Ashurst

Data Bytes 49: Your UK and European Data Privacy update for July 2024

7 August 2024

Welcome back to the July edition of Data Bytes. This month's edition includes our summary of the data protection and cyber related reforms trailed in the King's Speech and the ICO's annual report. July was also the month the EU's AI Act finally passed into legislation and we provide a summary of the key obligations and dates of enforcement below.

July also saw the Ashurst data protection and cyber team join forces with our environmental and sustainability colleagues to host a webinar on Green Cyber. What is this? we hear you ask. The phrase, as far as we are aware, was first coined in a review into cyber and economic growth for the Government undertaken by the former Conservative MP for Stevenage Stephen McPartland earlier this year. At Ashurst we have been considering what "green cyber" could mean in practice for organisations. Where organisations acknowledge that they are holding large quantities of data in breach of the data minimisation principle and increasing cyber risk, can their environmental and sustainability colleagues assist them with forming arguments and cost savings, to finally get management buy-in for data deletion projects? Is it possible to quantify cost savings and environmental benefits? For a summary of our webinar, keep scrolling to the Spotlight section.

If you are interested in discussing this further with us, we will be holding a roundtable at our London offices on 23 September. Please contact Constance Jarrett to register your interest.

UK Updates

1. The King's Speech

The UK Labour Government's legislative agenda, announced in the King's Speech on 17 July 2024, represents a new direction for technology regulation in the UK. The agenda includes several bills that will affect data protection, artificial intelligence (AI), and cyber security, as well as other areas of digital innovation.

Digital Information and Smart Data Bill

The King's Speech announced a new Digital Information and Smart Data Bill which would enable new, 'innovative' uses of data to help boost and power the economy and "harness the power of data for economic growth".

It would appear the new government has abandoned the previous approach of amending elements of the UK GDPR but retained the proposals regarding new data governance regimes.

The new Bill contains well received new data governance regimes which provide a framework for: (i) digital verification services (to enable users, including businesses, to "make the most of" digital ID verification checking

and save time and money whilst maintaining the security of online transactions) and (ii) setting up Smart Data schemes which are the secure sharing of a customer's data upon their request, with authorised third-party providers.

This is welcome news. The previous proposed Data Protection and Digital Information Bill had been much criticised for simply tinkering around the edges of the UK GDPR with few benefits.

AI Legislation?

While the King stopped short of naming a specific AI Bill, "*the Labour government will seek to establish the appropriate legislation to place requirements on those working to develop the most powerful artificial intelligence model,*" businesses nonetheless finally have the clarity they were urgently seeking as to whether the UK is going to legislate on AI. The UK's vision for regulating AI had up until this point been driven by the 'pro-innovation' approach with the previous government deciding not to legislate to create a single function to govern the regulation of AI, but rather support existing regulators to develop a sector-focused, principles based approach.

However, there is still a question mark on the how, which could likely take time to clarify and therefore still leave some uncertainty. It is possible that the Government may consult on different approaches to AI regulation before drafting specific legislation.

With the EU's AI Act now in force, any delay from the UK will only further accentuate the growing divergence between UK and EU AI regulations. Further, interestingly, the focus for UK legislation so far appears to be on large language models and general purpose AI, which therefore would make any legislation narrower than the EU AI Act given it focuses predominantly on AI use cases rather than the underlying technology itself. This therefore has the potential to create some contention between the UK and EU laws as they both look to wrangle with the opportunities and risk that general purpose AI presents.

Cybersecurity

The Government plans to update and expand the UK's existing cyber security regulation with a new Cyber Security and Resilience (CSR) Bill. The Bill will strengthen UK cyber defences and ensure that more essential digital services than ever before are protected, for example by expanding the remit of the existing regulation, putting regulators on a stronger footing, and increasing reporting requirements to build a better picture in government of cyber threats. The existing UK regulations (Network and Information Systems (NIS) Regulations 2018) reflect law inherited from the EU and are the UK's only cross-sector cyber security legislation.

The CSR Bill will likely reflect or align with the EU's more comprehensive "NIS 2" Directive, which is due to be implemented across the EU by October 2024 as it will expand the scope of regulations to cover more digital services and supply chains; strengthen enforcement and investigatory powers for regulators; and mandate increased incident reporting to provide better data on cyber threats and improve national cybersecurity resilience. These reforms are crucial to prevent incidents like the recent ransomware attack on London hospitals and ensure that the UK's infrastructure and economy are protected from emerging cyber threats.

2. The ICO's annual report – 2023-24

The ICO published its annual report for the period between 1 April 2023 and 31 March 2024 and useful insights are as follows:

- John Edwards, the Information Commissioner, reported that it has been presented with strategic challenges with regard to deployment of resources and "*has had to make a conscious decision to divide*

our finite resources – to both explore and support the new innovations coming down the track, and to continue providing expert guidance for the organisations we regulate and taking action where necessary for the people we protect";

- the ICO's audit programme focused on new technologies (clearly tracking the ICO's intention to explore and support innovations). A total of 64 audits and follow-up audits were conducted, including a series of audits on the use of AI in the recruitment sector and two audit programmes with police services looking at their use of mobile phone extraction technology;
- 39,721 data protection complaints were received by the ICO in 2023/24 (up from 33,753 in 2022/23); of which 62% led to action imposed and 38% led to informal action;
- the ICO imposed £15,648 million in monetary penalties (which was largely was made up of the £12.7m fine imposed on TikTok).

3. ICO emerging enforcement trends

Whilst the ICO has various enforcement powers at its disposal, it takes a risk-based approach, seeking to be effective and proportionate. Over time, the ICO's approach to enforcement changes and trends have clearly changed; we're seeing a move away from monetary penalty notices and the ICO seem to be favouring the use of reprimands (which are published on its website, a formal expression of its disapproval along with recommendations). The number of reprimands imposed are on the way up; in 2020 there were eight and in 2023, the ICO issued 37. In July itself, we have seen three new reprimands, bringing this year's count to 13:

- The Electoral Commission's recent reprimand followed a data breach affecting 40 million people. ICO investigations found the Electoral Commission to have a lack of appropriate security measures in place; servers were not updated with the latest security updates; insufficient password policies were in place (with many accounts still using passwords identical or similar to the ones originally allocated by the service desk).
- An Essex school also faced scrutiny through its implementation of facial recognition technology without having a data protection impact assessment (DPIA). This is a reminder that the use of facial recognition will be high risk and a DPIA should be conducted to manage risks that may be associated with the processing of sensitive biometric data.
- London Borough of Hackney's recent cyber-attack also attracted an ICO reprimand. The attack was widespread and was hackers had access to and encrypted 440,000 files including special category data, affecting at least 280,000 council residents and others including staff. Investigation found examples of a lack of proper security and processes, failure to ensure that a security patch management system was actively applied to all devices and again, failures connected to insecure passwords, this time for a dormant account connected to Hackney council servers which was exploited by the attackers.

4. ICO's response to the Ofcom consultation on the protection of children

On 19 July 2024, the ICO published a response to Ofcom's consultation on protecting children from harms online. The ICO stressed that implementing a type of age assurance method will not guarantee that processing of personal data will be compliant with data protection law. Ofcom previously mentioned that there is currently limited independent evidence about the capability of existing age assurance methods to distinguish between children's age groups but the ICO stressed that this position should not discourage organisations to take age assurance steps to comply with their responsibilities.

With regards to age assurance and proactive technology, the ICO would like Ofcom to clarify to readers that where proactive technology forms part of a service's age assurance function, it is not making a recommendation for the use of proactive technology where content is communicated privately. The ICO echoed Ofcom's sentiment

and acknowledged that setting performance targets can lead to a focus on speed rather than accuracy and interfere with users' right to privacy. Other topics that the ICO commented on included responding to age assurance complaints, signposting child users to support, provision of crisis prevention information and providing children with the option to accept or decline an invite to a group chat.

5. ICO responds to Google's cookies statement

The ICO has expressed its disappointment in response to Google's recent announcement that it will no longer proceed with blocking third-party cookies from the Chrome Browser. The ICO has been closely monitoring the digital advertising industry's progress towards ensuring privacy protections for individuals. It recognises the complexity of the AdTech industry and the role cookies play in digital advertising.

The ICO had anticipated that Google's initial commitment (which has now moved from) to phase out third-party cookies would be a positive step for consumer and towards enhancing online privacy standards. However, it is now concerned that Google's decision could hinder the progress towards a more privacy-focused web environment.

European Updates

EU AI Act enters into force

On 1 August, the EU AI Act, the world's first comprehensive legal framework on AI, entered into force. It provides key definitions on AI systems and a cascaded classification of risk (unacceptable, high, limited, and minimal) and regulatory duties that providers, deployers, importers, and distributors need to be aware of. The AI Act establishes jurisdiction over any entity developing, providing, deploying, operating or relying on the output of AI systems in the EU. The Act aims to create a secure and trustworthy environment for the development and use of AI systems.

The AI Act defines various transitional periods and exceptions until it fully applies, depending on the category of AI systems concerned:

- **From 2 February 2025**, the AI Act prohibits certain "AI practices" that are considered **unacceptable**, such as those that manipulate human behaviour, exploit human vulnerabilities, or carry out biometric categorisation based on sensitive characteristics.
- **From 2 August 2026**, providers and users (= "deployers") of **high-risk AI systems** will need to comply with strict obligations, including conducting a conformity assessment, registering the AI system in a public database, ensuring transparency and human oversight, implementing data and cybersecurity measures, and reporting any serious incidents or malfunctions. AI systems will be considered high-risk if they are used in the area of remote biometric identification, critical infrastructure, law enforcement, education, employment, health, or access to essential services in the private and public sector (Art. 6 para. 2, Annex III AI Act). There are exceptions, inter alia where an AI system is used to perform a narrow procedural task, to improve the result of a previously completed human activity, or where the AI system is used to detect decision-making patterns and identify any anomalies in these patterns without replacing the human assessment as such (Art. 6 para. 3 AI Act). Providers and deployers have an additional 12 months until **2 August 2027** to comply with the AI Act, if the AI system is intended to be used as a safety component in a product or is itself a product that is covered by the EU harmonisation legislation and therefore is subject to a third-party conformity assessment procedure (Art. 6 para. 1 AI Act).
- **From 2 August 2025**, providers of general purpose AI models ("GPAI models") (including in particular large language models) will need to follow specific rules, including that their models are robust, accurate, and reliable, and that they respect fundamental rights and values. They will have to provide clear and

comprehensive information to their users, and shall cooperate as necessary with the competent authorities in the exercise of their competences and powers to the AI Act. In case a GPAI model has high impact capabilities e.g. due to its number of registered users, providers will also have to report all relevant information on serious incidents and possible corrective measures to the competent authorities.

- **From 2 August 2025**, the EU and Member States will need to have an established **governance structure** to monitor, enforce, and coordinate the implementation of the AI Act. The **next steps** include the European Commission establishing an EU-wide "AI Office" that is responsible for supervising GPAI models and AI systems based on these GPAI models from the same provider. The AI Office will coordinate with the Member States to develop guidelines on the practical implementation, codes of practice on the GPAI rules, and delegated acts to establish relevant committees such as the scientific panel of independent experts. At a national level the Member States will need to adopt implementing acts, including in particular instituting national supervisory authorities and related procedural rules, as well as further rules on sanctions and fines, given that the Member States will be responsible for supervising all other AI systems.

Further news from across Europe

Click the links below for our summaries of the other news stories from across Europe in July.

1. German Federal Data Protection Authority emphasises the importance of regulatory sandboxes
2. CJEU strengthens data subject rights in two damage claims
3. Consumer protection associations can now bring representative class actions
4. The German Federal Government resolves final details for implementing the NIS2 Directive
5. VINTED fined €2.3 million for not complying with erasure requests, applying "shadow blocking" and poor accountability practices
6. CNIL Highlights Concerns Over EU Cloud Certification and Data Protection

Spotlight Section

Spotlight on Green Cyber

July saw the Ashurst data protection and cyber team join forces with our environmental and sustainability colleagues to host a webinar on Green Cyber. What is this? we hear you ask. The phrase, as far as we are aware, was first coined in a review into cyber and economic growth for the Government undertaken by the former Conservative MP for Stevenage Stephen McPartland earlier this year. At Ashurst we have been considering what "green cyber" could mean in practice for organisations. Where organisations acknowledge that they are holding large quantities of data in breach of the data minimisation principle and increasing cyber risk, can their environmental and sustainability colleagues assist them with forming arguments and cost savings, to finally get management buy-in for data deletion projects?

Quantifying the Benefits of Green Cyber

Cyber as an Enabler: Cybersecurity is often seen as a cost centre, but when integrated with green practices, it can provide tangible benefits. Effective data governance plays a crucial role in this integration by reducing unnecessary data storage. This not only lowers the carbon footprint but also enhances data insight and regulatory compliance. By retaining only essential data, organisations can mitigate the risks associated with data breaches and regulatory fines, thereby transforming cybersecurity from a cost burden to an enabler of sustainability and efficiency.

Supply Chain Security: The supply chain's cybersecurity is critical as governments increasingly require proof of cybersecurity and net zero compliance. This integration is anticipated to become a standard part of procurement

processes globally. Organisations must ensure that their data retention policies extend to their supply chains, maintaining stringent data governance practices across all tiers of their operations.

Transition to Net Zero: Organisations are under pressure to meet net zero targets and demonstrate their ESG commitments. Effective transition plans and credible sustainability reporting are essential to meet regulatory and stakeholder expectations. Meanwhile there is increasing scrutiny and legal consequences for greenwashing require that companies maintain transparent and accurate ESG reporting to avoid reputational and financial risks.

The Role of AI and Data Centres

Environmental Impact of AI: While AI can aid in addressing climate challenges, its growing energy consumption presents significant environmental concerns. Data centres, major consumers of energy, need to balance efficiency with the rising demand. Implementing effective data retention policies is crucial to minimise the environmental footprint of AI and data operations.

Technological Solutions: Innovations, such as using excess heat from data centres for other purposes, can mitigate energy consumption and emissions. Companies are investing in renewable energy to power their data operations sustainably. However, reducing the volume of retained data through rigorous data governance and retention policies remains a fundamental strategy for minimising the environmental impact of data centres.

Key Takeaways

By implementing stringent data retention policies, organisations can significantly reduce their carbon footprint, enhance data governance, and improve regulatory compliance. The evolving regulatory landscape demands transparency and accountability, pushing companies to innovate and lead in the green cyber domain. Effective data retention not only supports sustainability goals but also strengthens cybersecurity, making it a key component of modern, responsible business practices.

If you are interested in discussing this further with us, we will be holding a roundtable at our London offices on 23 September. Please contact Constance Jarrett to register your interest.

Authors: Rhiannon Webster, Partner; Nicolas Quoy, Partner; Alexander Duisberg, Partner; Andreas Mauroschat, Partner; Matt Worsfold, Partner; Joao Marques, Director; Cristina Grande, Counsel; Shehana Cameron-Perera, Senior Associate; Tom Brookes, Senior Associate; Antoine Boullet, Senior Associate; Lisa Kopp, Associate; David Plischka, Associate; Carmen Gordillo, Associate; Latasha Kirimbai; Junior Associate; Nilesh Ray, Junior Associate; Hana Byrne, Junior Associate; Saif Khan, Junior Associate; Melvin Cheung, Trainee Solicitor; Anne Wecxsteen, Trainee Solicitor; Jessica Nelson, Trainee Solicitor