BCLP. Client Intelligent

Insights

EMEA- DATA PRIVACY, DIGITAL AND AI ROUND UP 2024/2025

PRIVACY SPEAKS

Jan 14, 2025

SUMMARY

As expected in the data privacy and digital space, 2024 shaped up to be a year full of guidance, consultations, regulatory focus areas and legislative updates. Artificial Intelligence (**AI**) remained a hot topic with advertising technology (**AdTech**) closely following its heels. With the blizzard of global data protection developments continuing unabated in 2024 with no doubt more to come in 2025, it is a good moment to look back at what 2024 held for businesses as well as to consider what 2025 may hold in the EMEA region.

KEY DATA PROTECTION DEVELOPMENTS IN 2024

In this round-up, we look back over 2024 and consider the main developments across themes including artificial intelligence, data privacy, cybersecurity and cookies in the UK, EU and the Middle East.

UK

ARTIFICIAL INTELLIGENCE

The start of 2024 began with the Information Commissioner's Office (**ICO**) launching a consultation series on generative AI. The purpose of the series was to assess how data protection law should apply to the development and use of technology. The response to the series was published in December with the ICO retaining its position on topics such as purpose limitation, accuracy and controllership and updating its position data subject rights and where legitimate interest is used for data scraping activities.

A few months later the ICO published its strategic approach on regulating AI, which is broken down into 5 parts covering topics such as the opportunities and risk of AI, the role of data protection law, upcoming developments and the importance of working together. On the last point, the ICO makes clear that an integral part of its strategic approach involves working together with other regulators, governments, standard bodies and international partners. In November, the ICO published an outcomes report on AI tools in recruitment. The report follows consensual audit engagements carried out by the ICO with developers and providers of AI tools to be used in recruitment between August 2023 and May 2024. We have covered this in more detail.

ADTECH AND COOKIES

AdTech has long been an area in which the ICO has paid particular attention to, however in 2024 the ICO made clear that AdTech, and specifically cookies, is a key focus area. At the start of the year, the ICO published an update on its progress in making advertising cookies compliant. This follows on from the work started in 2023 where 53 of the UK's top 100 websites were contacted by the ICO about their advertising cookie compliance.

The statement noted that at the time of writing, a number of companies had positively responded to its call to action but warned that they are committed to writing to more companies to warn of potential enforcement action if the right steps are not taken. Whilst this was published at the beginning of the year, cookie compliance clearly remained an area of focus for the ICO who issued a reprimand in September to an organisation for non-compliant advertising cookie practices.

The ICO launched a call for views and updates on "consent or pay" mechanisms, and in this welcomed feedback on factors such as the power balance between the service provider and its users, equivalence, appropriate fee and privacy by design. We await the ICO's response following the call for views which ended in April but anticipate that this will hopefully be published in the coming months.

DATA (USE AND ACCESS) BILL

The UK's Data (Use and Access) Bill (**DUAB**) will amend certain aspects of the UK GDPR with noteworthy updates expected in relation to cookie compliance, the role of the ICO, legitimate interests and solely automated decision making to name a few. The DUAB is currently making its way through Parliament and is expected to enter report stage later this month. We have covered the DUAB's key updates in more detail.

EMPLOYEE DATA PROTECTION

The ICO continued work started in previous years and remained focussed on data protection in employment. In 2024, it published guidance on information sharing in mental health emergencies and concluded its consultation on draft employment practices including keeping employment

records, recruitment and selection. We can expect the publication of this guidance to follow this year.

FINING GUIDANCE AND AUDIT FRAMEWORKS

The ICO's new fining guidance was published which provided greater transparency about how the ICO uses its powers by setting out the criteria used for issuing penalties and the methodology behind calculating fines.

Another key development was the publishing of the ICO's data protection audit framework. The purpose of this framework is to help organisations of varying sizes assess their compliance with data protection law in order to encourage an improvement of data protection practices. The framework contains nine toolkits covering key areas such as records management, data sharing and information and cyber security and is intended to be a useful starting point when auditing and assessing privacy compliance.

NATIONAL AND INTERNATIONAL COLLABORATION AND CO-OPERATION

The ICO's intention of working together with other bodies was not confined to its strategic approach to regulating AI and in 2024, we have seen more collaboration from the ICO both nationally and internationally:

- The Office of Communications (**Ofcom**) and the ICO issued a joint statement in May addressing the overlap with some of the Online Safety Act's provisions with UK data protection rules and indicated how they intend to collaborate, including by exchanging information to effectively tackle issues of common interest in a coordinated manner.
- The ICO, Financial Conduct Authority and The Pensions Regulator all issued a joint statement for retail investment firms and pension providers in November. The idea behind this statement is to provide greater clarity for those in these sectors to help ensure that their regulatory communication messages comply with data protection requirements.
- In September, the ICO and National Crime Agency (**NCA**) signed an memorandum of understanding (**MOU**). The purpose of this MOU is to outline how the two organisations will collaborate to improve the UK's cyber resilience. The ICO restated their commitment to providing relevant information and guidance on how to improve cyber security and to work more closely with the NCA to ensure companies are given the tools required to report cybercrime.
- On the international front, the ICO announced that it was working with the Office of the Privacy Commissioner of Canada (**OPC**) on an investigation into the data breach in October 2023 of a global genetic testing company. This joint investigation shows the regulators' commitment to

pooling resources and expertise in order to protect individuals' right to privacy across different jurisdictions.

EU

ARTIFICIAL INTELLIGENCE

The EU's AI Act entered into force in August 2024, although most provisions will not apply until August 2026. Measures relating to higher risk AI systems and the provisions on AI literacy apply much sooner (with the AI literacy provisions applying from February 2025). The EU AI Act is the first comprehensive regulation on AI adopted in the world and it aims to provide a legal framework fostering innovation and protecting consumers. The new rules establish obligations for providers and developers depending on the level of risk from artificial intelligence. Like the EU GDPR, the EU AI Act could become a global standard because it applies to any AI system developed or used in the EU.

On the guidance front, at the end of the year, the European Data Protection Board (**EDPB**) published its anticipated opinion on AI models. The opinion comes as a response to the Irish supervisory authority's (**Irish SA**) request. The Irish SA's request made to the EDPB was prompted due to the current lack of harmonisation amongst supervisory authorities when it comes to assessing AI models and addresses key components of an AI system such as training, updating, developing and the operation of AI models where personal data is part of the dataset. We have covered the opinion in more detail.

CYBERSECURITY

The Cyber Resilience Act (**CRA**) entered into force in December 2024 and will apply in full in December 2027. The CRA aims to protect consumers and businesses buying software or hardware products with a digital component and introduces mandatory cybersecurity requirements for manufacturers and retailers, governing the design, development, and maintenance of such products. The CRA also requires manufacturers to provide assistance during the lifecycle of their products. Some critical products of particular relevance for cybersecurity will also need to undergo a third-party assessment by an authorised body before they are sold in the EU market. We have commented on the CRA in more depth in our blog post.

The **Network and Information Systems Directive** (**NIS 2**), while not yet transposed by all EU Member States, has effect from 18 October 2024. NIS 2 widens the scope of entities within the regulatory remit of NIS 1 and imposes more governance and cybersecurity risk management obligations, increased incident reporting obligations as well as personal liability for directors for failure to comply with NIS 2 requirements. Read our briefing on the key measures.

INTERNATIONAL DATA TRANSFERS

In July 2023, the adequacy decision for the EU-US Data Privacy Framework (**DPF**) was adopted by the European Commission. In November 2024, the EDPB adopted a report on the first review of EU-US DPF. The report covers the commercial aspects of the EU-US DPF such as the self-certification process and complaint-handling. It also covers the access and use of personal data transferred under the decision by US public authorities, focussing on the implementation of safeguards such as necessity and proportionality and the new redress mechanism.

DATA ACT

The Regulation on harmonised rules on fair access to and use of data, also known as the **EU Data Act**, entered into force on 11 January 2024 and will be applicable from September 2025. Designed to improve access to data, consumers and businesses will have greater access to data generated from use of tech-enabled products or services, as part of efforts to unlock the value of data in the Internet of Things era.

FRANCE

ARTIFICIAL INTELLIGENCE

The National Commission on Informatics and Liberty (**CNIL**) published in April 2024 its first recommendations on the development of AI systems, with our overview of the recommendations found. The recommendations are intended to reconcile and address innovation whilst embedding privacy by design into the development of AI systems and aimed principally at designers and developers. The recommendations include a step by step guide with each step of the design process mapped against the relevant EU GDPR obligation.

MOBILE APPS

The CNIL published its recommendations to help design mobile applications that respect privacy in September 2024. The CNIL's recommendations are aimed at operators developing and making available mobile applications such as mobile application publishers, mobile application developers, software development kit (**SDK**) providers, operating system providers and application store providers.

The recommendations aim to clarify and frame the role of each stakeholder, improve user information on the use of their data and ensure that consent is informed and not forced, and we have commented on these further.

DIGITAL SERVICES ACT IMPLEMENTATION

Pursuant to the Sécurité et Régulation de l'Espace Numérique (**Loi SREN**) enacted in May 2024, the CNIL will be the competent authority to ensure compliance with certain obligations arising from the EU Digital Services Act which is applicable to online platforms and includes reinforced transparency obligations in relation to targeted advertising, prohibition of profiling based on sensitive data and profiling of minors. In this context, the CNIL has been given new means of control such as the power to seize any document under the supervision of the judge, and the possibility of recording the responses of those interviewed. The CNIL will also be able to adopt corrective measures, including fines.

GERMANY

ARTIFICIAL INTELLIGENCE

The Data Protection Conference (**DSK**), the joint body of the German data protection authorities, published a guidance on "Artificial Intelligence and Data Protection" on 6 May 2024. The guidance is primarily aimed at companies that want to use AI applications for their own business purposes. However, it is indirectly relevant for developers and providers of AI applications also. In this first version, the DSK essentially compiles the typical data protection requirements for processing activities in connection with the use of AI applications, structured in three sections: (1) selecting AI applications, (2) implementing AI applications and (3) using AI applications.

COOKIES

On 20 November 2024, the DSK issued updated guidance for providers of digital services. The guidance covers the recently amended German provision that regulates the use of cookies and other tracking technologies, the design of consent banners, the lawfulness of processing of personal data in connection with digital services as well as the compliance with information obligations and data subject rights.

ASSET DEAL

On 11 September 2024, the DSK adopted a new resolution on the transfer of personal data in asset deals. The DSK provides guidance on the conditions under which personal data may be transferred to the buyer of a company in the context of an asset deal. The resolution primarily deals with the transfer of personal data during the due diligence phase, the transfer of customer, supplier and employee data as well as of special categories of personal data.

MIDDLE EAST

SAUDI ARABIA'S PERSONAL DATA PROTECTION LAW

Saudi Arabia's Personal Data Protection Law (**PDPL**) came into force in September 2024. The PDPL includes principles which are aligned with EU GDPR but also unique provisions tailored to its legal and cultural environment, necessitating region-specific compliance strategies. It mandates stringent data collection, storage and transfer standards.

Organisations that fail to comply risk substantial penalties and legal repercussions. It is designed to underpin the Kingdom's innovation in tech-intensive sectors such as fintech, e-commerce and AI, which all require robust data governance frameworks.

SAUDI ARABIA'S AI ADOPTION FRAMEWORK

The Saudi Data & Artificial Intelligence Authority (**SDAIA**) introduced the AI Adoption Framework in September 2024, a strategic initiative to accelerate the integration of artificial intelligence into Saudi Arabia's public and private sectors. The framework aligns with the Kingdom's Vision 2030 objectives, aiming to position Saudi Arabia as a global leader in AI-driven innovation while fostering sustainable economic growth.

The framework provides a comprehensive roadmap for organisations to adopt and scale AI responsibly. It outlines clear guidelines across three key dimensions: readiness, implementation and governance. The readiness phase focuses on equipping organisations with the infrastructure, talent and data management systems necessary to deploy AI solutions effectively. The implementation phase emphasises developing AI capabilities, piloting use cases and scaling AI across industries like healthcare, energy and smart cities. Governance principles ensure ethical AI use, prioritising transparency, accountability and compliance with Saudi data protection laws.

Key features include:

- a standardised AI maturity assessment model;
- tools for ethical AI evaluation; and
- a collaborative knowledge-sharing platform.

SDAIA also supports organisations with capacity building programs and partnerships to enhance AI literacy and technical expertise. By bridging the gap between AI potential and practical application, the framework enables sectors to enhance productivity, optimise decision-making and deliver transformative services. With this initiative, SDAIA aims to make AI an integral driver of Saudi Arabia's digital economy, reinforcing its position as a hub for AI innovation and excellence in the region.

WHAT TO EXPECT IN 2025?

Following on from the 2024 developments, we comment on our key predictions for this year below.

UK

INCREASED FOCUS ON ADTECH

Looking forward, it appears that the ICO and other regulators will have a renewed focus on data enforcement. We have seen that the ICO has published numerous consultations with a view to publishing updated guidance. In addition, we eagerly await the passing of the UK's **Data (Use and Access) Bill** which, amongst other things, will increase the maximum penalty under the **Privacy and Electronic Communications (EC Directive) Regulations** to align with that for breaches of UK GDPR. Recent trends suggest that cookie compliance will also be a focus in 2025.

EMPLOYEE MONITORING

Earlier last year, the ICO published guidance on the new standards for employee monitoring. Then, in February, the ICO issued enforcement notices against a UK based company and several associated trusts. The ICO found that this company had been unlawfully processing the biometric data of over 2,000 employees as they had failed to show why it is necessary or proportionate to use facial recognition technology and fingerprint scanning for the purpose of monitoring employee attendance. This decision suggests a strengthened commitment by the regulators to ensure that the privacy rights of individuals are protected in the workplace, and we anticipate further enforcement action will be taken in 2025 should companies fail to adhere to the guidelines.

DATA SECURITY AND CYBER RESILIENCE

Last year the National Cyber Security Centre (**NCSC**) concluded that recent AI developments will increase the number of cyber-attacks over 2025 and the more recent warning by the NCSC of an increase in "frequency, sophistication and intensity" of such attacks suggests we can expect to see this being an area of high priority in 2025.

We saw an increase in regulation in the space last year with the introduction of the **NIS 2** and the **EU Cyber Resilience Act**, and the UK's legislative proposals for updated cyber security requirements (in the form of the **Cyber Security and Resilience Bill**) are to be published. Organisations should plan and prepare for the fact that they will need to pay greater attention to protecting against cyber threats, noting that the ICO has already called on organisations to improve their cyber security amid the growing threat of such attacks.

In 2024, the NCSC regularly published advice and guidance on topics including vulnerability management. In its annual review, published in the beginning of December, it recognized the work done to counter the increased cyber threat facing the UK, its commitment to building the UK's cyber resilience, its efforts in developing the UK's cyber ecosystem and its assistance in helping the UK keep pace with evolving technology and associated threats and opportunities. We can expect the NCSC to continue its efforts in these areas in 2025 and beyond.

ARTIFICIAL INTELLIGENCE

In the UK, the new Government suggested that there are plans to move away from the principles based approach, at least in respect of higher risk AI applications, with the King's Speech setting out plans to establish '*appropriate legislation to place requirements on those working to develop the most powerful [AI] models*' and so we are likely to see further regulation in this area. However, it is clear that the government and regulators will also continue to encourage the use of AI.

The UK's DUAB will amend certain aspects of UK GDPR and gives the UK the opportunity to address some AI use cases whilst not directly regulating AI system development or deployment. More specifically, it will widen the types of decisions which can be made on a solely automated basis in certain instances.

EU

ARTIFICIAL INTELLIGENCE

While most of the provisions of the AI Act will not apply until 2 August 2026, the provisions on AI literacy will apply from 2 February 2025, and importantly, this provision is one of the few provisions of the AI Act that applies to *all* AI systems within the scope of the AI Act. The European Commission published a proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence (so-called AI liability directive) on 28 September 2022. The AI liability directive would create a rebuttable presumption of causality to ease the burden of proof for victims to establish damage caused by an AI system. This text is to be adopted this year.

DATA SHARING

The EU's **Data Act**, which will apply in the EU from 12 September 2025, will require companies to open their data sets for sharing with their customers and with third parties and also provide them with access to other data sets (e.g. information from transport operators or public sector data) in an attempt to encourage innovation and competitiveness while protecting rights of users and providers.

DATA SECURITY AND CYBER RESILIENCE – IMPACT OF NEW LEGISLATION

The EU's response to increasing threats to cyber security has been to establish harmonised processes and technological standards to combat cyber-attacks. Its new regulations include both provisions applying to companies whose business could be the target of a cyber threat, as well as provisions binding Member States whose information systems could also be affected by nation state attacks or cybercriminal groups.

INCREASE OF COOPERATION PROCEDURES BETWEEN MEMBER STATES SUPERVISORY AUTHORITIES

Last year saw a number of cooperative decisions leading to substantial fines. For example, a company providing transportation services has been fined 290 million euros as a result of a joint procedure for illegally transferring data to the US. The Lithuanian authority has fined a company operating a platform offering second hand clothing over 2 million Euros for several breaches targeting users of the platform. We can expect an increase of cross borders cases triggering a cooperation between the national supervisory authorities leading to significant fines.

FRANCE

EMPLOYEE MONITORING

In 2023, the CNIL fined a French entity of a global company €32 million for its “excessive” monitoring of employees due to several breaches of the EU GDPR identified such as a failure to comply with data minimisation principles, transparency

and integrity and confidentiality principles. The CNIL also released guidance in November on the use of AI augmented cameras to monitor employees for safety purposes. We therefore anticipate a further focus from the CNIL on how organisations monitor their employees in 2025.

MOBILE APPLICATION INVESTIGATION CAMPAIGN

In connection with the recommendations published last year, from early spring 2025 the CNIL will deploy a specific mobile application investigation campaign to ensure compliance with the applicable rules. The motivator behind the campaign is due to the CNIL’s view that “the mobile environment poses greater risks to data confidentiality and security than the web”.

In the meantime, CNIL will continue to deal with any complaints it receives, carry out any checks it deems necessary and adopt any corrective measures required to effectively protect the privacy of mobile application users.

INCREASE OF THE USE OF THE SIMPLIFIED SANCTION PROCEDURE BY THE CNIL

The simplified sanction procedure is one of the tools available to the CNIL to ensure compliance with the EU GDPR and respond to the many complaints received each year (16,000 in 2023). This simplified procedure, enshrined in law since 2022 at the CNIL's initiative, enables rapid sanctions to be issued for cases that do not present any particular difficulties, unlike “ordinary” sanctions. Simplified sanctions are not public, and the amount of fines that can be imposed cannot exceed 20,000 euros.

EXTENSION OF THE FRENCH DATA ACT SCOPE

enacted in May 2024 has slightly modified the French Data Act in order to widen its scope of application. The French Data Act now considers that the collection of personal data online with a view to match it with data relating to online activity is similar to the monitoring of data subjects' behaviour, as defined under Article 3 of the EU GDPR. As a result, many more data processors located outside of the EU will now fall under the scope of the French Data Act.

GERMANY

DSK FOCUS AREAS

In a press release of 8 January 2025, the chairmanship of the DSK announced that for 2025 it will focus its activities on the topics of anonymisation and pseudonymisation. Other priorities include the interaction between the EU GDPR and the European Digital Acts in practice as well as the standardisation of audit criteria for data protection supervisory authorities.

CONSENT MANAGEMENT

Later on this year, the new German Consent Management Ordinance is to likely enter into force. The Consent Management Ordinance establishes the legal framework for "recognised consent management services" to provide end users with a user-friendly and effective tool to manage their consent. These services are intended to significantly reduce and simplify the consent banners on websites. It should be noted that the use of consent management services by website operators is voluntary.

MIDDLE EAST

REGULATORY ALIGNMENT AND CROSS-BORDER STRATEGY

We see the laws of the Middle East reflecting international data protection frameworks like the EU GDPR, but businesses must be mindful of the nuances of local laws, as well as independent data protection laws that impose stringent compliance obligations in free zones like the Dubai International Finance Centre and the Abu Dhabi Global Market. Businesses operating in Gulf Cooperation Council (**GCC**) states are expected to adopt global standards of data governance, including privacy impact assessments, cross-border data transfer restrictions and adherence to cybersecurity frameworks. Compliance strategies should account for overlapping local and international requirements.

Both the UAE and Saudi Arabia emphasise data sovereignty and businesses must therefore be aware of data localisation requirements in 2025 and beyond, particularly for sensitive or government-related data and ensure infrastructure is aligned to store and process data within national borders. With increasing regional integration, businesses should navigate restrictions on

transferring personal data outside the GCC. Data sharing agreements, standard contractual clauses (SCCs), or adequacy agreements will likely become critical compliance tools.

HORIZON MAPPING PROJECTIONS

1. Convergence of AI and Data Protection Laws: AI frameworks will likely incorporate stricter privacy-preserving AI regulations, particularly for automated decision-making and profiling.
2. Regional Data Frameworks: The GCC may pursue regional adequacy mechanisms to simplify cross-border data flows and align data protection laws among member states.
3. Enhanced Cybersecurity Mandates: With global increases in cyber threats, regulators will likely require businesses to adopt predictive threat analysis tools and continuous compliance monitoring.
4. Blockchain and Emerging Tech Regulations: Data privacy frameworks could expand to address blockchain-based data processing and the rise of Web3 technologies in the GCC.

ARTIFICIAL INTELLIGENCE

Both Saudi Arabia and the UAE are leaders in AI adoption, creating frameworks to regulate its ethical use. Businesses must ensure transparency in AI models, manage biases in datasets and establish accountability in AI decision-making and be aware that the collection and analysis of massive datasets can lead to privacy concerns. Companies must maintain a balance between data utility and compliance with data minimisation and purpose limitation principles. Organisations must embed ethics in AI operations, ensuring compliance with emerging ethical AI principles. This includes developing explainable AI systems and conducting regular audits of AI models.

CONCLUSION

Based on 2024, 2025 is set to be another busy year in the data privacy and digital world. With various developments happening across the EMEA region, 2025 will be another year of organisations grappling with the varying global requirements and obligations some of which have some overlap and naturally some divergences. What is clear is that conversations around artificial intelligence, cybersecurity, AdTech and technology more widely, will continue to be had and we anticipate the developments in this space this year to ramp up significantly.

RELATED PRACTICE AREAS

- Data Privacy & Security
- BCLP Data Breach Hotline
- General Data Protection Regulation

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

Pierre-Emmanuel Froge

Paris

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

Olivia Wint

London

olivia.wint@bclplaw.com
+44 (0) 20 3400 4621
