BCLP. Client Intelligent

Insights

EMEA - DATA PRIVACY, DIGITAL AND AI ROUND UP

Jul 25, 2025

SUMMARY

As we pass the mid-point of 2025, it's a good time to review the important developments we have seen in the first 6 months of this year, particularly reforms to the UK's data protection laws, the EU's pathway to implementation of its AI Act, the CNIL's recent regulatory focus (AI, transfer impact assessments and connected vehicles) and the approach in the Middle East to tech innovation, particularly AI.

HIGHLIGHTS

We've seen the UK finally pass its long-awaited data protection legislation, the Data (Use and Access) Act, relaxing some rules on automated decision-making, whilst side-stepping the question of data scraping. The EU has produced guidelines on general-purpose AI models and published a voluntary code of practice for AI model developers. The CNIL's 2025-2028 strategic plan identifies AI, protection of minors and cybersecurity and resilience as key focus areas and it has also published two recommendations to support responsible AI innovation, as well as updated guidance on web scraping for AI development. Saudi Arabia has published for consultation a draft Global AI Hub Law that sets out a framework for establishing sovereign data centres under foreign jurisdiction and its AI regulator has issued ethical guidelines on development and use of deepfakes technology. The UK is yet to legislate specifically on the topic of AI, relying on a range of sectoral guidance issued by regulators, with the ICO and CMA issuing a paper on AI foundation models.

From an advertising perspective, the ICO has provided guidance on those organisations offering a 'consent or pay' model, which must also be seen in light of fines issued this year to large tech companies by the European Commission under the EU Digital Markets Act (DMA), with the investigations under the DMA identifying issues with the 'consent or pay' model, when used by the larger tech platforms.

STILL TO COME IN 2025

The EU has extended the UK's adequacy decision whilst it considers the substance of the UK's data reforms, so we will be watching for developments on that score. The ICO now has tougher enforcement powers under the Privacy and Electronic Communications Regulations, and can now issue higher fines for non-compliance with cookie rules, as a result of the Data (Use and Access) Act. We therefore anticipate increased enforcement activity on this front in the UK, with the ICO due to provide updated direct marketing and privacy and electronic communications guidance in winter 2025/Q1 2026, and updated guidance on the use of storage and access technologies.

Read on for a more in-depth review of the developments in 2025 to date.

UK

DATA USE AND ACCESS ACT 2025

After a tumultuous passage between the two chambers of the UK's Parliament, the Government has now passed the Data (Use and Access) Bill turning this into the Data Use and Access Act 2025.

A reminder – what are some of the key changes as a result of the Act?

- A wider category of legitimate interests recognised as a basis for the processing of personal data, with the Bill introducing a new right for the Secretary of State to amend the conditions for which processing of personal data for a legitimate interest may take place. The current balancing test which has to be performed (weighing legitimate interests against individual rights before organisations can disclose personal data) has been removed;
- The relaxation of some of the rules around automated decision-making, clarifying that a decision will be solely based on automated processing if there is 'no meaningful human involvement' in the decision-making process. However, the use of automated decision-making is still subject to conditions where it relies on special category personal data and is a 'significant' decision;
- Changes to the process for responding to DSARs, to permit extensions to the deadline for requests where an access request is complex as well as limiting information to be provided in response to a data subject access request to that which can be found through a 'reasonable and proportionate' search; and
- Changes to the rules around cookies which will require greater transparency when cookies are deployed, and, subject to various conditions, cookies for user security, analytics and user improvement purposes can be deployed without consent.

ICO GUIDANCE ON "CONSENT OR PAY"

Following the Information Commissioner's Office (**ICO**) call for views on "consent or pay" models in March 2024, the ICO published guidance to provide clarity and advice to organisations currently operating or considering a "consent or pay" model in the UK.

The guidance broadly sets out four factors that are important to consider when assessing whether an organisation's "consent or pay" model meets the standard of "freely given" consent under the UK GDPR which are: (i) power imbalance; (ii) appropriate fee; (iii) equivalence; and (iv) privacy by design.

The factors explore whether or not there is a clear power imbalance between the organisation and users, ensuring the fee for avoiding personalised advertising is reasonable, offering an equivalent core service whether users consent or pay to avoid personalised data, and presenting choices clearly and ensuring users are fully informed.

Organisations must document assessment of their "consent or pay" model as part of their data protection impact assessment under Article 35 of the UK GDPR.

CYBER GOVERNANCE CODE OF PRACTICE

The UK Government published its response to the call for views on a Cyber Governance Code of Practice, which took place from January to March 2024. The code has been designed to complement the National Cyber Security Centre's Cyber Security Toolkit for Boards, where the code sets out what directors should be doing to govern cyber risk within their organisation and the Toolkit provides further detail on how directors should undertake the activities outlined in the code and why. The responses given are in line with the five key themes identified:

1. design of the code;
2. the viability of an assurance scheme;
3. scope of the code and its implications on uptake;
4. clarity on the code's interplay with other standards, guidance and other resources; and
5. interest in government working with a wide range of stakeholders to promote uptake of the code.

The code was published in April 2025 and sets out the most critical governance actions for boards covering risk management, strategy, people, incident planning, response and recovery, assurance and oversight.

ICO'S DIRECT MARKETING ADVICE GENERATOR

The ICO launched a free online digital marketing advice generator to help small organisations ensure their direct marketing activities comply with the Privacy and Electronic Communication

Regulations and the UK GDPR. The tool is able to provide tailored advice depending on the direct marketing channel in question (email, SMS, postal, social media and telemarketing) and is designed with small organisations chiefly in mind who may have less time and resources to get reliable and tailored compliance advice. In 2024, the ICO also launched a privacy notice generator that can create tailored privacy notices relevant to small organisations operating in various sectors.

ICO AND CMA JOINT GUIDANCE ON AI FOUNDATION MODELS

The ICO and Competition Markets Authority (**CMA**) jointly published an article clarifying their shared positions on open and closed-access foundation model (**FM**) approaches. FMs are base models for AI systems that are trained on large amounts of data and can be released through an open-access or closed-access release approach. The ICO and CMA confirmed that they do not favour any specific release approach as long as developers and deployers comply with all regulatory requirements and put in place appropriate risk mitigations and safeguards to support effective data protection compliance and protection for consumers.

The article also provides examples of appropriate mitigations. Developers releasing open-access FM trained on personal data should consider using licences or terms of use to ensure that deployers downstream are using their models in a compliant way. Developers releasing closed-access FMs can rely on technical controls such as APIs to help monitor and control against data misuse downstream. Transparency about how a FM model is developed for both models is necessary to support deployers to make informed decisions about personal data processing and help them verify their accountability for their own data protection and consumer protection compliance.

The ICO and CMA welcome further engagement with stakeholders on their experiences of FMs and AI in general. They are also committed to working together to enhance regulatory coherence where their regulatory regimes interact, such as on the topic of FMs, focusing on promoting user choice and control, creating a level playing field for data access, and allocating accountability across the supply chain.

ICO ANNOUNCED INVESTIGATION INTO THE USE OF UK CHILDREN'S PERSONAL INFORMATION ON SOCIAL MEDIA AND VIDEO SHARING PLATFORMS

As part of the ICO's efforts to ensure companies are designing digital services that protect children, it announced investigations into how TikTok, Reddit, and Imgur protect the privacy of their child users in the UK. The ICO is investigating whether the social media and video sharing platforms infringe data protection legislation in the way they make recommendations to children and deliver suggested content to their feeds and their usage of children's personal information and of age assurance measures. The ICO has driven significant change in the way companies approach children's online privacy since the ICO's Children's code came into force in 2021. It will also work

closely with Ofcom, which is responsible for enforcing the Online Safety Act, to ensure that their efforts are coordinated.

REVIEW INTO USE OF CHILDREN'S DATA BY FINANCIAL SERVICES

The Information Commissioner's Office (ICO) carried out a review into the gathering of children's data from services supplying them with current accounts, savings accounts, trust accounts, ISAs and prepaid cards. The review focussed on: governance; transparency; use of information; individual rights; age verification; further contact and marketing.

In relation to governance, nearly all organisations provided data protection training to staff (97%) however, less than a fifth (18%) included specific training about the use of children's information.

Notably and in relation to transparency, several organisations passed their transparency obligations onto parents highlighting the risk potential of children signing up to terms and conditions that they do not understand.

The findings of the review are as of a result of a information gathering process from March-September 2024 and was done using a mix of questionnaires and direct engagement which provided the views of over 40 organisations (participants).

STATEMENT FROM THE ICO ON DATA PROTECTION COMPLAINT RESPONSE TIMES

The ICO published a statement admitting its current responses times are not where they would like them to be and confirmed its commitment to meeting its target of responding to 80% of complaints within 90 days. Several initiatives over the coming months are said to be introduced to help the ICO achieve this including the recruiting of additional staff.

ICO CONSULTATION ON DRAFT UPDATED ENCRYPTION GUIDANCE

The ICO on the 24 June 2025 closed its 6 week consultation on its draft updated guidance on encryption. The survey that forms part of the consultation is split into four sections and asks for views on the ICO's approach to encryption and data protection law along with any questions surrounding the encryption scenarios included in the guidance.

UK ANNOUNCES CYBER GROWTH ACTION PLAN

The Cyber Security Growth Action Plan aims to turbocharge growth in the UK's cyber sector and unlock more jobs, support innovation, and drive forward delivery of the government's Plan for Change.

The Growth Action Plan is envisaged to have four specific workstreams:

- Sectoral analysis: to assist with understanding the demand for cyber products and services and identifying the UK Cyber Sector's core strengths;
- Strategy Alignment: identifying opportunities presented by forthcoming legislation, including the Cyber Security and Resilience Bill, and policy impacts on innovation;
- Future Technologies and Societal Trends: identifying the future trends and the impact they might have on growth opportunities;
- Building on Strengths: identifying ways to better coordinate communities and capabilities across government, industry and academia to create future oriented growth.

The UK Cyber Security Growth Action Plan will publish a series of key insights for the Secretary of State to drive the growth of the UK cyber sector and encourage wider adoption across the UK economy.

ICO INTERNET OF THINGS GUIDANCE

The guidance is aimed at those in compliance roles (data protection officers, general counsel, risk managers a senior management) and covers consumer IoT products e.g. home entertainment products, domestic appliances, wellbeing products etc. The guidance specifically excludes connected and autonomous vehicles, smart meters, smart cities and the use of IoT products in enterprise and industrial settings.

EU COMMISSION RELEASES FAQS ON AI LITERACY

On 12 May the EU Commission published detailed FAQs on AI literacy (Article 4 EU AI Act), providing its interpretation of the provisions for the first time.

EU

EDPB STATEMENT ON AGE ASSURANCE:

The European Data Protection Board (**EDPB**) published a statement on age assurance. The statement focuses on the data protection principles (lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, confidentiality, integrity and accountability) applicable to different online use cases, including when a minimum age is prescribed by law or otherwise for buying products, for using services that may harm children or for performing legal acts; and when there is a duty of care to protect children (for example, to ensure that services are designed or offered in an age appropriate way).

The statement also explores automated decision making, data protection by design and default and accountability obligations noting that service providers and any third party involved should implement governance methods that allow them to be accountable for their approach to age assurance and for demonstrating their compliance with data protection regulation and other legal requirements and service providers should adopt a risk-based approach when designing and operating their services.

EDPB GUIDELINES ON PSEUDONYMISATION

On 16 January 2025, the EDPB adopted guidelines on Pseudonymisation. The guidelines clarify that pseudonymisation, as defined under the GDPR, is a security and privacy-enhancing technique that reduces the risk of identifying individuals by separating identifying data from other information. It is not the same as anonymisation, as re-identification remains possible under certain conditions. Pseudonymisation supports compliance with GDPR principles such as data minimisation, data protection by design and by default, and can help justify processing under legitimate interests or for further compatible processing. However, it is not a standalone safeguard and must be part of a broader data protection strategy.

DATA TRANSFER – EDPB PUBLISHED GUIDELINES ON ARTICLE 48 GDPR

Article 48 GDPR states that decisions by courts or authorities in non-EU countries requiring access to personal data from the EU are only valid if based on an international agreement, such as a mutual legal assistance treaty. The guidelines clarify that such foreign decisions cannot be automatically enforced in the EU, reinforcing the principle of EU legal sovereignty. Any transfer of personal data in response to such requests must still comply with GDPR requirements, including a valid legal basis under Article 6 and appropriate safeguards under Chapter V. The EDPB provides practical recommendations to help controllers and processors handle these requests lawfully.

GENERAL-PURPOSE AI CODE OF PRACTICE PUBLISHED BY THE EC

The European Commission published the General-Purpose AI Code of Practice. The Code consists of three chapters, covering transparency, copyright and safety and security.

This is a voluntary guidance tool, to supplement understanding of the obligations laid out in the EU's AI Act, to ensure that GPAI models placed on the EU market are safe and transparent, (including the most powerful ones) and setting out methods for those providers of GPAI models / GPAI models with systemic risk to demonstrate compliance with the AI Act’s relevant obligations.

Serving as a starting point for EU AI Act compliance, following publication, the EU Commission will assess the adequacy of the Code and then supplement with its guidelines on GPAI models, which will be published before the rules applicable to providers of GPAI models come into force. These guidelines will clarify: (i) what is a GPAI model; (ii) which GPAI models are models which pose a systemic risk; and (iii) who is a ‘provider’ of a GPAI model.

FRANCE

CNIL'S 2025-2028 STRATEGIC PLAN

The National Commission on Informatics and Liberty (**CNIL**) published in January 2025 its strategic plan for 2025-2028, highlighting its priorities for the coming years. Four key focus areas outlined in the plan are: (i) artificial intelligence; (ii) protection of minors; (iii) cybersecurity and resilience; and (iv) apps and online identity in everyday digital life. The plan also sets out CNIL's commitments and actions, including providing guidance to clarify rules and regulation on AI, strengthening requirements for online platforms to ensure age-appropriate protections, investigating and enforcing sanctions to reinforce compliance with data breach notification requirements under the EU GDPR, and monitoring the compliance of apps with applicable rules.

DATA TRANSFER IMPACT ASSESSMENT

The CNIL released the final version of its guide on Transfer Impact Assessments (**TIA**), providing organisations with guidance on ensuring equivalent levels of protection for data transferred outside the EEA. Generally, data exporters subject to the GDPR must carry out a TIA with the assistance of the importer before transferring data to a third country where that transfer is based on a tool in Article 46 of the GDPR (e.g., standard contractual clauses, binding corporate rules). The guide provides a methodology identifying the steps prior to carrying out a TIA and guidance on how the analysis can be carried out following the steps set out in the European Data Protection Board (**EDPB**) on additional measures complementing transfer instruments.

The methodology the CNIL's guide uses covers the following six different steps that should be followed in order:

In relation to the implementation of the TIA, this guide is organised according to the six different steps to be followed in order to carry out a TIA:

1. Know your transfer
2. Identify the transfer tool used
3. Evaluate the legislation and practices of the country of destination of the data and the effectiveness of the transfer tool
4. Identify and adopt supplementary measures
5. Implement the supplementary measures and the necessary procedural steps
6. Reassess the level of protection at appropriate intervals and monitor potential developments that could affect it

The use of this guide is not mandatory and other methodologies can be applied.

GDPR CERTIFICATION FOR DATA PROCESSORS

The CNIL launched a public consultation on a draft evaluation scheme for GDPR certification of data processors, which ended on 28 February 2025. The certification will help guide data controllers in choosing processors that adhere to data protection standards. Organisations established in Europe are eligible to apply for the certification, though the certification is better suited to “turnkey” or “off-the-shelf” services offered by processes as the assessment focuses on the operational implementation of the processing. The scheme consists of 90 control points organised according to the chronology of implementing personal data processing carried out on behalf of a data controller. An accredited certification body will conduct its assessment according to the data processing context and draw on CNIL’s recommendations and resources.

BINDING CORPORATE RULES (BCR)

CNIL published a self-assessment tool to support groups wishing to implement BCR to test the maturity level of their BCR projects. The tool can be completed by a Group Data Protection Officer, any other person in charge of the BCR project or by the Group Board. The CNIL recommends that the tool is utilized before an application is made to the CNIL and typically only projects that are considered “mature” by the tool should be submitted to the CNIL.

AI AND GDPR

CNIL published two recommendations to support responsible AI innovation, focusing on the flexible application of the purpose principle, the use of large training datasets, and the retention of training data.

The first concerns informing individuals when personal data is used to train an AI model with the second concerning individual rights.

In relation to the first recommendation, the CNIL makes clear certain requirements in relation to meeting transparency requirements that transparency requirements must still be complied with irrespective of whether personal data is collected directly or indirectly from data subjects and transparency information should be provided at the time of collection (in the case of direct personal data collection) or as soon as possible (in the case of indirect personal data collection).

In relation to the second recommendation, the CNIL notes the practical differences in complying with a rights request where the personal data in question relates to the training data or the model itself, the difficulties in identifying the person concerned ultimately concluding that a case-by-case analysis is necessary to determine what information is reasonable and proportionate to keep in order to ensure the rights of individuals over their data.

CNIL CONNECTED VEHICLES RECOMMENDATIONS

The CNIL published a draft recommendation on the use of location data from connected vehicles. The recommendations aimed at all vehicle stakeholders (car manufacturers, fleet managers, suppliers of telematics tools and data aggregators and integrators) seeks to provide clear recommendations on the most frequent uses of location data. It bolsters the “connected vehicles” compliance pack that was published by the CNIL in 2017 and contains both general and specific recommendations.

General recommendations include identifying the appropriate lawful basis, implementing appropriate security measures (encryption, access logs etc) and ensuring transparency obligations and the ability for data subjects to exercise their rights are met/made available.

Specific recommendations concern the anonymisation of local data and risk associated with telematic boxes and data aggregators.

The recommendations closed for comments on the 20 May 2025.

FRENCH CNIL ISSUES DRAFT GUIDANCE ON THE USE OF LOCATION DATA FROM CONNECTED VEHICLES | INSIDE PRIVACY

Following a public consultation, the CNIL published its recommendations on multi-factor authentication (MFA) in April 2025. The recommendation aim is to provide legal security for users of such solutions and to encourage providers to integrate privacy protection from the design stage of their products or services.

This recommendation is particularly intended to guide data controllers on:

- When the use of MFA is appropriate, based on security needs;
- How to comply with GDPR principles when using MFA, including determining a legal basis, minimizing collected data, setting retention periods, and respecting individuals' rights;
- How to define the roles and responsibilities of the actors involved in an MFA solution;
- How to choose authentication methods (factors of knowledge, possession, inherence) and ensure their compliance with GDPR;
- Key considerations regarding the use of inherence factors (like biometrics), solutions based on sending one-time codes via SMS, and the use of employees’ personal devices as a possession factor.

WEB SCRAPING FOR AI DEVELOPMENT

On 19 June 2025, the French Data Protection Authority (CNIL) published updated guidance clarifying the conditions under which web scraping of publicly accessible data may be used to

develop artificial intelligence systems.

MIDDLE EAST

UNITED ARAB EMIRATES (DIFC)

The Dubai International Financial Centre has completed its consultation on proposed updates to its Data Protection Law (DIFC Law No. 5 of 2020). The proposed amendments are intended to reinforce the DIFC's position as a leading data jurisdiction by aligning its regulatory framework with global benchmarks. Among the key proposals are an expanded scope of application, new obligations for data exporters, and enhanced rights for individuals to bring direct legal claims in the DIFC Courts. The draft amendments also envisage stronger enforcement measures, including increased penalties for non-compliance. Final changes are expected to be confirmed later in the year.

SAUDI ARABIA

On April 14, 2025, in a regional first, Saudi Arabia's Communications, Space and Technology Commission (CST) published for consultation a draft Global AI Hub Law that sets out a framework for establishing sovereign data centres under foreign jurisdiction - so-called "data embassies." The law categorises different types of AI and data hubs and is intended to facilitate bilateral cooperation while supporting the Kingdom's ambitions to be a global technology hub. The public consultation remains open until 14 May 2025.

On April 14, 2025, in a regional first, Saudi Arabia's Communications, Space and Technology Commission (CST) published for consultation a draft Global AI Hub Law that sets out a framework for establishing sovereign data centres under foreign jurisdiction - so-called "data embassies." The law categorises different types of AI and data hubs and is intended to facilitate bilateral cooperation while supporting the Kingdom's ambitions to be a global technology hub. The public consultation remains open until 14 May 2025.

SAUDI DATA AND ARTIFICIAL INTELLIGENCE AUTHORITY (SDAIA)

Saudi Arabia's data and AI regulator has issued ethical guidelines titled *Deepfakes Guidelines Version 1.0* on the development and use of deepfake technologies. These aim to mitigate the risks of misuse, particularly in the context of fraud and impersonation and set out principles for responsible deployment by developers and content creators alike. The Guidelines emphasise the importance of adhering to ethical principles, including privacy, transparency, accountability and social responsibility.

Together, these initiatives reflect a broader trend in the region toward regulatory innovation and cross-border alignment in the areas of data governance and AI.

RELATED CAPABILITIES

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

MEET THE TEAM

Geraldine Scali

London

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

Dominik Weiss

Hamburg

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

Oliver Hallsworth

Abu Dhabi

oliver.hallsworth@bclplaw.com
+971 2 652 0331

Pierre-Emmanuel Froge

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21
