BCLP. Client Intelligent

Insights

EMEA DATA PRIVACY, DIGITAL REGULATION & AI - 2026 MID-YEAR ROUND-UP

Aug 10, 2026

Key Data Protection Developments

Data protection regulation and the data landscape continue to evolve at pace across EMEA, driven in part by the regulatory response to the increasing capabilities of AI tools. In this round-up, we look back at the developments that defined the first half of the year, from landmark AI and cybersecurity initiatives to important changes in online safety and digital advertising regulation across the UK, EU and Middle East and what they mean for organisations navigating an increasingly complex compliance environment, whilst looking ahead to 2027.

UK

Data Use and Access Act 2025 (DUAA)

On 29 January 2026, the Data (Use and Access) Act 2025 (Commencement No. 6 and Transitional and Saving Provisions) Regulations 2026 brought the majority of the key amendments to the UK's data protection and e-privacy framework in Part 5 of the DUAA into force commencing 5 February 2026.

Key Changes introduced by the Legislation

1. **Statutory Definition of Scientific Research**
   The legislation introduces a formal definition of *scientific research*, providing greater certainty around when personal data can be used for research purposes.

2. **Recognised Legitimate Interests**
   A new category of *recognised legitimate interests* has been introduced, allowing organisations to rely on certain predefined legitimate interests without undertaking a full balancing test in specified circumstances.

3. **Changes to Automated Decision-Making (ADM)**
   The rules governing automated decision-making have been updated, providing organisations with greater flexibility to use ADM while maintaining safeguards for individuals.

4. **New Special Categories of Personal Data**
   The Secretary of State has been granted the power to designate additional special categories of personal data in the future.

5. **Clarification of DSAR Requirements**
   The legislation provides further clarity on how organisations should respond to Data Subject Access Requests (DSARs), helping to streamline compliance obligations.

6. **Mandatory Complaints Handling Process**
   Individuals must now be given the opportunity to raise complaints directly with organisations before escalating matters to the Information Commissioner's Office (ICO). Organisations are required to acknowledge complaints within 30 days and respond without undue delay.

7. **Enhanced ICO Enforcement Powers**
   The ICO has been granted stronger enforcement powers, including the ability to issue "stop notices" requiring organisations to cease unlawful processing activities. In addition, penalties for breaches of the Privacy and Electronic Communications Regulations (PECR), including cookie and direct marketing violations, have been aligned with UK GDPR-level fines.

ICO consultation on data protection enforcement procedural guidance

In October, the ICO published its draft Data Protection Enforcement Procedural Guidance for consultation, which sets out how it approaches investigations, from the initial opening of a case and information-gathering stage through to decisions on whether formal enforcement action is appropriate. The guidance also explains the range of regulatory tools available to the ICO, alternative ways compliance issues may be resolved, and the limits of the regulator's enforcement powers.

The guidance does not address the ICO's approach to criminal prosecutions, except where its statutory information-gathering powers are relevant to investigating potential breaches of data protection legislation or criminal offences. Once finalised, the guidance will sit alongside the ICO's Data Protection Fining Guidance (which replaced part of the ICO's Regulatory Action Policy) as part of the statutory guidance that the ICO is required to publish under the Data Protection Act 2018. It will also incorporate statutory guidance on the handling of privileged communications. The consultation closed on 23 January 2026, and the final version of the guidance is expected to be published later in 2026.

ICO updated guidance on international transfers - January 2026

The ICO updated and enhanced its guidance on international transfers to make it quicker and easier for businesses to understand international transfer rules under UK GDPR. The streamlined guidance sets out a clear 'three step test' for organisations to use to identify if they're making restricted transfers.

On 15 July, the Department for Science, Innovation and Technology (DSIT) published an open call for evidence, seeking practical evidence on how the UK's international data transfer framework operates following reforms introduced by the Data (Use and Access) Act 2025. It is not the intention to consult on specific policy proposals but rather seek practical evidence to inform future policy development. Any future UK policy announcements will consider the importance of maintaining frictionless data flows with all international partners, including UK-EU data flows.

DSIT has structured the call around four themes:

- awareness and behaviour around international transfers (how organisations approach international data transfers in practice and whether behaviour matches the intention behind the development of transfer tools).
- understanding and use of international transfer mechanisms (how the UK's international data transfer regime operates, including adequacy decisions and alternative mechanisms such as Standard Data Protection Clauses (UK IDTA/Addendum) and Binding Corporate Rules, and use of Transfer Risk Assessments (TRA).
- balancing compliance with accountability, which examines how organisations manage transfer risk in practice.
- ensuring trust in the face of a changing world, which considers whether existing safeguards remain responsive to an evolving threat and technology landscape. Evidence suggests organisations use security measures such as encryption, virtual private networks (VPNs), and secure file transfer protocols when transferring data internationally.

The call for evidence is open until 11:59 pm on 9 September 2026.

ICO report on rise of agentic AI - January 2026

The ICO published a report on the rise of agentic AI. The report reflects the ICO's early stage thinking on agentic AI and covers the data protection and privacy risks (governance, rapid generation of personal data by agentic systems, data subject rights, accuracy etc) as well as innovation opportunities. On a more commercial note, the report covers some of the main drivers impacting the use of AI, examples including venture capital funding and the AI bubble (in the first half of 2025, agentic AI startups worldwide received approximately £ 2.8 billion of venture capital funding), cost savings from reduced staff costs and labour and a push on AI from national governments. The ICO has also been working with other sector regulators as part of the Digital

Regulation Cooperation Forum on horizon scanning activity in relation to agentic AI, in particular on a foresight paper – The Future of Agentic AI, published in March 2026.

Memorandum of Understanding with the UK Government

On 8 January the ICO and the UK Government signed a Memorandum of Understanding ("MOU") which sets out the government's commitment to raise data protection standards.

The commitment follows several serious, high-profile data breaches that undermined public trust in government, some of which also placed lives at risk.

The MOU covers key considerations such as early engagement in design of projects and new uses of people's data, reporting and accountability and ensuring compliance and creating a data safety culture.

Automated decision making in recruitment: ICO report March 2026

Following the launch of the ICO's AI and biometrics strategy in 2025, where automated decision making (**ADM**) was a key area, in March 2026 the ICO opened a consultation on its draft guidance on automated decision making in recruitment, which was open for consultation until May 2026. The new guidance provides clarity on how all organisations can use ADM and sets out where and how safeguards must be used. Key findings from the ICO's accompanying report outline that employers should increase transparency measures to ensure candidates are aware of the use of ADM, human involvement should be meaningful to ensure fair treatment and compliance, and the use of ADM should be monitored for fairness and bias.

The ICO has also consulted on its draft guidance about automated decision-making, including profiling to take into account the changes introduced by DUAA. The consultation closed on 29 May 2026.

Child Safety Online

UK Government consultation on online safety and AI chatbots

The UK Government's consultation, "Growing up in the online world," closed on 26 May 2026 and considered whether additional safeguards are needed for children using AI chatbots. The consultation explored a range of measures, including restricting access to sexually explicit content, requiring features that encourage users to take breaks, and imposing controls on chatbots that provide potentially harmful or unverified mental health advice.

Launched by the Department for Science, Innovation and Technology (DSIT) in March 2026, the consultation was prompted by concerns about the risks posed to young users by generative AI

tools. The Government is now considering whether certain AI services should be subject to enhanced protections for children, such as age verification requirements, limits on functionality, or restrictions on access. It has also published research on children's circumvention behaviours online (such as use of VPNs and bypassing age checks) and has proposed new default overnight curfews as well as automatic switching off of default features (such as the infinite scroll and use of personalised content) for older teens. This follows the announcement of a ban on social media services for under-16s, due in force in Spring 2027.

ICO and Ofcom joint statement: March 2026

The ICO and Ofcom joint statement on age assurance outlines the main areas of interaction between online safety and data protection laws. Both regulators expect organisations to use effective methods to verify users' ages where children may be exposed to online risks. Simply asking users to self-declare their age is generally not considered sufficient.

Any age-checking method will involve processing personal data, but this is permitted where it is necessary, proportionate and compliant with data protection laws. Organisations should also ensure that age checks are accurate and difficult to bypass.

Both regulators recognise that there is no one-size-fits-all solution and do not expect organisations to use age assurance technologies that are impractical or create disproportionate privacy risks.

Cyber Security and Resilience Bill

The proposed Cyber Security and Resilience Bill was reintroduced to Parliament following the May 2026 King's Speech. This will update the UK's NIS Regulations to expand their scope to cover managed IT service providers, data centres and operators managing electricity flows to smart appliances. Regulators would be given new powers to designate critical suppliers to essential services, and in-scope organisations will also be required to comply with the cyber security standards set out in the Bill. Organisations in scope would be required to notify regulators and the National Cyber Security Centre of significant cyber incidents within 24 hours, with a full report due within 72 hours. Data centres and managed service providers facing significant cyber incidents would also be required to take reasonable steps to identify and promptly notify affected customers. The Bill would introduce turnover-based penalties for serious breaches and grant ministers powers to direct regulators and the organisations they oversee to take specific, proportionate steps to prevent cyber-attacks where there is a threat to national security.

Read our insight on the UK's new Cyber Security and Resilience Bill and what it means for your organisation.

Data Security Governance ruling

In a judgment handed down on 19 February 2026, the Court of Appeal has confirmed that controllers remain subject to data security obligations in respect of personal data even where that data, if exfiltrated by a third party such as a cyber attacker, could not be used to identify the related individuals.

The CoA judgment confirmed that DSG was required to take appropriate security measures to protect personal data from unauthorised access.

Copyright and AI

On 18 March 2026, the UK government published a report on Copyright and Artificial Intelligence, assessing how copyright works are used to develop AI systems. It follows the government's consultation on Copyright and Artificial Intelligence, which ran from 17 December 2024 to 25 February 2025. The first section of the report considers the four policy options on copyright and the training of artificial intelligence models set out in the government's consultation, as well as alternative approaches. Subsequent sections consider aspects of copyright and AI training, including the wider regulatory environment. The government has concluded that it will not at this stage legislate to permit widening of the current text and data mining exception, so as to permit AI model developers to train their models on copyright works. The government proposes to address the gaps in evidence on copyright reform, consider alternative options (such as licensing models) and review the approach in light of wider market and international developments. Alongside this, it will support right holders to control and license their work, including through encouraging greater transparency.

EU

Digital Omnibus

On 11 February 2026, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) published a joint opinion on the European Commission's Digital Omnibus Regulation proposal (which aims to simplify certain requirements under the EU AI Act and facilitate its practical implementation), supporting the framework simplification but warning against diluting fundamental rights. It recognises the complexity of the AI regulatory landscape and welcomes initiatives designed to reduce administrative burdens for organisations.

The AI Omnibus entered into force on 27 July 2026. Amongst other changes, it extends timelines for the entry into force of the rules in relation to high-risk AU systems in Annex III to 2 December 2027, and 2 August 2028 for High-Risk AI embedded in physical products.

European Union and Brazil mutual adequacy

On 27 January 2026, the European Commission published a decision which now allows for the free flow of personal data between the European Union and Brazil with Brazil also adopting its own adequacy decision for data transfers from Brazil to EU. The mutual adequacy decisions come in the backdrop of the Partnership Agreement (EMPA) and Interim Trade Agreement (iTA) signed on 17 January 2026 between the EU and Mercosur countries (Argentina, Brazil, Paraguay and Uruguay) to increase further trade and investment through stronger and clearer rules. For the UK however, the position remains the same, transfers from the UK to Brazil should be subject to an adequate mechanism being in place.

EDPB and EDPS: Joint Statement on AI Generated Imagery (February 2026)

The statement represents the united position of 61 authorities across the world and reflects increasing global regulatory concern about the ability of AI systems to generate convincing images and videos of real individuals without their consent. While advances in AI are unlocking new opportunities and benefits, the widespread availability of image and video generation tools has also created new avenues for harm, including the production of non-consensual intimate imagery, defamatory content and other abusive material. The co-signatories emphasise the particular risks faced by children and vulnerable individuals, including cyberbullying, harassment and exploitation and remind all organisations developing and using AI content generation that these systems must be developed and used in accordance with applicable legal frameworks.

EDPB right to be forgotten report: February 2026

The EDPB has published a report on its Coordinated Enforcement Framework action on the right to be forgotten. This topic was selected as it is one of the most frequently exercised GDPR rights and one that is frequently complained about by data subjects. The 2025 involved 32 Data Protection Authorities (DPAs) (9 DPAs have initiated new formal investigations or have continued ongoing ones, and 23 DPAs carried out a fact-finding exercise). Some of the challenges identified included the absence of a documented and updated internal procedure to handle erasure requests, absence or inadequate training of staff members and insufficient information given to data subjects (especially as the right is not absolute).

The 2026 Coordinated Enforcement Framework action exercise will examine organisations' compliance with the GDPR's transparency and information requirements. Over the course of 2026, 25 DPAs will participate in the initiative, assessing how controllers meet their obligations to provide clear and transparent information to individuals.

ENISA updated cybersecurity market analysis

On 26 March 2026, the European Union Agency for Cybersecurity (ENISA) published version 3.0 of its Cybersecurity Market Analysis Framework (ECSMAF), updating its practical guidance for analysing cybersecurity markets. The framework is intended to support policymakers, regulators and businesses by providing a structured approach to assessing supply and demand across

specific cybersecurity sectors, while also enabling long-term market monitoring and more informed decision-making.

The updated framework introduces a streamlined seven-step methodology covering the entire analysis process, from defining the scope of a market study through to ongoing monitoring. It also includes standardised templates and reusable tools to improve the efficiency and consistency of data collection and analysis. Importantly, version 3.0 has been updated to reflect recent EU cybersecurity legislation, including the Cyber Resilience Act, ensuring greater alignment with current regulatory priorities and market developments.

EDPB case digest on the legitimate interest lawful basis: March 2026

The case digest collates decisions taken from the EDPB register of final one stop shop decisions and list of binding decisions and the decisions considered between December 2018 and June 2025. Themes that emerge from OSS decisions are the retrospective reliance on legitimate interest as a lawful basis for processing, the overlap with the ePrivacy Directive, and rental vehicle monitoring.

European Commission EU age verification app rollout

The European Commission has adopted a recommendation calling on EU Member States to accelerate the deployment of the EU age verification solution and make it available by the end of 2026. The initiative is intended to strengthen the protection of children online by enabling users to verify that they meet minimum age requirements while preserving their privacy.

The Commission has developed a blueprint for an age verification app that allows users to prove their age without disclosing their exact age, identity or other personal information. Member States may either launch the solution as a standalone application or integrate it into the European Digital Identity Wallet. The recommendation sets out steps to ensure the solution is deployed quickly and works consistently across the EU, supporting the Digital Services Act's objective of enhancing the privacy, safety and security of minors online.

EDPB and EDPS Joint Statement on Proposal for a Cybersecurity Act 2 and amendments to NIS 2 Directive

In their joint statement, the EDPB and EDPS emphasise the close and interdependent relationship between cybersecurity and data protection. While robust cybersecurity measures play a critical role in safeguarding personal data against unauthorised access, alteration and loss, the statement notes that certain cybersecurity measures may also have implications for individuals' fundamental rights, particularly the rights to privacy and data protection. The EDPB and EDPS therefore stress the importance of ensuring that cybersecurity initiatives are designed and implemented in a manner that respects applicable data protection principles and safeguards.

The statement broadly supports several key elements of the proposed Cybersecurity Act 2 package, including the creation of a single-entry point for incident reporting to simplify and streamline regulatory notifications. It also endorses the development of a European Cybersecurity Skills Framework under the leadership of ENISA, the further enhancement of the European Cybersecurity Certification Framework, and the establishment of a Trusted ICT Supply Chain Framework. Notably, the latter would address a range of non-technical risks affecting ICT supply chains in highly critical and other critical sectors, including geopolitical, legal, ownership, dependency and strategic interference risks.

EDPB DPIA template: April 2026

As part of its efforts to simplify GDPR compliance and promote greater consistency across the EU, in line with the commitments set out in the Helsinki Statement, the EDPB has adopted a standardised template for Data Protection Impact Assessments (DPIAs). The template is intended to assist organisations in preparing, documenting and demonstrating DPIA compliance in a more structured and harmonised manner across jurisdictions.

To support its use, the EDPB has also published an accompanying explainer document that provides practical guidance on completing the template. The document explains key DPIA concepts in accessible terms and addresses common questions and areas of uncertainty that controllers may encounter when carrying out and documenting their assessments. The template was open for public consultation until 9 June.

Cybersecurity Act and NIS2 Directive

On 20 January 2026, the European Commission published a comprehensive new Cybersecurity Package including a Proposal for a revised Cybersecurity Act and targeted amendments to the NIS2 Directive aimed at updating and strengthening cybersecurity resilience and capabilities in the EU.

The package introduces measures to simplify compliance with EU cybersecurity rules and risk-management requirements for companies operating in the EU, complementing the single-entry point for incident reporting proposed in the Digital Omnibus. Targeted amendments to the NIS2 Directive aim to increase legal clarity by simplifying jurisdictional rules, streamlining the collection of data on ransomware attacks and facilitating the supervision of cross-border entities with ENISA's reinforced coordinating role.

Read our briefing on the EU's Cyber Resilience Act.

Cyber incident reporting template under NIS2 Directive: May 2026

The EU has taken an important step towards reducing the compliance burden associated with the NIS2 Directive, with the NIS Cooperation Group, comprising EU Member States, the European

Commission and the EU Agency for Cybersecurity (ENISA), agreeing on common templates for incident reporting.

The templates establish a standardised format for reporting cybersecurity incidents across the EU. The initiative is intended to simplify reporting obligations for organisations, promote greater consistency among Member States and reduce the administrative complexity associated with NIS2 compliance.

The adoption of the templates forms part of the EU's broader drive towards regulatory simplification and lays the groundwork for further harmonisation measures, including the proposed single-entry point for incident reporting under the Digital Omnibus package. By aligning reporting requirements across the EU, the initiative aims to create a more streamlined and user-friendly reporting framework while supporting organisations in meeting their cybersecurity obligations and strengthening their overall cyber resilience.

FRANCE

CNIL recommendations on AI System development

In France, the CNIL started the year publishing its recommendations on AI system development and compliance with the GDPR. The recommendations which are clearly scoped to capture the development phase of an AI system (and not the deployment phase) include a checklist for designers and developers of AI systems, including an 11 step plan for compliance, defining a legal basis for processing (step 3), adapting safeguards to data scraping (step 4) and ensuring the exercise of data subject rights (step 5). The recommendations cover systems based on machine learning, systems whose operation use is defined from the development phase and general-purpose AI that can be used for various applications and systems for which the learning is done either 'once and for all' or continuously.

The CNIL published its 2025 sanctions and corrective measures findings. In total, there were 259 decisions, 83 sanctions, 143 compliance orders, 31 reminders of legal obligations and 2 warnings and €486,839,500 in cumulative fines. Cookies, employee monitoring and (inadequate) data security were the main subjects of sanctions imposed by the CNIL in 2025.

CNIL recommendation on email tracking pixels

The CNIL adopted a recommendation on 12 March 2026 clarifying the rules applicable to the use of tracking pixels in emails. The guidance confirms that email tracking pixels are subject to the consent requirements under Article 82 of the French Data Protection Act (which implements Article 5(3) of the ePrivacy Directive). Tracking pixels generally require consent where they are used to measure email open rates, optimise marketing campaigns, personalise communications, create user profiles, support advertising activities or detect fraud.

CNIL's work programme for 2026

In 2026, the CNIL is strengthening its transparency approach by presenting details of the resources it plans to submit to public consultation or publish, to allow stakeholders to prepare for future consultations and to anticipate developments. The CNIL's areas of focus as incorporated into its work programme covers AI in the workplace and healthcare sector (including the updating of health research standards), cybersecurity and tools for Data Protection Officers.

CNIL: processor data breach case study

The CNIL published a case study highlighting the challenges organisations face when a processor suffers a cyberattack that affects both its own data and customer data. The scenario describes a cloud service provider whose systems are compromised following a social engineering attack, resulting in unauthorised access to both internal company data and customer environments.

The CNIL reiterates that processors must notify affected controllers without undue delay and support them in meeting their GDPR obligations, while also managing any reporting obligations arising from their own role as controller. Where a personal data breach presents a risk to individuals, it must be notified to the supervisory authority within 72 hours, and affected individuals must be informed where the risk is high. The CNIL also stresses the value of having pre-established breach response procedures, customer support mechanisms and communication templates in place to facilitate timely notifications and ensure an effective response during a cyber incident.

GERMANY

The State Commissioner for Data Protection of Lower Saxony recorded a drastic increase in data protection complaints in 2025. A total of 4,022 complaints were received last year. This represents an increase of 70% compared with 2024's 2,361 complaints. The sharp increase could be due to the increased interest of citizens in data protection. However, AI chatbots that are now integrated into search engines often point out the possibility of sending a complaint to the responsible data protection authority when it comes to questions about data protection and also provide suggestions for cover letters. This is indicated by the texts of some complaints, which contain remnants of communication with AI chatbots.

Germany Launches ReguLab Data Protection Sandbox

Germany's Federal Commissioner for Data Protection and Freedom of Information (BfDI) has launched ReguLab, a new regulatory sandbox designed to support organisations developing innovative, data-driven solutions. The initiative enables participants to engage directly with the regulator to explore data protection requirements and obtain practical compliance guidance before bringing new technologies to market.

The programme aims to reduce legal uncertainty by allowing the BfDI and participating organisations to jointly assess specific use cases and identify how data protection laws can be applied in practice.

The initial focus areas include healthcare digitalisation, public sector digital infrastructure and digital identity solutions, including projects related to the EU Digital Identity Wallet.

ReguLab operates as a standalone data protection advisory initiative and is separate from the AI regulatory sandboxes and real-world testing environments contemplated under the EU AI Act.

Frankfurt high court decision on third party cookie liability

The court confirmed that liability for unlawfully deployed cookies is not limited to website operators. Third-party analytics, advertising and tracking providers that contribute to, facilitate or technically enable the placement of cookies without valid consent may also be held responsible, notwithstanding contractual arrangements that place responsibility for obtaining consent on the website operator.

MIDDLE EAST

New Federal Decree-Law No. 26/2025 on Child Digital Safety in the United Arab Emirates

Effective from **1 January 2026**, the UAE's new **Child Digital Safety Law (Federal Decree Law No. 26/2025)** introduces a comprehensive framework aimed at protecting children from harmful online content and digital practices that may negatively affect their physical, psychological or moral wellbeing. The legislation places significant new obligations on digital platforms, including restrictions on the collection, processing and sharing of personal data relating to children under the age of 13, except in limited circumstances. Platforms must also implement child-safe privacy settings by default and deploy effective age-verification measures.

The law further requires online service providers to take proactive steps to create a safer digital environment for children. This includes preventing children's access to gambling-related games and betting activities, implementing content-filtering tools, and adopting measures to minimise exposure to harmful or inappropriate content. The legislation applies broadly to a wide range of online services, including websites, social media platforms, messaging services, online gaming platforms, streaming services, search engines, mobile applications and e-commerce platforms. Notably, the law has extraterritorial effect, applying to platforms operating in or targeting users within the UAE.

In addition to imposing obligations on businesses, the legislation introduces specific responsibilities for parents and other caregivers, who are expected to supervise children's online

activities, utilise parental control tools and avoid creating accounts on platforms that are not age-appropriate. To support implementation, the law establishes a new **Child Digital Safety Council**, chaired by the Minister of Family, which will coordinate national digital safety initiatives and strengthen collaboration between government bodies and the private sector to promote a consistent approach to protecting children online.

Oman's Personal Data Protection Law Executive Regulations enter into force

On 5 February 2026, the extended one-year grace period for the Executive Regulations (Ministerial Decision 34/2024) issued under the Oman Personal Data Protection Law (Royal Decree No. 6/2022) (together, the "Oman Data Protection Laws") came to an end. The Oman Data Protection Laws are now fully in force, and Oman's Ministry of Transport, Communications and Information Technology is now exercising its full supervisory and enforcement mandate as Oman's data protection regulator.

The Oman Data Protection Laws establish a framework governing the collection, use, disclosure, storage and transfer of personal data in or from Oman, including obligations on controllers and processors, specific restrictions on the processing of sensitive personal data, rules on cross-border transfers and enhanced data subject rights. With the transition period now concluded, entities operating in Oman should promptly, if they have not already done so, familiarise themselves with these requirements and undertake any necessary updates to their policies, procedures, contracts and technical measures to ensure compliance.

Regional adequacy: mutual recognition between the ADGM, DIFC and QFC

In January 2026, the Abu Dhabi Global Market ("ADGM"), Dubai International Financial Centre ("DIFC"), and Qatar Financial Centre ("QFC") each adopted mutual, reciprocal data protection adequacy decisions, adding one another to their respective adequacy lists. Each regulator has therefore recognised the others' data protection regimes as providing an essentially equivalent level of protection for personal data.

Practically, this enables entities established in any of the DIFC, ADGM or QFC to transfer personal data to entities in the other two jurisdictions without implementing additional transfer safeguards such as binding corporate rules or standard contractual clauses. This should streamline cross border data flows within the three financial centres and reduce the contractual and operational burden of regional compliance.

UAE: New Federal Authority for Data and AI

On 14 June 2026, the United Arab Emirates announced the establishment of the **Artificial Intelligence and Data Authority**, a new federal body responsible for overseeing artificial intelligence, data governance and digital government initiatives under a single national framework. Reporting directly to the Cabinet and chaired by UAE Minister of State for Artificial Intelligence Omar Sultan Al

Olama, the Authority is intended to consolidate the UAE's digital governance capabilities and support the country's next phase of AI-driven transformation.

The Authority will assume functions previously carried out by several government bodies, including the UAE Data Office and the Digital Government Sector, and will be responsible for developing national AI strategy, proposing legislation and policies, and strengthening the management and sharing of government data. The announcement reflects the UAE's continued ambition to position itself as a global leader in AI and the digital economy and may signal further regulatory and governance developments in the AI and data space in the coming years.

Related Capabilities

- Data Privacy & Security
- General Data Protection Regulation
- Data Privacy, Telecommunications & Collections

Meet The Team

Geraldine Scali

Partner and EMEA Lead of Data Privacy and Security, London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483

Dominik Weiss

Partner, Hamburg

dominik.weiss@bclplaw.com
+49 (0) 40 30 33 16 148

Pierre-Emmanuel Frogé

Counsel, Paris

pierreemmanuel.froge@bclplaw.com

+33 (0) 1 44 17 76 21

Michael Geier

Counsel, Frankfurt / Hamburg

michael.geier@bclplaw.com
+49 (0) 69 970 861 288
