPR. ANACOM (Autoridade Nacional de Comunicações/National Communication Authority) has been designated as the Digital Services Coordinator under the EU's Digital Services Act. ANACOM's role alongside the CNPD is not clearly defined, meaning that there is a risk of non-compliance and inconsistency in the application of the Act. The CNPD have set out recommendations to correct this, including a specific harmonisation agreement setting out clearly the nature, duty and powers of each organisation.

Impact: For information only, at this stage.

Contact a specialist in Portugal

Romania

ANSPDCP Annual Report for 2024

On August 11, 2025 the Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP) published its 2024 Annual Report, offering an overview of its activity across core areas such as advisory work, monitoring and control, international cooperation, and institutional management.

Throughout 2024, the Authority received 5,354 complaints, notifications, and security incident reports, which led to 476 investigations. As a result, 83 fines totalling approximately 1,855,907 RON (around EUR 370,000) were imposed, alongside 161 reprimands and 180 corrective measures.

The ANSPDCP also handled 882 requests for interpretation of GDPR provisions from public and private entities and issued 99 opinions on draft legislative acts with data protection implications.

In terms of litigation, the Authority managed 173 court cases at various procedural stages, several of which concluded favourably for the institution.

At the international level, 40 multinational companies submitted requests for the approval of binding corporate rules (BCRs) governing personal data transfers.

The report includes statistical indicators, comparative analyses with previous years, and summaries of significant cases, reflecting the growing complexity of the Authority's enforcement and advisory work.

Impact: Overall, the report serves as a clear indicator that enforcement activity is intensifying, and organizations should prioritize GDPR compliance to mitigate the risk of fines, corrective measures, and reputational damage.

Contact a specialist in Romania

Sanction for unauthorized disclosure of personal data (in the context of the presidential election in Romania)

The Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP) recently concluded two investigations – one concerning a political party and another involving a presidential candidate.

In the case of the political party, the ANSPDCP found violations of Articles 32(1)(b), (d) and (2), in conjunction with Articles 25(1)–(2) GDPR (security and data protection by design), and Articles 5(1)(c), 5(2), and 6(1) GDPR (data minimisation, accountability, lawful basis). A configuration error and vulnerable API in a campaign app exposed personal data such as names and ID numbers. A third party exploited the flaw, gaining unauthorized access to the source code. In a separate case, the Permanent Electoral Authority reported two websites collecting excessive personal data for campaign promotion without a valid legal basis. Both sites were later deactivated. The ANSPDCP imposed fines of EUR 10,000 and EUR 15,000.

In the case of the presidential candidate, the ANSPDCP found breaches of Article 4(5)(a)–(b) of Law no. 506/2004 and Articles 12–14 GDPR. Between December 2024 and April 2025, the candidate's website installed cookies without prior consent and failed to inform users about data processing via its contact form. A fine of approximately EUR 10,000 was imposed.

Impact: The cases highlight the ANSPDCP's growing scrutiny of political data processing and its expectation that digital campaign tools comply with data protection by design and default. Organisations developing or managing political apps or campaign websites should review their security configurations, consent mechanisms, and data minimisation practices to ensure compliance.

Contact a specialist in Romania

Singapore

Publication of the Singapore Cyber Landscape

On September 3, 2025, the Cyber Security Agency of Singapore (CSA) published the Singapore Cyber Landscape 2024/2025 report, highlighting rising cyber threats and recommending a multi-pronged strategy to bolster resilience.

The report identifies five priorities: (i) protecting critical information infrastructure to secure essential services; (ii) developing resilient infrastructure, including operational technology systems; (iii) enabling a safer cyberspace through awareness initiatives, cyber hygiene programmes, and the Cybersecurity Labelling Scheme; (iv) growing the cybersecurity talent pipeline via education, industry collaboration, and training; and (v) enhancing international cooperation by deepening regional and global partnerships.

These measures address escalating threats in 2024: phishing incidents rose by 49%, ransomware cases by 21%, while Advanced Persistent Threat groups intensified their activities and supply chains were increasingly exploited. Global disruptions, such as the CrowdStrike outage and submarine cable cuts, underscored the fragility of digital infrastructure.

The report also highlights the dual use of artificial intelligence in cyber operations, alongside evolving social engineering techniques such as voice phishing. CSA emphasises the need for adaptive strategies, collective responsibility, and sustained preparedness to safeguard Singapore's digital economy and ensure resilience against emerging cyber risks.

Impact: Organisations operating in sectors vulnerable to cyber-attacks should anticipate and prepare for increased regulation. More robust security strategies should also be adopted to adapt to more complex cyber threats.

Contact a specialist in Singapore

Singapore High Court clarifies scope of deemed consent and actionable loss under the Personal Data Protection Act 2012

In a judgment dated August 29, 2025, the Singapore High Court clarified the scope of deemed consent and the standard for actionable loss under the Personal Data Protection Act 2012 (PDPA).

The case concerned a not-for-profit organisation's disclosure of an individual's name and email to a third party which formed the subject of his complaint. The Court held that while the individual was deemed to have consented under section 15 of the PDPA (having provided the data for investigation), such consent is limited by purpose and reasonableness under section 18(a) of the PDPA. Disclosures must be strictly necessary to fulfil the stated purpose; in this case, revealing the individual's identity and email was found to be unreasonable and breached the PDPA.

On damages under section 48O of the PDPA, the Court reaffirmed that claimants must establish a direct causal link between the breach and the harm alleged. The individual's claim for emotional distress failed, as the harm stemmed from subsequent legal proceedings and disclosures by the third party, breaking the chain of causation.

Impact: Organisations should carefully assess disclosures made under deemed consent, ensure they are necessary and reasonable, and document their rationale to mitigate PDPA liability.

Contact a specialist in Singapore

Publication of Advisory on New Endpoint Detection and Response Killer Tool Used by Multiple Ransomware Groups Advisory

On August 16, 2025, the Cyber Security Agency of Singapore (CSA) issued Advisory AD-2025-018, highlighting the emergence of a new Endpoint Detection and Response (EDR) killer tool actively used by at least eight ransomware groups, including Blacksuit, RansomHub and Medusa.

The tool exploits vulnerable signed drivers to disable EDR systems, randomises driver names to evade detection, and can terminate security processes. Its modular design allows threat actors to create "blind spots" in organisational defences, significantly increasing the risk of ransomware infection.

CSA has recommended several key measures, including: (i) enforcing strict driver controls and blocking untrusted or unsigned drivers; (ii) using EDR solutions with self-protection and anti-tampering features; (iii) prompt patching of systems and reviewing remote access tools; (iv) conducting threat hunts using CSA's published indicators of compromise; and (v) restricting privileged accounts and applying least privilege principles.

Impact: Organisations should urgently assess their endpoint security posture, strengthen EDR configurations, and adopt the recommended safeguards to reduce their exposure to this evolving ransomware tactic.

Contact a specialist in Singapore

Proposed amendments to the Public Sector (Governance) Act 2018

On August 12, 2025, the Ministry of Digital Development and Information (MDDI) launched a public consultation from August 12, 2025, to September 2, 2025, on proposed amendments to the Public Sector (Governance) Act. MDDI aims to enhance the use of data by enabling public sector agencies to share data more effectively with authorised external partners who work closely with them, under the existing public interest purposes prescribed in the PSGA.

MDDI also aims to clarify the legal basis for data sharing with authorised external partners and introduce safeguards to ensure responsible data use by these partners. Additionally, MDDI is considering clarifying that public sector agencies may internally use data they are authorised to share with other public sector agencies under the same legal framework.

Impact: Organisations involved in providing services or managing data for public agencies should monitor the consultation outcomes and prepare to align their operations with new regulations.

Contact a specialist in Singapore

Publication of Remediation Guide for a Compromised SharePoint Environment related to CVE-2025-53770 and CVE-2025-53771 Advisory

On July 24, 2025, the Cyber Security Agency of Singapore (CSA) published Advisory AD-2025-016, a remediation guide for organisations affected by CVE-2025-53770 and CVE-2025-53771 vulnerabilities in on-premises SharePoint servers.

The advisory warns that patching alone may not suffice if a SharePoint server has already been compromised. It outlines a four-phase incident response framework: Identification, Containment, Remediation, and Recovery, and provides detailed steps such as rotating keys, restarting IIS, removing web shells, and rebuilding servers or restoring from known clean backups.

Impact: Organisations operating internet-exposed SharePoint servers must urgently assess whether they were vulnerable or compromised, enact the full response playbook (beyond just patching), rotate cryptographic keys, rebuild or restore systems where necessary, and enhance hardening (e.g. stricter logging, EDR deployment, network segmentation) to prevent reinfection.

Contact a specialist in Singapore

Publication of Protecting Yourself and Your Organisation from Data Breaches Advisory

On July 11, 2025, the Cyber Security Agency of Singapore (CSA) published an advisory on "Protecting Yourself and Your Organisation from Data Breaches." A data breach is broadly defined to include unauthorised access, disclosure, loss or misuse of personal data, and remains a key cybersecurity risk.

For individuals, adopting strong cyber hygiene practices, such as secure passwords, multi-factor authentication, and caution when handling links or attachments, can help reduce the impact if their data is compromised. For organisations, strengthening defences against common breach vectors and implementing robust cybersecurity and incident response measures are essential to reduce breach risks and safeguard customer trust.

CSA has also published tailored resources: (i) a guide for individuals on common causes of breaches and protective steps; and (ii) organisational guidance on preventive measures and breach response.

This advisory highlights that both proactive prevention and incident preparedness are essential baseline practices for safeguarding trust and resilience in Singapore's digital ecosystem.

Impact: Organisations should review and update their data breach response plans, ensure staff are trained on incident handling, and strengthen baseline security controls (e.g. access management, MFA) to align with CSA's expectations and reduce liability in the event of a breach.

Contact a specialist in Singapore

Publication of Choosing the Right Authentication Methods Advisory

On July 8, 2025, the Cyber Security Agency of Singapore (CSA) issued Advisory AD-2025-015, titled Choosing the Right Authentication Methods.

The advisory warns that weak or misconfigured authentication systems are increasingly targeted by attackers, and guides organisations and users in selecting authentication mechanisms that balance security, usability, and risk.

It reviews four main authentication approaches:

1. Multi-Factor Authentication (MFA): Adds a second factor (e.g. app-based code) to improve security
2. Federated Single Sign-On (SSO) via OIDC: Allows login using trusted third-party identity providers
3. FIDO2 (password-less, hardware or biometric tokens): Offers strong protection without relying on passwords
4. Magic links / One-Time Passwords (OTPs): Provide simpler methods for lower-risk scenarios

Impact: Organisations should assess their current authentication setups, phase out weak methods (e.g. single passwords or poorly secured OTPs), adopt stronger options like MFA or FIDO2 where appropriate, and calibrate choices based on their risk profile and user convenience to reduce exposure to credential-based attacks.

Contact a specialist in Singapore

Slovakia

Draft amendment to limit soft opt-in to direct marketing to one year

On November 12 2025, a draft amendment to Slovakia's rules on direct marketing is scheduled to take effect if adopted. Currently, businesses may promote their own similar goods and services without prior consent if contact details were obtained during a sale or contractual relationship, provided customers can opt out at any time.

The proposal would introduce a new safeguard: contact details collected in connection with a sale could only be used for marketing purposes for up to one year after the contractual relationship ends. After that, companies would need fresh consent.

This measure builds on existing provisions that prohibit anonymous emails, misleading links, and unsolicited messages where an individual has opted out. Lawmakers argue that the change would strengthen consumer protection, set clearer boundaries for businesses, and reduce the risk of misuse of personal data in the digital space.

Impact: If adopted, the draft amendment will limit how long companies in Slovakia can rely on the "existing customer" exemption for direct marketing. Contact details collected during the sale of goods or services could only be used for marketing for one year after the end of the contractual relationship. After this period, businesses would need to obtain fresh consent before sending further marketing communications.

Clients should review how they collect, store and use customer data, and prepare to update internal marketing practices, privacy notices and consent mechanisms if the proposal is passed. The draft is not yet law, so no immediate action is required, but monitoring of legislative progress is recommended.

Contact a specialist in Slovakia

Employer fined for taking employee photographs for attendance system

The Slovak Data Protection Authority (DPA) fined an employer EUR 1,500 and ordered corrective measures for unlawfully processing employee biometric data. The employer had introduced an attendance system requiring workers to have their facial images captured and linked to personal ID numbers when clocking in, leaving work, taking lunch breaks or recording business-related movements.

Under the GDPR, such data may only be processed with a valid legal basis under Article 6 GDPR, and in some cases Article 9. In this case, no lawful basis applied. Employees had not given consent and the employer could not rely on legitimate interest or legal obligation. The employer justified the system by citing past attempts by staff to falsify attendance. Employees repeatedly objected to the use of facial images and asked for their objections to be recorded, but management refused. The system remained in use from 2018 until February 2025, when the authority intervened following a complaint. Although the employer has since stopped using the camera system, the authority concluded that the long-term use of the data without legal grounds breached GDPR.

Impact: The decision by the DPA highlights the risks of using biometric systems for workplace attendance without a valid legal basis under the GDPR. Employers cannot rely on arguments of convenience or past misuse to justify such processing. Facial images used for identification require strict compliance with Article 6 GDPR, and in some cases Article 9.

For clients, the ruling underlines the importance of conducting a lawful basis assessment before introducing monitoring systems that rely on sensitive data. Where consent is sought, it must be freely given and cannot be bundled with the employment relationship. Employers must also document and respond to employee objections, rather than dismiss them.

Although the employer has ceased using the system, the fine confirms that historic practices may still result in sanctions. Clients should review existing attendance and monitoring tools to ensure GDPR compliance.

Contact a specialist in Slovakia

South Africa

Court rules on use of CCTV with line of sight over neighbour's private space

On September 17, 2025, the High Court of South Africa (Court) handed down judgment in the case of Phillips and Another v Bradbury (Appeal) (A200/2024) [2025] ZAWCHC 430 (*Phillips* case).

The *Phillips* case is a dispute between neighbours which demonstrates the tension in South Africa between security concerns and privacy rights. In this case, a party had installed CCTV cameras on its property, with a line of sight over the neighbouring property's pool, entertainment area, patio and a bedroom. It was not disputed that the CCTV use infringed on the neighbour's constitutionally protected right to privacy, and the Court was tasked with determining whether this amounted to a justifiable limitation of the right to privacy. The Court also considered common law protections under the nuisance doctrine, and emphasised that the areas under surveillance were 'essential private spaces' and clear zones of 'intimacy and autonomy', which are deserving of 'increased constitutional protection'. In this instance, the Court ultimately concluded that the limitation of the neighbouring party's rights to privacy and dignity is not justified.

Impact: Persons using CCTV cameras with a line of sight over the private spaces of others, may be found to be an unjustifiable limitation of their right to privacy. Such persons should consider whether there are alternative, and less intrusive, options available to address their security concerns, such as repositioning CCTV cameras to prevent surveillance of private spaces, or installing electric fencing, burglar bars or motion detector security systems.

Contact a specialist in South Africa

Spain

Agencia Española de Protección de Datos (AEPD) imposes fine of €500,000 against bank for major data breach

On September 5, 2025, the AEPD (the Spanish Data Protection Agency) fined a bank for breaching Article 5.1 (f) of GDPR (confidentiality and integrity). A ransomware attack was detected in October 2022 at subcontractor managing debt collection for the bank. The breach exposed data of more than 124,000 individuals, including personal data. The AEPD concluded that the bank failed to ensure adequate security measures and oversight of its processors. The company's appeal for reconsideration was dismissed confirming the sanction and ordering implementation of robust safeguards within six months. The bank's appeal for reconsideration was dismissed.

Impact: Financial institutions and large corporations must verify security standards, contractual clauses, and risk management throughout their supply chain. This example also demonstrates expectations for proactive breach notification and mitigation.

Contact a specialist in Spain

AEPD fines bank €300,000 for failing to Implement adequate data security measures

On September 4, 2025, the Agencia Española de Protección de Datos (AEPD) sanctioned Sociedad de Gestión de Activos Procedentes de la Reestructuración Bancaria (SAREB) after a ransomware attack affecting its processor, Stratesys. This exposed the data of around 7,200 individuals, including SAREB employees. The AEPD found that SAREB failed to ensure that sufficient security measures were implemented under Article 5(1)(f) GDPR and did not properly regulate the processing agreements as required by Article 28 GDPR. The sanction included fines of €250,000 for breach of integrity and confidentiality and €50,000 for deficiencies in the processor agreement. The AEPD ordered corrective measures requiring SAREB to implement stronger safeguards and revise and update its data processing agreements.

Impact: This sanctioning procedure is noteworthy because it reinforces that controllers must actively supervise compliance. The new Directors of the AEPD also emphasized the sensitivity of exposing national ID data (DNI) and considered its exposure particularly serious.

Contact a specialist in Spain

AEPD resolution concerning the exercise of rights of access and erasure

The AEPD partially upheld a complaint against the Directorate-General of Traffic (DGT). The Claimant alleged that DGT failed to properly address their requests for access and erasure under the GDPR. The AEPD confirmed that DGT was right to deny erasure, since retention of traffic data is required for legal and public interest purposes (Article 17(3)(b) GDPR). It also accepted that DGT did not have to disclose the names of staff members who accessed the claimant's data, as employees are not considered "recipients" under Article 15 GDPR. However, the AEPD held that DGT's generic reference to its Records of Processing Activities (RAT) was insufficient: the authority should have provided specific categories of actual recipients of the claimant's data. The AEPD ordered DGT to issue a proper certification within 10 business days.

Impact: This Decision is important because it clarifies the scope of the right of access: while the data subjects cannot obtain the names of staff members who access their data, they are entitled to know the categories of actual recipients of their personal data. Controllers must provide specific and meaningful information, not just generic references. The case sets a precedent for how Spanish entities must align access rights with CJEU case law (C-154/21), reinforcing transparency obligations.

Contact a specialist in Spain

Switzerland

DPS issues revised General Terms and Conditions for public authority ICT contracts

On March 17, 2025, Digital Public Services Switzerland (DPS) brought into force the revised General Terms and Conditions for ICT goods/services (GTC). The 2025 edition applies to all ICT contracts concluded by Swiss public authorities from that date onwards. The revision introduces a clearer structure, consistent terminology, and strengthened provisions on data protection, information security, and sustainability.

Key updates include: the introduction of clearer definitions for contracting parties (**"service procurer"** and **"provider"**), consistent references to "ICT goods/services", and explicit rules on processing personal data, including transfers abroad. Providers must now obtain prior written consent before involving subcontractors and must impose contractual obligations relating to data protection, confidentiality, and information security on them. The rules also set stricter requirements on staff reliability and the careful use of resources supplied by the procurer.

The revised GTC place stronger emphasis on information security: the procurer retains sole authority over personal data, providers must take appropriate technical and organisational measures, review them regularly, and report security breaches immediately. Contract penalties have been consolidated and clarified, covering breaches of confidentiality, data protection, information security, and delays in performance.

Impact: Since March 17, 2025, all new ICT contracts between Swiss public authorities and providers have been subject to the revised GTC. Private-sector contracts are not affected. Providers working with the public sector must ensure compliance, particularly in subcontracting approvals, cross-border data processing, staff checks, and security breach reporting. Public authorities should already have aligned procurement and contract templates accordingly. For providers entering into new agreements with the state, failure to adapt may result in penalties or stricter enforcement by contracting authorities.

Contact a specialist in Switzerland

Federal Act on Electronic Identity Verification (E-ID)

On September 28, 2025, Swiss voters approved the Federal Act on Electronic Identity Verification (E-ID) in a national referendum. The new law establishes a government-run electronic identity system that allows individuals to securely verify their identity online when accessing digital services. The E-ID is intended to be voluntary, privacy-friendly and managed entirely by the federal government, which is a shift from the previously rejected model based on private providers. The new system is designed to improve online security and simplify interactions with both public authorities and private companies. The Federal Council stated that the E-ID will meet strict data protection standards and will be rolled out gradually over the coming years.

Impact: For information only at this stage. Implementation details, including timelines and technical requirements, will be provided once the Federal Council issues further guidance on the rollout.

Contact a specialist in Switzerland

United Kingdom

Proposals to update the Telecommunications Security Code of Practice 2022

On August 28, 2025 the UK Government opened a consultation on its proposals to update the Telecommunications Code of Practice 2022. This is the guidance for medium-large telecoms providers on their compliance with the Communications Act 2003.

The consultation is part of the government's review of the Code to ensure it takes account of new threats and evolving technologies in addition to being clear on the approach to compliance.

Impact: Public telecoms providers (and others who operate in this field) should consider reviewing and responding to the proposals. Consultation closes on October 22, 2025.

Contact a specialist in the United Kingdom

NCSC guidance on how cyber security measures can mitigate risks in genAI systems

On September 2, 2025 the National Cyber Security Centre (NCSC) published a blog post containing guidance on how far cyber security approaches can help mitigate risks in generative AI systems.

The guidance explores how traditional cyber security practices like vulnerability management and disclosure can help mitigate risks associated with AI systems (including safeguard bypasses such as jailbreaking, prompt injection etc).

The guidance goes on to discuss the benefits of public disclosure programmes – which work by crowdsourcing security testing of a system by encouraging a researcher community to find and report successful bypasses – to mitigate AI cyber risks.

The guidance says that effective disclosure programmes require a clearly defined scope, robust internal controls, and easy-to-track reports.

Developers should implement strong internal security before launching public disclosure programmes.

Impact: The guidance is recommended reading for decision-makers involved in the design, development, and deployment of AI systems, researchers exploring AI safety and security and anyone interested in frontier AI and/or cyber security.

Contact a specialist in the United Kingdom

NCSC outlines importance of planning and rehearsing cyber incident recovery

On September 9, 2025 the NCSC published a blog post on the importance of planning and rehearsing cyber incident recovery.

The guidance emphasises that no organisation is immune to every type of cyber-attack and that even the best defences can be breached. The ability to respond quickly, recover operations, and minimise damage when incidents occur can support cyber resilience. Effective resilience planning will involve preparing response plans, regularly testing them, and ensuring all staff know their roles in a crisis.

The NCSC advises organisations to treat resilience as a core part of their cyber strategy, not just an afterthought to technical defences. Practising recovery (e.g. through exercises and simulations) can help identify weaknesses and ensure a coordinated response when real incidents happen.

Impact: The guidance is recommended reading for those responsible for security incident defence, response and/or recovery in medium and large organisations.

Contact a specialist in the United Kingdom

No de minimis threshold of seriousness for GDPR compensation claims says Court of Appeal

In *Farley v Paymaster (1836) Ltd (trading as Equiniti) [2025] EWCA Civ 1117* (judgment dated August 22, 2025), the Court of Appeal found that there is no *de minimis* threshold of seriousness for GDPR compensation claims, i.e. compensation is recoverable for data infringements involving "non-material" damage. Such damage could include the fear of what *could* happen as a consequence of a data breach even if that fear did not actually come to pass, as long as *"the alleged fear is objectively well-founded but not if the fear is… purely hypothetical or speculative"*.

Impact: For our insights on the judgment, see ByteSize: Court of Appeal reshapes the foundations of data breach litigation from our TMT Litigation and Disputes Management team.

For commentary on how the judgment impacts the pensions sector specifically, see this article from our specialists.

Contact a specialist in the United Kingdom

ICO aims to clarify how law applies to storage and access technologies

On September 11, 2025, the ICO published a blog post aiming to address common misunderstandings on how the law applies to storage and access technologies (including the rules governing the use of cookies).

On July 7 the ICO launched a public consultation on its updated guidance for storing and accessing information on user devices (developed with the new Data (Use and Access) Act 2025 provisions in mind). The guidance clarifies when cookies can be used without consent, provided the risk to user privacy is low. Stakeholders were encouraged to submit feedback by September 26, 2025.

Impact: For more information, see our article What's in the oven, or going stale with the UK's cookies?

Contact a specialist in the United Kingdom

ICO releases guidance on encryption

On September 2, 2025, the Information Commissioner's Office (ICO) published on social media details of its new encryption guidance, following consultation.

The ICO highlights encryption as a valuable security measure in maintaining trust and confidence in digital services, and guarding against potentially very serious consequences.

The guidance covers what is encryption, how encryption relates to data protection, data storage and transferring data, how to implement encryption (including algorithm and key selection and management), as well as practical encryption scenarios. It doesn't cover end-to-end encryption (E2EE), privacy-enhancing technologies, encryption and ransomware, or the potential impact of quantum computing.

The guidance outlines a number of scenarios when encryptions may be used, including: (i) when storing data on a device or network to render it unintelligible to unauthorised users without a key; (ii) when transferring data across a network to shield it from interception; and (iii) during processing. The guidance notes that organisations should consider an appropriate review period for their use of encryption in line with their obligations under the security provisions in the UK GDPR.

Impact: Organisations should refer to the guidance to ensure their use of encryption techniques aligns with their data protection obligations.

Contact a specialist in the United Kingdom

ICO shares cyber security tips for small businesses

On September 17, 2025 the ICO shared its cyber security tips for small businesses to take to improve their data security and resilience. The tips include: backing up your data; using strong passwords and multi-password authentication; installing anti-virus and malware protection; and making sure wi-fi connections are secure.

Contact a specialist in the United Kingdom

September online safety round-up

Consultation on online safety fees regime

On September 1, 2025 Ofcom published its third consultation in connection with the implementation of the online safety fees regime.

The consultation is open until October 1, 2025 and outlines proposed guidance for preparing and submitting fees-related notifications, including required details and supporting evidence. This will enable compliance with The Online Safety Act 2023 (Fees Notification) Regulations 2025 which will come into effect on October 8, 2025.

This consultation follows consultations on the Qualifying Worldwide Revenue (QWR) in July and aims to help providers of regulated services prepare their QWR returns and navigate the notification process.

These measures implement the requirements of the Online Safety Act 2023 (OSA) which allow Ofcom's operating costs for the online safety regime to be recovered through fees imposed on providers of regulated services. Providers are required to notify Ofcom in certain circumstances in relation to the fees regime, unless they are exempt.

Consultation on super-complaints guidance

On September 8, 2025 Ofcom opened a consultation on its draft guidance for making super-complaints under the OSA. The aim of super-complaints is to allow designated organisations to bring evidence of the most significant online harms and restrictions on freedom of expression to Ofcom's attention.

Consultation closes on November 3, 2025.

Self-harm content to be brought into priority offence band

On September 8, 2025 the Department for Science, Innovation and Technology announced that the OSA will be amended to make content encouraging or assisting serious self-harm a priority offence for all users. This means that providers will need to remove all such content before users are exposed to it. Secondary legislation to implement this change is expected this autumn.

Consultation on data preservation notices

On September 16, 2025 Ofcom launched a consultation on guidance for online platforms on the information to retain if a child's death is investigated by a coroner. From September 30, 2025 Ofcom has the power to issue a data preservation notice, requiring a platform to preserve data about a deceased's child's activity if requested by a coroner. Ofcom's guidance on these notices is being introduced by way of updates to its Online Safety Information Powers Guidance. The consultation also covers updates to its guidance on responding to Coroner Information Notices.

Responses to consultation are due by October 28, 2025.

Contact a specialist in the United Kingdom

UK trusted third party AI assurance roadmap published

On September 3, 2025 the Department for Science, Innovation and Technology (DSIT) published a trusted third-party AI assurance roadmap.

The purpose of AI assurance is to increase confidence in AI, which should in turn promote AI adoption and economic growth. DSIT has identified that the UK third-party AI assurance sector is struggling to grow, due to factors including under-developed technical standards, skills-shortages, lack of access to information about AI systems, and the pace of AI development. The roadmap is intended to address these issues and boost the market.

Impact: The Government intends to take targeted action to:

- establish a consortium of stakeholders to support AI assurance professionalisation, including by developing a voluntary professional code of ethics, a skills and competencies framework, and mapping information access requirements for AI assurance providers, with the intention of a certification or registration scheme for AI assurance being developed in the future
- establish the AI Assurance Innovation Fund to support development of the AI assurance market

Contact a specialist in the United Kingdom

NCSC publishes updated version of Cyber Assessment Framework

On August 6, 2025, the National Cyber Security Centre (NCSC) announced the release of a new version of its Cyber Assessment Framework (CAF).

Version 4.0 of the CAF introduces the following changes:

- a new section on building a deeper understanding of attacker methods and motivations to inform better cyber risk decisions;
- a new section on ensuring software used in essential services is developed and maintained securely;
- updates to the section on security monitoring and threat hunting to improve the detection of cyber threats; and
- improved coverage of AI-related cyber risks throughout the CAF.

The NCSC produced the update in full consultation with the cyber regulators and other cyber oversight bodies that use the CAF. The NCSC invited stakeholders to provide feedback on the new version of its CAF to Support to Regulation mailbox.

Impact: The NCSC will ensure that future iterations of the CAF keep pace with the regulatory proposals in Cyber Security and Resilience Bill, which will be laid before parliament later this year.

Contact a specialist in the United Kingdom

Data (Use and Access) Act 2025: Key provisions take effect

On Wednesday August 20, 2025, key provisions of the Data (Use and Access) Act 2025 come into force – pursuant to *The Data (Use and Access) Act 2025 (Commencement No. 1) Regulations 2025* – including provisions relating to:

- access to customer data and business data (Part 1)
- processing of special categories of personal data (section 74)
- duties of the Commissioner in carrying out functions (section 91)
- the PECRs (section 109)
- duty to notify the Commissioner of personal data breach: time periods (section 111)
- the Information Commission (section 117, except subsection (4)(a))
- information for research about online safety matters (section 125)
- the eIDAS Regulation (section 129)

The full list of provisions coming into force can be found here.

Impact: To recap, on June 19, 2025, the Data (Use and Access) Act 2025 (DUAA) officially became law in the UK, introducing significant changes to the UK GDPR, Data Protection Act 2018 and Privacy and Electronic Communications Regulations. The DUAA reforms how UK data protection law is regulated and enforced and amends the rules relating to access to customer data and business data, transfers of personal data out of the UK, individuals' rights in relation to their personal data, the use of cookies and similar technologies and automated decision-making.

For further information, you can read our Guide to the UK's Data (Use and Access) Act 2025 or watch our client webinar.

Contact a specialist in the United Kingdom

Understanding the UK Data (Use and Access) Act 2025 – Webinar

Understanding the UK Data (Use and Access) Act 2025 – Webinar: in our recent webinar on Thursday, 24 July, we explored the UK's Data (Use and Access) Act 2025.

We are pleased to share some key highlights from the session and provide you with access to the recording.

During the webinar we covered:

- the governance, structure and enforcement powers of the UK's data protection regulator (including the new complaint mechanism)
- data protection fundamentals, including lawful bases for processing and special categories of personal data
- individuals' rights, including in relation to automated decision making
- international data transfers
- e-privacy issues, including direct marketing communications, breach reporting and the use of cookies

Contact a specialist in the United Kingdom

ICO consults on new guidance brought about by DUAA – recognised legitimate interests and the right to complain

On August 21, 2025, the Information Commissioner's Office (ICO) launched two public consultations, seeking views on draft guidance it has produced to help organisations with the application of new compliance obligations brought about by the Data (Use and Access) Act 2025 (DUAA).

The first piece of draft guidance relates to the new lawful basis of recognised legitimate interest. The consultation closes on October 30, 2025. The guidance outlines what a 'recognised legitimate interest' is – one of the seven lawful bases for processing personal data- and explains the five purposes for which it may be relied on: (i) public task disclosure requests; (ii) national/public security and defence (iii) emergencies (iv) prevention/detection/investigation of crime, and (v) safeguarding. The guidance also sets out how organisations can carry out the 'necessity test' in respect of each purpose. In addition, the guidance reminds organisations of some of the other considerations they should have when relying on the recognised legitimate interest test.

The second piece of draft guidance, Complaints guidance for organisations, relates to the new right to complain. The consultation closes on October 19, 2025. The guidance sets out the elements of the new right, including how the right must be made available to exercise, and how/when complaints must be acknowledged and responded to.

These guidance topics relate to the more practically significant changes brought about by the DUAA. Most organisations in the UK will need to amend their data protection compliance documentation, systems and/or processes as a result of them.

Impact: UK organisations should review the guidance and consider responding to the consultations.

Contact a specialist in the United Kingdom

Government responds to data intermediaries consultation

On August 1, 2025, the Government published a response to its call for evidence on data intermediaries (launched on 17 March).

The call for evidence explored: (i) the reasons for the limited exercise of some data subject rights, particularly the right to data portability, and whether rules around the delegation of data subject rights to third parties should be more explicit; (ii) the activity of data intermediaries, seeking to define the nature and activities of data intermediaries; (iii) the barriers preventing data intermediaries from working to their full extent, as well as critical success factors; and (iv) risk factors associated with the wider exercise of data subject rights by third parties and the prospect of growth in the activities of data intermediaries.

In its response, the Government concludes that the challenges faced by stakeholders – which are currently limiting the uptake and growth of the sector – can be summarised in three groups: (i) awareness – stemming from people not knowing their data subject rights or how they could benefit from using them; (ii) friction – where third party data access requests are often slow and burdensome, and data controllers lack the incentives to improve this; and (iii) legal ambiguity – which underpins the other challenges by causing confusion about the legal roles of data intermediaries and the ability to delegate data subject rights to them.

Impact: The government is assessing policy options to support the data intermediaries sector and wider economy, and will provide an update in due course. Organisations engaged in or looking to become engaged in 'smart data' initiatives should watch out for updates. Please also consider contacting our Data, Privacy and Cybersecurity team for advice on how the new access to customer data and business data provisions in the DUAA might apply.

Contact a specialist in the United Kingdom

ICO reminds law enforcement authorities of obligations regarding use of facial recognition technologies

On August 13, 2025 the ICO released a statement alongside seven data protection reminders regarding the use of facial recognition technology in law enforcement.

The seven reminders regarding live facial recognition (LFR) are as follows:

- use of LFR must be strictly necessary for law enforcement purposes
- the purpose and justification should be clearly defined and limited
- appropriate data protection documentation must be put in place
- effectiveness is a key consideration for strict necessity and proportionality
- watchlists should be used in accordance with the data protection principles
- organisations deploying LFR should consider how to provide applicable privacy information to the public
- there should be periodic testing and reviews of the technology to ensure that it remains accurate and effective towards understanding and eliminating bias

Impact: The ICO conducts regular audits of police forces' data protection practices. The statement was made in light of the ICO's recent audits of police forces' use of LFR. Law enforcement authorities deploying facial recognition technologies should read the statement and reminders.

Contact a specialist in the United Kingdom

FCA working group releases report on using synthetic data

On August 19, 2025, the Financial Conduct Authority (FCA) released a report on assessing and mitigating challenges associated with synthetic data use. The report highlights insights and best practices identified by Synthetic Data Expert Group (SDEG) members.

The latest report builds on the considerations outlined by the SDEG in its first report, published in March 2024. This second report responds to feedback from the FCA's 2022 call for input and discusses what synthetic data is doing, how it does it, and how firms are working through governance, compliance, and trust issues.

The key aim of the report is to explore potential governance considerations for organisations and practitioners planning to work with synthetic data. Among other things, the report sets out nine key principles relevant to synthetic data projects which may serve as a reference point for discussion and exploration.

Impact: The report is recommended reading for synthetic data practitioners and those working with synthetic data across the financial services sector.

Contact a specialist in the United Kingdom

Call for views on adoption of trust services

On August 4, 2025 the Department for Science, Innovation & Technology launched a call for views on adoption of trust services.

Trust services, such as electronic signatures, confirm the authenticity and integrity of electronic documents and transactions. In the UK the provision of trust services is regulated by the UK eIDAS Regulation, as modified by the Data (Use and Access) Act 2025.

Trust services can be simple, advanced or qualified, on a sliding scale of technical security and evidential weight. There are currently no registered qualified trust service providers in the UK, and take up of advanced or qualified e-signatures has generally been low in the UK.

Impact: The aim of the call for views is to gather information to help inform policy development in this area. It was open until September 20, 2025 and views are sought from organisations providing trust services in the UK and organisations that use, or could use, those services.

Contact a specialist in the United Kingdom

CMA final report on public cloud infrastructure services market

On July 31, 2025, the Competition and Markets Authority (CMA) published its report on investigations into public cloud infrastructure services.

The report concludes that competition is not working well in this market. Main concerns related to market power, customers' ability to switch, and licensing practices. The CMA recommends launching Strategic Market Status investigations under the Digital Markets Competition and Consumers Act 2024 (DMCC), which could lead to targeted interventions in the sector to address competition concerns.

Impact: Businesses that are likely targets of the planned market investigation are encouraged to analyze the DMCC in more detail. Reviewing data sources and governance, as well as setting up internal response teams, can help navigate stressful investigations. It is recommended to train and prepare staff in advance to ensure adequate cooperation with the authorities and mitigate risk.

Contact a specialist in the United Kingdom

Online Safety Act super complaints

On July 22, 2025 The Online Safety Super-Complaints (Eligibility and Procedural Matters) Regulations 2025 were made. The regulations will come into force on December 31, 2025, setting out which entities can bring super-complaints under the Online Safety Act 2023 and how they go about doing this.

Contact a specialist in the United Kingdom

Call for evidence on human rights and AI

On July 25, 2025 the Joint Committee on Human Rights launched an inquiry into how human rights can be protected in the age of AI.

A call for evidence was open until September 5, 2025. This asked for views on various matters, including whether changes to the current legal and regulatory framework are required.

Contact a specialist in the United Kingdom

Discussion paper on AI and the law

On July 31, 2025 the Law Commission published a discussion paper on AI and the law. It says "*the paper aims to raise awareness of legal issues regarding AI, prompting wider discussion of the topic, and to act as a step towards identifying those areas most in need of law reform*".

Issues discussed include autonomy and adaptiveness; causation and liability; mental element of offences; opacity; oversight and reliance on AI; training and data; legal personality.

Contact a specialist in the United Kingdom

Boosting AI chip design in the UK

On August 18, 2025, the Council for Science and Technology (CST) published an advice paper to Government (provided in July) on building a sovereign AI chip design industry in the UK.

The CST made six recommendations to boost the role of semiconductors in the UK which include:

- Boosting the number of chip designers in the workforce by 2030
- Reviewing investment in training and skills and investment across the "entire innovation pipeline"
- Setting clear objectives for the semiconductor industry so they can engage with the direction of travel
- Support to SMEs and start-ups through access to semiconductor infrastructure and leading edge technology

Impact: With the forecast for AI chips to grow globally in the next decade there is prime opportunity to invest and gain the economic benefits of such predicted growth. We wait to see how the Government responds to this "once in a 20 year opportunity for the UK to build a profitable AI chip design industry in one of the largest markets in the world".

Contact a specialist in the United Kingdom

Data (Use and Access) Act 2025 (Commencement No. 1) Regulations 2025 made

On July 21, 2025 the Data (Use and Access) Act 2025 (Commencement No. 1) Regulations 2025 (Regulations) were made.

We reported in June that the Data (Use and Access) Act 2025 had received Royal Assent on June 19, 2025 and that its provisions would take effect in stages.

Under the Regulations, a number of key provisions will take effect on August 20, 2025, including:

- Part 1 (access to customer data and business data)
- section 74 (processing of special categories of personal data)
- section 91 (duties of the Commissioner in carrying out functions)
- section 92 (codes of practice for the processing of personal data)
- section 104 (court procedure in connection with subject access requests)
- section 107 (regulations under the UK GDPR)
- section 109 (the PEC Regulations)
- section 110 (interpretation of the PEC Regulations), except subsection (2)(a) and (b) and subsection (3)
- section 111 (duty to notify the Commissioner of personal data breach: time periods)
- section 117 (the Information Commission), except subsection (4)(a)
- section 129 (the eIDAS Regulation)
- section 136 (report on the use of copyright works in the development of AI systems)
- Schedule 14 (the Information Commission)

Contact a specialist in the United Kingdom

Investigatory Powers (Communications Data) (Relevant Public Authorities and Designated Senior Officers) Regulations 2025

On July 7, 2025 the Investigatory Powers (Communications Data) (Relevant Public Authorities and Designated Senior Officers) Regulations 2025 (Regulations) were made.

The Regulations amend Schedule 4 to the Investigatory Powers Act 2016 (c. 25) (IPA). This schedule sets out the public authorities, other than local authorities, who may exercise powers under Part 3 IPA to obtain communications data, the statutory purposes for which that data may be obtained, the type of communications data which may be obtained and any designated senior officers within those authorities who may authorise the obtaining of communications data internally, including in urgent cases.

Impact: The amendments allow certain public authorities to apply for an authorisation (a section 60A authorisation) to acquire communications data from the Investigatory Powers Commissioner for purposes such as preventing or detecting crime, interests of public safety or interests of national security.

Contact a specialist in the United Kingdom

ICO consults on regulatory approach to online advertising

On July 7, 2025 the Information Commissioner's Office (ICO) launched a call for views on its enforcement approach to Regulation 6 PECR (the rules governing consent and the use of cookies and similar technologies).

Specifically, the ICO is exploring whether a risk-based approach to enforcing PECR could allow publishers to deliver online advertising to users who have not granted consent, where there is a "*low risk to their privacy*".

The responses will inform the ICO's statement – to be published in early 2026 – identifying advertising activities unlikely to trigger enforcement action under PECR. The ICO will consider safeguards to reduce risks to users and enable new commercially viable approaches to online advertising. The ICO will support the development of secondary legislation to amend the PECR rules and create a new exception to the PECR consent requirements for specific low-risk advertising purposes, as needed.

The call for views remained open until August 29, 2025.

Contact a specialist in the United Kingdom

ICO consults on revised cookies guidance

On July 7, 2025 the ICO launched a consultation on its updated cookies guidance (rebadged to guidance on storage and access technologies).

The ICO has updated the guidance to reflect the amendments contained in the Data (Use and Access) Act 2025. In particular, the ICO has added a new chapter to explain the five new exceptions (the communication exception, the strictly necessary exception, the statistical purposes exception, the appearance exception and the emergency assistance exception).

In addition, the "How do we comply?" chapter has been split into multiple chapters and now includes refreshed examples as well as some new policy lines.

The consultation ended on September 26, 2025.

Contact a specialist in the United Kingdom

ICO releases 2024-25 annual report

On July 15, 2025 the ICO released its 2024-25 annual report.

The report is split into three main sections: (a) a performance overview which reviews the ICO's work across 2024/25 including its three strategic causes identified as its key areas of focus: children's privacy, AI and biometrics and online tracking, (b) an accountability report which includes declarations about corporate governance, remuneration and staffing, parliamentary accountability and audit reporting, and (c) financial statements which set out the ICO's financial performance.

Contact a specialist in the United Kingdom

Compute roadmap – advancing AI in the UK

On July 17, 2025 the Government unveiled its new Compute Roadmap, a 10 point plan "*to deliver on UK national priorities*".

The aim is to deliver on the Government's commitment to increase the compute infrastructure within the UK and includes:

- launching and expanding the capacity of the AI Research Resource – "*a suite of advanced supercomputers that provides AI-specialised compute capacity to researchers, academia, and industry*"

- setting up a network of National Supercomputing Centres (the first being in Edinburgh)
- establishing the AI Sovereignty Unit to focus on developing the UK's domestic AI capabilities and compute ecosystem
- investing in Wales and Scotland with AI Growth Zones to aid data centre development powered by responsible energy sources and support R&D

Impact: Alongside Compute, the AI for Science strategy has been announced to embed and grow AI in the science sector.

Contact a specialist in the United Kingdom

Evaluation survey on Software Security Code of Practice

On June 27, 2025 the Department for Science, Innovation and Technology launched an evaluation survey to assess uptake and feedback on the Software Security Code of Practice (CoP) and its supporting materials. The voluntary CoP was launched in May and is intended to set minimum – or baseline – standards for cyber security in software development and supply to help protect against software supply chain cyber-attacks and incidents. See the May edition of Commercially Connected for more detail.

Impact: The survey closes on December 16, 2026 and is open to both suppliers and buyers of software. All organisations should familiarise themselves with the principles of the CoP and consider responding to the survey; software developers and suppliers to ensure that they can comply with the principles, and buyers to ensure that they understand what "good" looks like when it comes to software security and to help them assess their suppliers' compliance.

Contact a specialist in the United Kingdom

New laws proposed to tackle cybercrime

On July 22, 2025 the UK Home Office published its response to its January 2025 consultation on proposals for legislation to mitigate the threat of ransomware, together with a press release stating its intention to go ahead with these measures.

Ransomware is malicious software that prevents or restricts use of IT systems or data and/or enables data theft. The perpetrators usually demand a ransom payment (typically in cryptocurrency) in return for restoration of systems and/or to prevent publication of stolen data. In the UK ransomware is regarded as the most serious type of organised cyber crime and cyber security threat.

The consultation put forward three proposals:

- **Proposal 1:** a targeted ban on ransomware payments for public sector bodies and owners and operators of regulated critical national infrastructure. Views were also sought on whether essential suppliers to these sectors should be included in any ban. The response to consultation showed strong support for a targeted ban on ransomware payments and so the Government intends to go ahead with developing this proposal. Feedback also demonstrated a need for clarity on who precisely would be included in the ban and whether the ban would have extraterritorial effect, as well as guidance to support compliance. There was also positive feedback on extending the ban to essential suppliers, but it was recognised that further scoping would be required to work out how this would work in practice.
- **Proposal 2:** a new ransomware payment prevention regime. This would apply to all organisations and persons not subject to the total ban on ransomware payments, potentially subject to a threshold. They would have to liaise with authorities, who would provide support and guidance, before making any ransomware payment. Authorities would have the power to block payments in certain circumstances, e.g. if the payment could breach sanctions or terrorism legislation. The responses to this Proposal were more mixed, with the highest proportion of support for an economy-wide regime for those who are not included in the ban.
- **Proposal 3:** a new ransomware incident reporting regime, regardless of whether or not the victim intends to make a ransomware payment. The responses showed strong support for a mandatory regime.

Impact: The aims of the proposals are to reduce the amount of money paid from the UK to ransomware criminals; to gain intelligence on this criminal sector in order to improve operational agencies' capabilities to disrupt and investigate ransomware actors; and to improve Government understanding of ransomware threats to help drive interventions. All organisations should monitor developments and engage with future consultations to help shape this legislation.

Contact a specialist in the United Kingdom

Ofcom Online Safety Act 2023 consultation

On June 30, 2025 Ofcom opened a consultation on its proposals to strengthen its first edition Illegal Content and Protection of Children Codes of Practice under the Online Safety Act 2023.

The proposals aim to address the latest emerging risks and the latest developments in tech, as well as evidence obtained by Ofcom in its engagement with stakeholders. The proposals include:

- preventing illegal content going viral, by online service providers having protocols to respond to spikes in illegal content during a crisis; potentially illegal content to be checked by service providers before being recommended to users; enhanced oversight of livestreams through reporting functions and human August 2, 2025akAugust 2, 2025ainst users who share or upload illegal content or content that is harmful to children
- increased use of technology to prevent illegal content from being seen by users, including hash matching to identify intimate image abuse, terrorist content and child sexual abuse material; and automated tools to detect illegal and harmful content
- protecting children through better age assurance; better controls over livestreaming including preventing comments and reactions to children's livestreams; and banning individuals who share child sexual abuse content

Impact: Consultation closes on October 20, 2025 and Ofcom is planning to publish its revised guidance by summer 2026. All in-scope organisations should carefully review the proposals and share their views with Ofcom on how appropriate and feasible these proposals are.

Contact a specialist in the United Kingdom

DSIT releases Final Statement of Strategic Priorities for Online Safety

On July 2, 2025 the Department for Science, Innovation & Technology designated its Final Statement of Strategic Priorities for Online Safety (SSP) for the purpose of Sections 172 and 173 of the Online Safety Act 2023 (OSA).

The SSP sets out the UK government's focus areas for online safety and Ofcom is required to have regard to the SSP in acting as regulator for the OSA.

The SSP sets out 5 priorities:

- embed safety by design to ensure safe online experiences, in particular for children, and to work towards expulsion of illegal content and illegal disinformation
- transparency and accountability for delivering online safety outcomes, including to improve understanding oJuly 16, 2025July 16, 2025, 202July 14, 2025o tackle them, and to ensure that terms of service are clear and consistently enforced
- an agile and robust approach to regulation to monitor and tackle emerging harms, including threats from AI-generated content
- create an inclusive and informed digital society that is resilient to harms, misinformation and disinformation
- foster innovation in online safety technologies to improve safety and drive growth

Ofcom now has 40 days in which to state its proposed actions in relation to the SSP, and will also be required to report on these on an annual basis.

Impact: Organisations in-scope of the OSA should review the SSP so that they understand Ofcom's areas of focus and can build their own compliance pathways.

Contact a specialist in the United Kingdom

Final form Protection of Children Codes published under Online Safety Act 2023

On July 4, 2025 Ofcom published updated versions of its Protection of Children Codes under the Online Safety Act 2023 (OSA) for user-to-user services and for search services.

Providers of in-scope services are required to carry out a children's risk assessment by July 24, 2025 in respect of services that are likely to be accessed by children. From July 25, 2025 (subject to the Codes completing the Parliamentary process) they will need to use proportionate safety measures to protect children using their services from harmful content.

The Code for user-to user services contains guidance on governance and accountability, terms of service for users, age assurance measures, content moderation, user reporting and complaints, recommender systems and user support.

The Code for search services contains guidance on governance and accountability, publicly available statements, search moderation, user reporting and complaints and user support, including on search features and functionalities.

Ofcom also reminds organisations that it is currently consulting on proposals to apply the parts of the Illegal Content Codes that cover blocking and muting user accounts and disabling comments to a wider range of services, in order to capture smaller services that are likely to be accessed by children. Responses were due by 22 July 2025.

All providers of in-scope services should ensure that they complete children's risk assessments and put appropriate child safety measures in place to comply with the OSA requirements. Ofcom has made it clear that it will be taking enforcement action against non-compliant services.

UPDATE: on July 9, 2025 Ofcom announced the start of an enforcement programme to check whether services are complying with the children's risk assessment duties under the OSA. It has issued formal information requests to a number of service providers, requiring them to submit records of their children's risk assessments by 7 August 2025.

Impact:

Contact a specialist in the United Kingdom

Government report on the impact of social media algorithms

On July 11, 2025 the Science, Innovation and Technology Committee published a report on its inquiry into the spread of misinformation and the sufficiency of the online safety regime.

The current online safety regulation does not go far enough and the report urges the Government to regulate further on gen-AI and the spread of misinformation via social media companies by focussing on five "fundamental principles":

- public safety – gen-AI content needs clear labelling and fact checked misinformation needs demoting by platforms – further work between government and platforms is required
- free and safe expression – a proportionate approach is necessary
- responsibility for content – platforms and advertisers are currently "*unable or unwilling to address the monetisation of false and harmful content*" – they need to be accountable for content, undertake risk assessments and report on these measures
- control over content and data – users need the power to control their information feeds (they also need to be liable for what they post and take responsibility)
- technological transparency – further work is required to uncover how algorithms operate and other measures. This is one of the key pieces of information needed to further regulate online harms

We expect the Government to respond to the following recommendations within two months:

- a greater role for Ofcom in holding platforms accountable for misinformation
- the level of responsibility social media companies have in the "publication" of content
- a research project on the level and nature of harm caused by "recommendation systems" with online services being made accountable for harms caused
- social media platforms to embed tools in their systems to deprioritise and address misinformation posts and give users control to re-set their data recommended algorithms
- minimum standards for platforms to comply with in addressing online content – risk assessments and reporting will form part of this together with tracking the source of misinformation
- an annual report to Parliament by Government which sets out the state of misinformation online, tracking trends and issues and setting out successes and failures
- regulation of "small but risky" platforms
- government to be clear on responsibilities for foreign disinformation campaigns perhaps by using the National Security Online Information Team which should be placed on a statutory footing
- pass legislation on gen-AI platforms to provide risk assessments and provide transparency information on how their models operate and what safeguards are in place

- to regulate and scrutinise digital advertising (including the current opaque supply chain), a new arm's length body should be created (or alternatively Ofcom's powers extended)
- the ASA should develop comprehensive guidelines for all actors within the digital advertising ecosystem and supply chain
- "know your customer" checks for participants in the advertising supply chain to heighten transparency
- Ofcom should be empowered to give penalty notices to platforms when they allow harmful content to be monetised through their services

Impact: In the light of this report, businesses operating in the tech, media, advertising and online service sectors should:

- consider their content moderation and crisis protocols – are these robust?
- review their policies for references to user well-being in the light of harmful content and empower users to control their content
- to the extent practicable, increase transparency when engaging with public bodies
- understand their advertising supply chain; and
- be prepared for (and track) future regulatory changes

Contact a specialist in the United Kingdom

July updates from Ofcom

On July 8, 2025 Ofcom published a report pursuant to its obligations under the Online Safety Act 2023. This addresses researcher access to platform data and sets out three potential frameworks including using existing rules, introducing new duties backed by a regulator and enabling access through an independent intermediary. Ofcom's analysis suggests a combination of the 3 approaches would best meet researcher need and so it will engage with the Government on its findings.

On July 11, 2025 Ofcom published a discussion paper following on from its 2024 paper on Deepfake Defences. This second paper focuses on deepfake attribution, evaluating the effectiveness of watermarking, metadata, provenance tools, and AI-generated labels. These measures are currently non-mandatory, but Ofcom has indicated they will inform future enforcement, codes of practice, and platform oversight– especially in scenarios involving fraud, impersonation, and user harm.

On July 18, 2025 Ofcom launched a consultation on draft guidance to help providers of regulated services determine their qualifying revenue for the purpose of fees and penalties. Views are invited until September 10, 2025 and will be reviewed as part of finalising the guidance. This will be of interest to providers of regulated services who may wish to respond.

On July 21, 2025 Ofcom published a transparency statement and final transparency reporting guidance to support in implementing phase 3 of the Online Safety Act 2023. Only providers listed on Ofcom's public register of "categorised services" are required to publish transparency reports so they will be interested to understand how to prepare these in compliance with Ofcom's requirements.

Contact a specialist in the United Kingdom

Consultation on self-driving vehicles

On July 21, 2025 the Government opened a public consultation to help shape the future of self-driving vehicles. It seeks views on the regulation of taxi, private-hire and bus-like self-driving vehicles once they hit roads in Great Britain.

This forms part of the Government's plan to bring forward pilots of such vehicles to Spring 2026. All stakeholders are invited to share their views to help shape policy on aspects such as accessibility, permits and approval processes. The consultation closed on September 28, 2025.

Contact a specialist in the United Kingdom

Government to work with ChatGPT provider

On July 21, 2025 Open AI and the UK Government signed a non legally binding strategic partnership with plans to expand AI security research collaboration, explore investment into data centre infrastructure and look at how public services can make best use of advancing technologies.

This follows on from the AI Opportunities Action Plan unveiled by the Government in January.

Contact a specialist in the United Kingdom

Welsh Strategic AI Advisory Group and Office for AI

On June 28, 2025 the Welsh Government announced that it had set up a Strategic AI Advisory Group to provide advice on adopting AI in the public sector in Wales, as well as Office for AI within the Welsh Government.

Contact a specialist in the United Kingdom

With special thanks to our authors **Lizzie Charlton**, **Sara Ellis** and **Angela Kindness**.

United States

California Governor Signs Transparency in Frontier Artificial Intelligence Act

On September 29, 2025, the California Governor passed the Transparency in Frontier Artificial Intelligence Act. This act regulates foundation models that are trained with high levels of power.

Developers of these frontier models will be required to publish two documents – a transparency report and an AI framework. The AI framework must include descriptions of how the developer is meeting global AI practices, mitigating and addressing risk, and instituting internal governance to monitor these risk and mitigation strategies.

Impact: This follows a trend of greater AI restrictions being instituted in California, a hub of many leading AI companies.

Contact a specialist in the United States

California Privacy Health Data Location and Research Act

California's Privacy Health Data Location and Research Act was signed into law September 26, 2025. This act makes it unlawful to collect, use, sell, or share information gathered from a person at a family planning center unless it is required to perform the services requested. A family planning center includes all clinics that provide reproductive health services.

Additionally, this act prohibits the creation of a geofence around in-person health care service locations. This regulation includes a ban on geofences that are designed to send notification to the consumer or to send advertisements to the consumer.

Impact: This law extends California protections over consumer data which is collected for health and medical purposes.

Contact a specialist in the United States

California Privacy Protection Agency Announces Investigation on Non-Compliance with Right to Opt Out of Sale of Personal Information

California joins Colorado and Connecticut in an effort to investigate non-compliance with the Global Privacy Control (GPC). The California Consumer Privacy Act requires that businesses allow consumers the chance to opt-out of the sharing or sale of their personal data. GPC is a tool which allows businesses and consumers a streamlined way to facilitate this opt out process.

California will investigate businesses that are failing to accommodate consumers' opt out requests, in violation of state law.

Impact: This is in line with several states' increased attention to enforcing regulations allowing consumers to opt out of the selling and sharing of their personal data. Businesses should ensure their opt-out features work as described.

Contact a specialist in the United States

North Carolina Executive Order on AI

On September 2, 2025, the North Carolina Governor signed an Executive Order on AI, which created the AI Leadership Council and AI Oversight Teams for each state agency.

The AI Leadership Council will advise the North Carolina government on AI policies and training by creating an AI Strategic Roadmap, recommending AI policies, recommending AI literacy strategies, making AI workforce recommendations, and submitting a yearly AI Strategic Recommendation to the Governor.

Impact: This executive order follows a trend of states implementing strategies to encourage responsible AI innovation.

Contact a specialist in the United States

Texas Acts in Data Brokers Take Effect

Two Texas acts came into effect September 1, 2025, SB 1343 and SB 2121.

- SB 1343 requires that data brokers with internet websites or mobile applications provide consumers with conspicuous notice of their consumer rights. Data brokers will be required to provide a link to this notice as part of their data broker registration.
- SB 2121 redefines data brokers as any business entity that collects, processes, or transfers personal data that it did not directly collect from the individual. Data collection, processing, or transferring does not need to be the principal source of revenue for the data broker.

Impact: These acts are in line with other states acts that seek to expand consumer rights over the collection of their data.

Contact a specialist in the United States

Amended Texas Mini-TCPA will go into Effect on September 1, 2025

On September 1, 2025, Texas Senate Bill 140 (SB 140) will go into effect, significantly expanding the scope of telemarketing regulations in Texas. SB 140 impacts multiple subsections of Texas Business and Commerce Code Sections 301-305 (Texas Mini-TCPA) that are applicable to businesses that call or text Texas residents as well as businesses that call or text from Texas. SB 140 is just the latest amendment to a state-level equivalent of the Telephone Consumer Protection Act (TCPA). As with other "mini-TCPAs," the revised Texas Mini-TCPA compounds the litigation risk for companies that communicate with their customers and consumers at large via phone and text.

Impact: Businesses that call and text Texas residents should be aware of the risk of repeat litigants, as the revised law explicitly permits claimants to bring multiple claims for violations of the different requirements under the Texas Mini-TCPA. Businesses that market to consumers in Texas should bring their policies and procedures into compliance.

Discover more

Contact a specialist in the United States

National Institute of Standards and Technology (NIST) Publishes NIST SP 800-53 Control Overlays for Securing AI Systems Concept Paper

NIST published a concept paper August 14, 2025 detailing the design and implementation of a secure, trustworthy AI system. This approach assists organizations in implementing security controls on their AI use and gives guidelines to identify potential risks. The concept paper discusses types of AI systems that organizations could employ and the specific risks of each.

Impact: For information only at this stage.

Contact a specialist in the United States

Operational Technology Cybersecurity Guidance

On August 13, 2025, the Cybersecurity and Infrastructure Security Agency (CISA) released guidance on operational technology and cyber-concerns. The guidance encouraged operational technology owners and operators to develop asset inventories to track assets that require greater security. By developing and maintaining these systems, organizations can begin to create targeted security systems and can assess their existing vulnerabilities.

Impact: Businesses should evaluate whether any of their assets are subject to the asset inventory guidance.

Contact a specialist in the United States

Operation Robocall Roundup

As of August 7, 2025, the Anti-Robocall Litigation Task Force was created with over 50 Attorneys General to target voice providers and downstream service providers that route and accept robocalls, which is against the Federal Communications Commission's rules. The Task Force is mandating that the providers submit plans to reduce illegal robocalls.

Impact: Businesses should review practices and policies related to robocalls and ensure compliance.

Contact a specialist in the United States

Illinois: Wellness and Oversight for Psychological Resources Act

Illinois's Governor signed the Wellness and Oversight for Psychological Resources Act on August 1, 2025. This act prohibits entities from using AI to offer therapy or psychotherapy services without a licensed professional's involvement.

The act permits licensed professionals to employ AI in therapy or psychotherapy only after informing the patient, in writing, of its use. However, licensed professionals must not use AI to make any independent therapeutic decisions, to detect mental states, to generate treatment plans, or to interact with clients.

Impact: For information only at this stage.

Contact a specialist in the United States

Minnesota's Consumer Data Privacy Act Takes Effect

On July 31, 2025, Minnesota's comprehensive privacy act went into effect. This legislation applies to all businesses conducting business in Minnesota or targeting Minnesota residents who process at least 100,000 consumers' personal data yearly or who process over 25,000 consumers' personal data and receive over 25% of their gross revenue from sale of this data. There is a carveout for small businesses.

Affected businesses are required to publish policies and procedures for compliance with the MCDPA. Additionally, businesses must ensure that consumers have the option to access, correct, and delete their personal data, opt out of personal data collection for certain purposes, and obtain a list of third parties to whom this data has been disclosed.

Impact: These regulations follow comprehensive data privacy laws in other states, with a focus on consumer rights over data. Businesses should evaluate their compliance.

Contact a specialist in the United States

The CCPA's Automated Decision-making Tool Rules: New Consumer Rights and Compliance Challenges

On July 24, 2025, the California Privacy Protection Agency (CPPA) unanimously adopted a comprehensive rulemaking package under the California Consumer Privacy Act (CCPA) that primarily addresses automated decision making technology (ADMT), cybersecurity audits, risk assessments, and CCPA's application to insurance. The rules are focused on three key matters: (1) the use of ADMT to make a significant decision affecting consumers, with increased transparency and new consumer and worker rights; (2) cybersecurity audits and risk assessments; and (3) greater accountability through expanded reporting requirements to the CPPA. The regulations also revise and attempt to provide clarity to certain terms, such as multifactor authentication, automated decision making, privileged accounts, and sensitive personal information, and train the spotlight on nuanced areas, such as employment and insurance.

Impact: Organizations should ensure that companies and employers understand their use cases, data maps, and data collection points; the automated technologies that they or a vendor, service provider, or contractor may use; ensure that recordkeeping practices and retention schedules have been updated, revisit their cybersecurity audit, and risk assessment frameworks; update their vendor commercial agreements (particularly if they support automated decision making); review privacy policy updates and internal policies; and confirm that systems are set up to support the new consumer rights. Further, with the increased access requirements, employers should consider training human resources personnel and individuals tasked with responding to rights requests so they are aware of potential employment claims that could arise from disclosure.

Discover more

Contact a specialist in the United States

The Trump Administration's Plan to Win the AI Race – a Legal Perspective

The recent release of the White House's "Winning the Race: America's AI Action Plan" (AIAP or Plan), bolstered by three Executive Orders, is a resounding call for new agency priorities; new cooperative arrangements, rollbacks and reinterpretations of legal precedents; and new challenges to the states' legal authority, all intended to ensure that the US prevails in the global AI race. The AIAP and EO#3 require that large language models procured by the federal government be free from ideological bias and social agendas, such as references to diversity, equity and inclusion and climate change. The National Institute of Standards and Technology (NIST) at the Department of Commerce is instructed to revise the NIST AI Risk Management Framework to remove references to DEI, perceived misinformation and climate change. Finally, the AIAP stresses that the nation must prevent "our advanced technologies from being misused or stolen by malicious actors," and must monitor for emerging and unforeseen risks from AI.

Impact: Despite the federal de-emphasis on regulation and enforcement, organizations should nonetheless pay careful attention to state regulation and take the steps necessary to have appropriate AI cybersecurity (especially when providing the federal government with advanced technologies), export control compliance for overseas expansion and contractual allocations of risk.

Contact a specialist in the United States

United States and Indonesia Publish Joint Statement on Agreement on Reciprocal Trade

The United States and the Republic of Indonesia agreed on July 22, 2025, to strengthen reciprocal trade agreements in existence since 1996. Included in this trade agreement is a commitment on digital trade, services, and investment.

Indonesia agreed to strengthen data transfer protections out of Indonesia and into the United States. On July 24, 2025, Indonesia clarified that this agreement focused on limited and legitimate data transfers, including for the use of search engines, cloud computing services, social media digital communications, e-commerce transactions, and digital research and innovation.

Impact: For information only at this stage.

Contact a specialist in the United States

California Judiciary Publishes AI Policies for the Judiciary

On July 18, 2025, the California Judicial Council published rules on use of generative AI in the judiciary. These rules require that any court not prohibiting the use of generative AI adopt a generative AI policy by December 15, 2025 that outlines the prohibited uses of AI, the steps required to ensure accuracy and to remove bias, and the requirement to disclose AI use.

Impact: Practitioners should continue to check both state and local court rules related to AI use.

Contact a specialist in the United States

Online Retailer Sued for Violating Kentucky Consumer Protection Act (KCPA)

The Kentucky Attorney General filed a lawsuit on July 17, 2025, against an online retail platform for violations of the KCPA.

Kentucky alleges that the retailer collected sensitive user personal information without consumer consent and beyond collection permitted in the ordinary course of business. These violations of the KCPA are underscored by the retailer's obligation as a Chinese Company to share data information with the Chinese Government.

Impact: This follows a trend of states pursuing violations of data regulations. Businesses should evaluate their compliance with applicable consumer protection and privacy laws.

Contact a specialist in the United States

Eighth Circuit Vacates FTC's "Click-to-Cancel" Rule in Custom Communications v. FTC

On July 8, 2025, the Eighth Circuit vacated an FTC rule citing the FTC's failure to comply with procedural requirements under 15 U.S.C. § 57b-3(b)(1). In October 2024, the FTC attempted to modernize its Click-to-Cancel Rule to keep pace with changes in the online marketplace by requiring businesses to: clearly disclose material terms; obtain express informed consent; and provide a cancellation mechanism as simple as the method used to enroll.

Businesses remain subject to Section 5 of the FTC Act, which prohibits unfair or deceptive practices, as well as similar state laws designed to prevent unfair or deceptive acts or practices. They should continually review company practices to prevent violations of these requirements.

Impact: The FTC's Click-to-Cancel Rule is no longer enforceable, however businesses should continue to transparently disclose all material terms of negative option offers, obtain consumers' express informed consent, and make it as easy for customers to cancel as it was for them to enroll.

Discover more

Contact a specialist in the United States

Who's Next? What the Patriots' Class Action Settlement Might Mean for Data Privacy

In a striking example of applying old laws to modern tech, the New England Patriots faced legal scrutiny under the 1998 Video Privacy Protection Act (VPPA)–a statute originally aimed at video rental stores like Blockbuster. A recent class action lawsuit alleges the team improperly shared personal data from users of its mobile app, leading to a preliminary settlement approval in federal court.

This case reflects a growing trend: as sports organizations increasingly adopt data-driven technologies, they also expose themselves to heightened privacy litigation and regulatory risk.

Impact: Organizations should mitigate risks by taking steps to: update privacy policies and consent language to improve transparency; implement Data Processing Agreements (DPAs); and conduct regular oversight, including privacy audits, to verify that collection practices are consistent with DPAs.

Discover more

Contact a specialist in the United States

Online Ticket Broker Settles over Violation of Connecticut Data Privacy Act (CTDPA)

An online ticket broker settled with the Connecticut Attorney General on July 8, 2025, over a violation of the CTDPA. The ticket broker was warned of deficiencies in their privacy notice on the grounds that it was unreadable, inoperable, and lacking in required data rights.

The broker failed to respond to Connecticut's investigation and did not cure the deficiencies within the CTDPA's allotted timeframe.

The broker settled the investigation for $85,000. It must comply with the CTDPA and must provide reports to the state for all consumer rights request received.

Impact: Businesses should ensure compliance with the CTDPA and should promptly respond to any deficiency notice received.

Contact a specialist in the United States

New York Amendment on Algorithmic Pricing

New York Senate Bill 3008 took effect July 8, 2025, prohibiting retailers from using algorithmic pricing models unless the consumer is notified in a clear and conspicuous manner of its use. Retailers are required to state: "THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA" on all relevant consumer goods. Personalized algorithmic pricing is defined as dynamic pricing derived by an algorithm using consumer data.

The law also requires that operators notify users when they use an AI companion, which includes any system using AI to simulate social human interaction.

Impact: Retailers that dynamically set prices with the assistance of algorithmic tools or use AI companions should ensure compliance with New York law.

Contact a specialist in the United States

10-year federal moratorium on state AI regulation rejected

On July 1, 2025, the proposed 10-year federal moratorium on state AI regulation was decisively rejected by the Senate (99–1 vote), reinforcing states' autonomy in AI governance.

The moratorium was introduced by Senator Marsha Blackburn, with the support of many technology companies, to prevent diverging state regulations. The companies feared that over-regulation could discourage further AI innovation. This moratorium was eventually abandoned upon the belief that it would be unwise to prevent states from regulating in this space given the lack of federal regulations.

Impact: For information only at this stage.

Contact a specialist in the United States

Virginia Senate Bill 487 on Artificial Intelligence Takes Effect

On July 1, 2025, Virginia Senate Bill 487 took effect preventing public bodies, including legislatures, courts, agencies, and organizations wholly supported by public funds, from using AI unless they first perform an impact assessment to evaluate potential unlawful discrimination or disparate impact.

The Act defines AI as the simulation of human intelligence by a machine that can learn and adapt to analyze large volumes of data and make predictions based on future data inputs. The law also created the Virginia Commission on Artificial Intelligence which is tasked with studying the impacts of AI. This Commission will provide the General Assembly and Governor with AI recommendations.

Impact: Although limited to the public sector, this Bill demonstrates states' continued focus on AI.

Contact a specialist in the United States

Amendments to the Virginia Consumer Protection Act (VCPA)

As of July 1, 2025, Virginia requires businesses to get consent from consumers to obtain, sell, or disseminate any personally identifiable reproductive or sexual health information.

The VCPA amendments define reproductive or sexual health information to include reproductive or sexual health information services, reproductive or sexual health conditions, use of contraceptives, information related to menstruation or pregnancy, and information on diagnoses or diagnostic testing and treatment.

Impact: Businesses should evaluate their consumer consent mechanisms and data collection practices to ensure they obtain consumer consent prior to collecting, selling, or sharing any personally identifiable sexual and reproductive health information.

Contact a specialist in the United States

Colorado Privacy Act Biometric Data Amendments

As of July 1, 2025, Colorado's amendments to its Privacy Act are effective, requiring that businesses adopt a written policy relating to biometrics. With certain exceptions, businesses must make this written policy available to the public. Processors must also establish breach protocols specific to biometric data.

Biometric identifiers are defined as the processing, measurement, or analysis of a consumer's biological, physical, or behavioral characteristics that may be used to identify an individual.

Impact: Businesses collecting biometric data in Colorado should ensure that they have written policies satisfying the CPA and meet all consent requirements before collection. This follows a trend of states enacting specific consumer protections over biometric data, similar to the Illinois's Biometric Information Privacy Act.

Contact a specialist in the United States

Health Information Publisher settles over Violation of California Consumer Privacy Act

On July 1, 2025, a health information publisher settled with the California Attorney General for $1.55 million. The company was accused of violating the CCPA by informing consumers that they had disabled their cookies while simultaneously collecting these cookies for sale to third parties.

In addition to the settlement amount, the company must follow the requirements of the CCPA and develop a process to monitor consumer opt-out requests.

Impact: Businesses operating in California should evaluate compliance with the CCPA, including whether their opt-out and consent options work as advertised.

Contact a specialist in the United States

Virginia Act Regarding AI in Criminal Justice

A Virginia code amendment took effect July 1, 2025, which restricts the use of AI in the criminal justice process.

Judicial officers and others charged with criminal justice decisions are prohibited from making any decision solely based on the recommendation of an AI tool. These decisions include anything related to pre-trial detention, release, prosecution, adjudication, sentencing, probation, parole, correctional supervision, or rehabilitation.

AI tools include any machine-based system that analyzes data to make recommendations.

Impact: This reflects states' continued focus on AI regulation.

Contact a specialist in the United States

U.S. Department of Health and Human Services (HHS) Sued for Data Sharing

Several states brought suit against HHS on July 1, 2025, for the agency's decision to share sensitive personal information of recipients of Medicaid with the Department of Homeland Security (DHS).

The complaint alleges that the transfer of private sensitive information without consent of the recipient violates the federal Privacy Act, Health Insurance Portability and Accountability Act, and Federal Information Security Management Act.

Impact: This action follows a trend of coalition of states objecting to vast sharing of personal information without consumer's consent.

Contact a specialist in the United States

Oregon Consumer Privacy Act Takes Effect for Non-Profit Organizations

On July 1, 2025, the Oregon Consumer Privacy Act's provisions took effect for all entities organized as a 501(c)(3) under the Internal Revenue Code. Oregon's comprehensive privacy law went into effect generally on July 1, 2024. However, nonprofit organizations that meet the 501(c)(3) status were given one year before the provisions applied to them.

Nonprofit organizations will now be subject to regulations relating to the collection, sharing, sale, and retention of personal data.

Impact: Privacy laws in most states provide exemptions for nonprofit, 501(c)(3) organizations. Oregon's law diverges from other states by applying data privacy regulations to nonprofit organizations. 501(c)(3) entities should ensure compliance with Oregon's data requirements.

Contact a specialist in the United States

Our global team

Editorial team

Lizzie Charlton
Senior Associate PSL
T: +44 20 7919 0826
lizziecharlton@
eversheds-sutherland.com

Kirsty Howells-Greyling
Senior Associate
T: +44 20 7919 0756
kirstygreyling@
eversheds-sutherland.com

Supported by **Zak Ullah**, **Karandeep Singh**, **Lily Rooney-Walters**, **Nicole Morrick**, **Rhys Mabbitt**, **Eoghan Doyle**, **Katharine Dorkins**, **Jasmine Bunting**, **Matthew Audcent**, **Ciara Aveyard** and **Estelle Asante**

General Europe and International

Michael Bahar
Co-Lead of Global Cybersecurity and Data Privacy
T: +1 202 383 0882
michaelbahar@
eversheds-sutherland.com

Paula Barrett
Co-Lead of Global Cybersecurity and Data Privacy
T: +44 207 919 4634
paulabarrett@
eversheds-sutherland.com

Caroline Lyannaz
Partner
T: +33 1 55 73 40 00
carolinelyannaz@
eversheds-sutherland.com

Nils Mueller
Partner
T: +49 8 95 45 65 19 4
nilsmueller@
eversheds-sutherland.com

Rachel Reid
Head of Artificial Intelligence, US and Co-Lead of Global Cybersecurity and Data Privacy
T: +1 404 853 8134
rachelreid@
eversheds-sutherland.com

Olaf van Haperen
Partner
T: +31 6 1745 6299
olafvanhaperen@
eversheds-sutherland.nl

Austria

Manuel Boka
Partner
T: +43 15 16 20 162
manuel.boka@
eversheds-sutherland.at

Georg Roehsner
Partner
T: +43 1 51 62 01 60
georg.roehsner@
eversheds-sutherland.at

Michael Roehsner
Partner
T: +43 15 16 20 160
michael.roehsner@
eversheds-sutherland.at

Julian Maurer
Associate
T: +43 1 51620 137
julian.maurer@
eversheds-sutherland.at

Belgium

Maarten Stassen
Partner
T: +32 471 48 21 77
maartenstassen@
eversheds-sutherland.com

Céline Wauters
Partner
T: +32 2 737 93 44
celinewauters@
eversheds-sutherland.com

Bulgaria

Nikolay Bebov
Partner
T: +35 9 24 39 07 07
nikolaybebov@
eversheds-sutherland.bg

Victoria Marincheva
Senior Associate
T: +35 9 2 439 07 07
victoria.marincheva@
eversheds-sutherland.bg

China

Jack Cai
Partner
T: +86 21 61 37 1007
jackcai@
eversheds-sutherland.com

Sam Chen
Legal Director
T: +86 21 61 37 1004
samchen@
eversheds-sutherland.com

Olivia Chen
Associate
T: +86 21 61 37 1003
oliviachen@
eversheds-sutherland.com

Czech Republic

Radek Matous
Partner
T: +42 0 25 570 6554
radek.matous@
eversheds-sutherland.cz

Jaroslav Tajbr
Partner
T: + 42 0 255 706 561
jaroslav.tajbr@
eversheds-sutherland.cz

Estonia

Tambet Toomela
Partner
T: +37 2 61 41 99 0
tambet.toomela@
eversheds-sutherland.ee

Adu Arvisto
Lawyer
T: + 37 2 62 29 99 0
adu.arvisto@
eversheds-sutherland.ee

Erika Tuvike
Lawyer
T: + 37 2 62 29 99 0
Erika.tuvike@
eversheds-sutherland.ee

Finland

Anu Mattila
Partner
T: +358 50 550 5768
anu.mattila@
eversheds.fi

France

Gaëtan Cordier
Partner
T: +33 1 55 73 40 73
gaetancordier@
eversheds-sutherland.com

Caroline Lyannaz
Partner
T: +33 1 55 73 40 00
carolinelyannaz@
eversheds-sutherland.com

Camille Lehuby
Senior Associate
T: +33 1 55 73 42 33
camillelehuby@
eversheds-sutherland.com

Mélanie Dubreuil-Blanchard
Associate
T: +33 155 7 34 20 9
melaniedubreuil-blanchard@
eversheds-sutherland.com

Lea Khalife
Associate
T: +33 155 734 171
leakhalife@
eversheds-sutherland.com

Lucie Rontchevsky
Associate
T: +33 1 5573 4066
lucierontchevsky@
eversheds-sutherland.com

Germany

Nils Mueller
Partner
T: +49 8 95 45 65 19 4
nilsmueller@
eversheds-sutherland.com

Kevin Kurth
Senior Associate
T: +49 89 54565 174
kevinkurth@
eversheds-sutherland.com

Alexandra Klaus
Associate
T: + 49 8 95 45 65 28 3
alexandraklaus@
eversheds-sutherland.com

Domagoj Pavic
Associate
T: +49 895 456 5160
domagojpavic@
eversheds-sutherland.com

Viktoriia Khilinichenko
Professional Support Lawyer
T: +49 175 8727 687
viktoriiakhilinichenko@
eversheds-sutherland.com

Dr. Constantin Herfurth
Principal Associate
T: +49 8 95 45 65 29 5
constantinherfurth@
eversheds-sutherland.com

Christian Duerschmied
Senior Associate
T: +49 30 700140 958
christianduerschmied@
eversheds-sutherland.com

Isabella Norbu
Senior Associate
T: +49 16 09 36 02 368
isabellanorbu@
eversheds-sutherland.com

Jeanette Da costa leite
Senior Associate PSL
T: +49 89 54 56 54 38
jeanettedacostaleite@
eversheds-sutherland.com

Hong Kong

Cedric Lam
Partner
T: +852 2186 3202
cedriclam@
eversheds-sutherland.com

Duncan Watt
Legal Director
T: +852 2186 3286
duncanwatt@
eversheds-sutherland.com

Frankie Tam
Partner
T: +852 2186 4919
frankietam@
eversheds-sutherland.com

Hungary

Agnes Szent Ivany
Partner
T: +36 1 39 43 12 1
szent-ivany@
eversheds-sutherland.hu

Gergely Dzsinich
Co-Managing Partner
T: +36 1 39 43 12 1
dzsinich@
eversheds-sutherland.hu

Katalin Varga
Partner
T: +36 1 39 43 12 1
varga@
eversheds-sutherland.hu

Gréta Zanócz
Senior Associate
T: +36 1 39 43 12 1
zanocz@
eversheds-sutherland.hu

Iraq

Tawfiq Tabbaa
Partner
T: +96 2 77 77 11 22 9
tawfiqtabbaa@
eversheds-sutherland.com

Ireland

Daniel Jackson
Senior Associate
T: +35 31 66 44 975
danieljackson@
eversheds-sutherland.ie

Teniola Ayeni
Associate
T: +353 1 554 6179
teniolaayeni@
eversheds-sutherland.com

Italy

Massimo Maioletti
Partner
T: +39 06 8932 7025
massimomaioletti@
eversheds-sutherland.it

Edoardo Coia
Associate
T: +39 06 8932 7034
edoardocoia@
eversheds-sutherland.it

Valentina Palmisano
Associate
valentinapalmisano@
eversheds-sutherland.it

Andrea Zincone
Partner
T: +39 3357 818 196
andreazincone@
eversheds-sutherland.it

Andrea Mantovani
Counsel
T: +39 06 893 2701
andreamantovani@
eversheds-sutherland.it

Jordan

Nadim Kayyali
Partner
T: +96 2 77 97 77 77 6
nadimkayyali@
eversheds-sutherland.com

Latvia

Agris Bitans
Partner
T: +37 1 67 28 01 02
agris.bitans@
eversheds-sutherland.lv

Ilze Rozentāle
Associate
T: +37 1 67 28 01 02
ilze.rozentale@
eversheds-sutherland.lv

Elina Mucina
Partner
T: +37 1 67 28 01 02
elina.mucina@
eversheds-sutherland.lv

Dmitrijs Nemirovskis
Associate
T: +37 1 67 28 01 02
dmitrijs.nemirovskis@
eversheds-sutherland.lv

Lithuania

Rimtis Puisys
Partner
T: +37 0 52 39 23 73
rimtis.puisys@
eversheds.lt

Juste Sabanskaite
Assistant Lawyer
T: + 37 0 52 39 23 91
Juste.sabanskaite@
eversheds-sutherland.lt

Mauritius

Michael Hough
Partner
T: +23 0 21 10 55 0
michaelhough@
eversheds-sutherland.mu

Urvi Bhoowabul
Associate
T: + 23 058 20 93 90
urvibhoowabul@
eversheds-sutherland.mu

Nitish Hurnaum
Partner
T: +23 021 10 550
nitishhurnaum@
eversheds-sutherland.mu

Netherlands

Olaf van Haperen
Partner
T: +31 6 1745 6299
olafvanhaperen@
eversheds-sutherland.nl

Judith Vieberink
Senior Associate
T: +31 6 5264 4063
judithvieberink@
eversheds-sutherland.nl

Ilham Ezzamouri
Junior Associate
T: +31 1 0248 8063
ilhamezzamouri@
eversheds-sutherland.com

Robbert Santifort
Senior Associate
T: +31 6 8188 0472
robbertsantifort@
eversheds-sutherland.nl

Nathalie Djojokasiran
Junior Associate
T: +31 6 3820 3704
nathaliedjojokasiran@
eversheds-sutherland.com

Frédérique Swart
Junior Associate
T: +31 6 4812 7136
frederiqueswart@
eversheds-sutherland.nl

Poland

Marta Gadomska-Gołąb
Partner
T: +48 22 50 50 732
marta.gadomska-golab@
eversheds-sutherland.pl

Maciej Jakubowski
Associate
T: +48 22 50 50 730
maciej.jakubowski@
eversheds-sutherland.pl

Aleksandra Kunkiel-Kryńska
Partner
T: +48 22 50 50 775
aleksandra.kunkiel-krynska@
eversheds-sutherland.pl

Portugal

Paulo Sampaio Neves
Partner
T: +35 1 21 35 87 50 0
psampaioneves@
eversheds-sutherland.net

José Luís Monteiro
Lawyer
T: +35 1 22 83 46 74 0
jlmonteiro@
eversheds-sutherland.net

Margarida Roda Santos
Partner
T: +35 1 21 35 87 50 0
mrodasantos@
eversheds-sutherland.net

Tiago Macaia Martins
Principal Associate
T: +351 228 346 740
tmacaiamartins@
eversheds-sutherlnd.net

Qatar

Dani Kabbani
Partner
T: +97 4 44 02 59 11
danikabbani@
eversheds-sutherland.com

Cristina Craciun
Senior Associate
T: +97 4 44 02 59 09
cristinacraciun@
eversheds-sutherland.com

Romania

Mihai Guia
Partner
T: +40 2 13 11 25 61
mihaiguia@
eversheds-sutherland.ro

Alexandra Sulea
Partner
T: +40 2 13 11 25 61
alexandrasulea@
eversheds-sutherland.ro

Alexandra Chiorescu
Associate
T: +40 2 13 11 25 61
alexandrachiorescu@
eversheds-sutherland.ro

Cristian Lina
Partner
T: +40 2 13 11 25 61
cristianlina@
eversheds-sutherland.ro

Daniela Stanica
Associate
T: +40 2 13 11 25 61
danielastanica@
eversheds-sutherland.ro

Kingdom of Saudi Arabia

Mohammed Al AlDhabaan
Founding Partner
T: +96 6 11 27 79 84 4
aldhabaan@
aldhabaan-es.com

Leen Al Moaiqel
Associate

leenalmoaiqel@
aldhabaan-es.com

Anum Saleem
Legal Director
T: +96 6 11 27 79 83 6
anumsaleem@
aldhabaan-es.com

Singapore

Sharon Teo
Partner
T: +65 93 80 2637
sharonteo@
gtlaw-llc.com

Teo Wen Xuan
Associate
T: +65 66 37 88 85
wenxuanteo@
gtlaw-llc.com

Slovakia

Bernhard Hager
Partner
T: +42 1 232 786 411
bernhard.hager@
eversheds-sutherland.com

Simona Makúchová
Senior Associate
T: +421 23 27 86 41 1
simona.makuchova@
eversheds-sutherland.sk

Jana Sapáková
Counsel
T: +421 232 786 411
jana.sapakova@
eversheds-sutherland.sk

South Africa

Matthew Anley
Partner
T: +27 0 10 00 31 38 2
matthewanley@
eversheds-sutherland.co.za

Kelly Nevin
Partner
T: +27 10 003 1380
kellynevin@
eversheds-sutherland.co.za

Grant Williams
Partner
T: +27 10 003 1375
grantwilliams@
eversheds-sutherland.co.za

Meghan Annandale
Senior Associate
T: +27 10 003 1443
meghanannandale@
eversheds-sutherland.co.za

Spain

Vicente Arias
Partner
T: +34 9 14 29 43 33
varias@
eversheds-sutherland.es

Lucía Jurado
Lawyer
ljurado
@eversheds-sutherland.es

Sweden

Torbjörn Lindmark
Partner
T: +46 8 54 53 22 27
torbojnlindmark@
eversheds-sutherland.se

Sara Malmgren
Partner
T: +46 73 322 84 28
saramalmgren@
eversheds-sutherland.se

Hanna Ullerholt
Associate
T: +46 7 03 31 28 00
hannaullerholt@
eversheds-sutherland.se

Switzerland

Markus Näf
Partner
T: +41 58 255 56 50
markus.naef@
eversheds-sutherland.ch

Nadine Zollinger
Partner
T: +41 58 255 56 50
nadine.zollinger@
eversheds-sutherland.ch

Oliver Scharp
Associate
T: +41 58 255 56 50
oliver.scharp@
eversheds-sutherland.ch

Tunisia

Fares El Heni
Partner
T: +21 67 18 60 23 5
fareselheni@
eversheds-sutherland.com

United Arab Emirates

Geraldine Ahern
Partner
T: +97 1 24 94 36 32
geraldineahern@
eversheds-sutherland.com

Richard Chudzynski
Partner
T: +97 1 56 344 2786
richardchudzynski@konexoglobal.com

Andrew Garbett
Senior Associate
T: +97 1 49 43 638
andrewgarbett@
eversheds-sutherland.com

Lucrezia Berto
Senior Associate
T: +971 2 494 3600
lucreziaberto@
eversheds-sutherland.com

Skanda Reddy
Data Privacy Consultant
skandareddy@konexoglobal.com

Aben Pagar
Konexo Consultant
T: +971 50 91 75 19 6
abenpagar@konexoglobal.com

United Kingdom

Paula Barrett
Co-Lead of Global Cybersecurity and Data Privacy
T: +44 20 7919 4634
paulabarrett@
eversheds-sutherland.com

Karishma Brahmbhatt
Partner
T: +44 207 919 0727
karishmabrahmbhatt@eversheds-sutherland.com

Lorna Doggett
Partner
T: +44 20 7919 4698
lornadoggett@
eversheds-sutherland.com

Dave Hughes
Partner
T: +44 1223 44 3642
davidlhughes@
eversheds-sutherland.com

Liz Fitzsimons
Partner
T: +44 1223 44 3808
lizfitzsimons@
eversheds-sutherland.com

United States

Michael Bahar
Co-Lead of Global Cybersecurity and Data Privacy
T: +1 202 383 0882
michaelbahar@
eversheds-sutherland.com

Neal Higgins
Partner
T: +12 0 23 83 01 68
nealhiggins@
eversheds-sutherland.com

Frank Nolan
Partner
T: +1 212 389 5083
franknolan@
eversheds-sutherland.com

Rachel Reid
Head of Artificial Intelligence, US and Co-Lead of Global Cybersecurity and Data Privacy
T: +1 404 853 8134
rachelreid@
eversheds-sutherland.com

Mary Jane Wilson-Bilik
Partner
T: +1 202 383 0660
mjwilson-bilik@
eversheds-sutherland.com

Pooja Kohli
Counsel
T: +1 212 389 5037
pkohli@
eversheds-sutherland.com

Janell Johnson
Counsel
T: +1 202 383 0327
janelljohnson@
eversheds-sutherland.com

Tanvi Shah
Senior Associate
T: +1 858 252 4983
tanvishah@
eversheds-sutherland.com

Soroosh Faegh
Associate
T: +1 713 425 3574
sorooshfaegh@
eversheds-sutherland.com

Melissa Fox
Partner
T: +1 404 853 8109
melissafox@
eversheds-sutherland.com

Deepa Menon
Partner
T: +1 202 383 0928
deepamenon@
eversheds-sutherland.com

Brandi Taylor
Partner
T: +1 858 252 6106
branditaylor@
eversheds-sutherland.com

Alexander Sand
Partner
T: +1 512 721 2721
alexandersand@
eversheds-sutherland.com

Leslie Bender
Senior Counsel
T: +1 202 383 0274
lesliebender@
eversheds-sutherland.com

Claire Scavone
Associate
T: +1 404 853 8558
clairescavone@
eversheds-sutherland.com

Jonathan Freimann
Senior Associate
T: +1 202 383 0282
jonathanfreimann@
eversheds-sutherland.com

Dina Qubain
Associate
T: +1 415 869 6411
dinasqubain@
eversheds-sutherland.com

Rebekah Whittington
Associate
T: +1 404 853 8283
rebekahwhittington@
eversheds-sutherland.com

Christian Lamot
Senior Attorney
T: +1 612 713 9330
christianlamot@
eversheds-sutherland.com

Atiana Johnson
Staff Attorney
T: +1 202 383 0315
atianajohnson@
eversheds-sutherland.com

eversheds-sutherland.com

Connect

244703299\2