Ashurst

Data Bytes 48: Your UK and European Data Privacy update for June 2024

05 July 2024

Welcome back to the June edition of Data Bytes. This edition includes an interesting case in the UK High Court on subject access requests and the CNIL's (the French data protection regulator) latest recommendations on AI and privacy.

Keep reading down to our spotlight section where we look at a significant increase in the numbers of laws and regulations that seek to impose cyber security obligations on companies. It can be hard to keep track of where these obligations sit and whether they apply to you. In this month's data bytes we turn our spotlight on some key pieces of current and upcoming legislation and guidance relevant to cyber security in UK and Europe.

UK Updates

1. Genetic company breach affecting 6.9 million Individuals under UK and Canadian investigation

The ICO and the Office of the Privacy Commissioner of Canada have opened a joint investigation into an October 2023 data breach at the global direct to consumer genetic testing company 23andMe. The cyberattack reportedly resulted in the threat actor gaining access to 6.9 million customer profiles with information including customer display names, predicted relationships and percentage of DNA shared with other users. Given that there was an "international impact", the investigation will be carried out in accordance with an agreement between the regulators on mutual assistance in the enforcement of personal information protection laws.

The joint investigation will explore whether the company had adequate safeguards in place to protect sensitive information under its control. In addition, the investigation will consider if 23andMe complied with its breach notification obligations under both the Canadian and the UK data protection laws. Privacy Commissioner of Canada Philippe Dufresne emphasised that an individual's genetic information could be misused for surveillance or discrimination and reminded developers that new technologies, such as generative artificial intelligence, are still required to comply with current law.

The investigation as to whether the company adequately met its breach notification obligations in Canada and the UK will be interesting and sends out a signal to companies that the importance of reporting a breach in a timely fashion to regulators and individuals is a potential enforcement area. Companies would be advised to dust off their breach reporting plans and test them to ensure if the worst happens, they understand and act upon their reporting requirements to statutory deadlines in multiple jurisdictions.

2. UK Case on Subject Access Requests

In the recent case of Harrison v Cameron and another [2024] EWHC 1377, the High Court (Steyn J) ruled that, in the context of a data subject access request, data subjects are entitled to know the specific identities of the recipients of their personal data and not just the categories of recipients. The case concerned a subject access request under Article 15 of the UK GDPR following a recorded telephone call in which the claimant was making a series of threats of violence.

Of significance in this case is the continued relevance of EU case law to the interpretation of the UK GDPR: The High Court referred to, and agreed with, the CJEU Austrian Post decision (C-154/21), which considered comparable questions under Article 15 EU GDPR. The CJEU decision is not binding on UK courts (as a post-Brexit judgment), but the judge could have regard to it as far as it was relevant.

The case has a number of pertinent findings for those responding to subject access requests:

- Data subjects have the right in principle to know the identities of the recipients of their personal data. It is the choice of the data subject to request either the specific identifies or just the categories of recipients of their personal data;
- Controllers can withhold this information where the request is manifestly excessive, or disclosure would be outweighed by the interests and rights of the recipients (i.e. on the basis of the “rights of others exemption” under Schedule 2 of the Data Protection Act 2018); and
- The case also confirms that the motive of a data subject access request can in certain instances be a relevant factor for refusing a request and reiterates the specific and limited purpose of the subject access regime;
- The case also considers whether a director of a company is a controller in its own right, concluding that as directors make decisions as to how data should be processed as agents for the company, they themselves are not controllers, only the company is.

3. ICO Publishes Enterprise Data Strategy

On 13 June 2024, the Information Commissioner's Office (**ICO**) published the final version of its Enterprise Data Strategy (**EDS**) following a public consultation. Developed as part of the ICO25 strategic plan, the EDS is centred on a vision of four guiding principles and two overarching goals.

The ICO's vision is that it will be "…an exemplar of responsible innovation using data. Data and insight will maximise our impact, guide all our work and accelerate our transformation." In light of this vision, the ICO has developed the following principles to guide its actions and behaviours:

- **"We democratise**. Data is everyone's job. We share data internally and externally, appropriately. We invest in data literacy for all our people, and in creating rewarding careers for our data professionals.
- **We dignify**. Our use of data doesn't take agency and control from people. It empowers them to do their best and most valuable work, freeing them up from the routine through intelligent automation. It shapes how we understand and serve our customers.
- **We're disciplined**. We put the effort in to make sure our data is high quality, structured and available. We seek out data and insights to inform critical decisions from the get-go. We apply sensible mitigations to data risks.

- **We're daring**. We innovate with data, challenging our in-built tendency to take the safest path."

In order for it to deliver its vision, the ICO has identified the following overarching goals: (1) to measurably grow its data maturity; and (2) to deliver tangible value from data and analytics for the ICO and its customers. These goals sit at the foundation of the ICO's implementation plan for 2024/25, which prioritises balancing value delivery with foundational development.

For further information, see the EDS here.

EU Updates

1. EU Data Market Study 2021-2023

The European Data Market Study 2021 –-2023, conducted by the International Data Corporation ("IDC"), a global provider of market intelligence, – and the Lisbon Council, a Brussels based think tank and policy network, provides an updated overview of the growth, and trends of the data market and economy in the EU27. The Study is part of the European Commission's efforts to monitor and support the development of a data-driven economy in Europe.

The study analyses the data policy framework in the EU and European Commission's data strategy published in 2020, namely the Digital Markets Act, Digital Services Act, Data Act, Data Governance Act, Open Data Directive. The study compares the EU's data market and economy with other regions, such as the United States, China, Brazil, and Japan. The study notes that the EU faces challenges in terms of technological dependencies and geopolitical tensions that may affect its digital autonomy and sovereignty and indicates that the EU has the potential to lead in global AI policy making and ethical AI development, as well as to foster data-driven innovation in sectors such as energy and mobility.

According to the study, the EU27 data market had a value of EUR 82 billion in 2023, and is projected to reach EUR 118 billion by 2030 under a baseline scenario. The data economy, which measures the direct and indirect impacts of data on the GDP, was valued at EUR 544 billion in 2023, and is expected to exceed EUR 723 billion by 2030 under the same scenario. The number of data professionals in the EU27 reached EUR 7.7 million in 2023, with 363,000 unfilled positions.

2. New EU High-Value Dataset Regulation

On 9 June 2024, new EU rules on the reuse of public data have entered into force ("High-Value Dataset Regulation"). Under these rules, Member States are required to oblige public sector bodies holding "high-value datasets" to make them publicly available. Re-users, such as individuals and companies alike, will have access and re-use such datasets. "High-value datasets" are datasets that have a high potential for socio-economic benefits, covering geospatial data, earth observation and environment data, meteorological data, statistical data, data on companies and company ownership, and mobility data. The availability of high-value datasets is expected to boost AI and data-driven innovation as they can provide valuable inputs for training and testing AI systems and developing new products and services.

The rules harmonize certain licensing and technical conditions for the reuse of these datasets, based on open and standard licenses and formats. The High-Value Dataset Regulation is an implementing act of the Open Data Directive, which sets the general framework for the reuse of public sector information in

the EU. The new rules have implications for data protection and data subjects' rights, as some of the high-value datasets may contain personal data or could be linked to other data sources that do. In such cases, Member States must comply with the GDPR by applying appropriate methods and techniques (such as generalisation, aggregation, suppression, anonymisation, differential privacy or randomisation) to make as much data as possible available for reuse.

3. CJEU rules: Right of access personal data regardless of the purpose of the request

On 27 May 2024, the CJEU issued a judgment (C-312/23), on the right of access to personal data under the GDPR and clarified that a data subject has the right to obtain an accurate reproduction of personal data held by controllers, regardless of the data subject's motivation for requesting the data. The CJEU notes that the term "copy" does not refer to a document as such, but to the personal data it contains. The right of access must enable the data subject to check that the personal data is accurate and processed lawfully. Therefore, the data controller must provide an accurate and intelligible copy of all personal data, not just a summary or an extract.

The judgement has far reaching implications for controllers who: (i) must comply with data subjects' requests without requiring them to state their reasons or imposing any restrictions; and (ii) may need to provide entire documents containing personal data, especially if extracts/summaries would not be intelligible or would not allow the data subject to verify the accuracy and lawfulness of the processing. We recommend that organisations review their data subject rights handling procedures in light of this judgment.

4. EDPS publishes Orientations for ensuring data protection compliance when using Generative AI systems

On 3 June 2024 the European Data Protection Supervisor ("EDPS") published its first "Orientations on data protection compliance ("Orientations") for when EU institutions, bodies, offices, and agencies ("EUIs") use GenAI systems. The Orientations:

- follows a series of AI and data protection guidance publications from national data protection authorities such as the German Data Protection Conference guidance (please see our summary of it here);
- emphasises the general principles of data protection to guide EUIs in the development and implementation of GenAI Systems, such as accountability, data protection by design and by default, under a risk-based approach as well as the need for transparent, explainable, consistent, auditable, and accessible GenAI Systems;
- highlight the need for regular monitoring and review of GenAI Systems and their impact on fundamental rights and freedoms of individuals, as well as the involvement of the DPO and other relevant stakeholders in the process of developing and deploying GenAI Systems. It acknowledges that some questions related to processing personal data when sing GenAI Systems remain open.

The EDPS considers the Orientations as a first step towards more detailed guidance that it will provide within the next 12 months.

5. EU Council agrees on GDPR enforcement rules

On 13 June 2024, the Council of the European Union agreed on a common position regarding the proposal for a new EU regulation to improve GDPR enforcement in cross-border cases, with the aim to speed up the handling of complaints and investigations, harmonize national admissibility requirements for complaints, and clarify procedural deadlines and steps. Negotiations with the European Parliament, which agreed on its position in April 2024, will follow.

The GDPR establishes a cooperation system between national data protection authorities (DPAs) that ensures a consistent application of the law throughout the EU whilst enabling complainants to deal with their own local data protection authority. However, cross-border issues were previously hampered by differences in administrative procedures. The Council's position maintains the proposal's general direction, but introduces amendments for clearer timelines and enhanced cooperation. For example, it specifies that DPAs must decide on complaints within a reasonable timeframe depending on the circumstances of each case. It also supports an enhanced cooperation procedure, with an option to bypass additional rules for simpler cases to reduce administrative burden.

6. Commission Opens Proceedings Against Meta for child protection failures on Facebook and Instagram

On 16 May 2024, the European Commission initiated formal proceedings against Meta, for alleged breaches of the Digital Services Act related to the protection of minors. The Commission's concerns centre on whether Meta's systems and algorithms on these platforms may encourage addictive behaviours in children and create "rabbit-hole effects." Additionally, the adequacy of Meta's age-assurance and verification methods is under scrutiny. This move follows a preliminary analysis of Meta's risk assessment report from September 2023, along with subsequent information requests and publicly available reports.

From a practical standpoint, this development highlights the importance for companies operating large online platforms to rigorously assess and mitigate risks associated with their design, especially when it concerns vulnerable groups like minors. Meta is now tasked with demonstrating compliance with DSA mandates, which include implementing effective age-verification tools and ensuring robust privacy and safety measures for children. The proceedings underscore the necessity for businesses to proactively address potential regulatory issues, as failure to comply can lead to significant legal and financial repercussions. Furthermore, this case serves as a reminder of the broader regulatory landscape in the EU, where digital platforms must continuously adapt to evolving standards to protect user rights and well-being.

France Updates

1. Passing of the French Law SREN

The French law on securing and regulating the digital environment (“SREN”) was officially passed on 21 May 2024 and published in the Official Journal dated 22 May 2024, representing a major legislative step towards strengthening the security and regulation of technology and online spaces in France. It marks a significant advancement in safeguarding digital environments and ensuring responsible digital governance in France.

On 21 June 2024, the CNIL publicly announced its appointment as France's designated authority for data altruism, effective since the implementation of the French law SREN on 21 May 2024, under Article 23 of the European Data Governance Regulation.

For further information on the key provisions of SREN and what is meant by data altruism, please see here.

2. CNIL's recommendations on AI and Privacy

On 10 June 2024, the CNIL released a second series of recommendation factsheets ("guidelines") and a questionnaire on the development of AI systems, underscoring how the GDPR fosters innovative and responsible AI. They are open for public consultation until 1 September 2024 and supplement the initial guidelines addressing the development of AI systems processing personal data that the CNIL published on 8 April 2024 (see here for our summary of these guidelines).

Building on its initial guidelines for AI system development from a data protection perspective, the CNIL has published seven new guidelines covering the following topics:

1. Reliance on legitimate interest as the legal basis for the development of AI systems
2. Legal basis of legitimate interest: focus on the dissemination of open source AI models
3. Legal basis of legitimate interest: focus on different measures to implement when collecting data via web scraping
4. Importance of informing data subjects
5. Respecting and facilitating the exercise of data subject rights
6. Data annotation
7. Security in the development of AI systems

As part of this public consultation, the CNIL is inviting suppliers and users of AI systems, along with all stakeholders, to share their perspectives, via the questionnaire, on the conditions under which AI models can be considered anonymous or must be regulated by the GDPR, and the implications of these classifications. At the conclusion of the public consultation, all contributions will be analysed and the final guidelines will be published on the CNIL's website.

3. CNIL's recommendations on open data and the re-use of personal data on the Internet

On 12 June 2024, following a public consultation, the CNIL issued two sets of guidelines concerning:

1. **open data** – these guidelines assists entities that make personal data publicly available in open data formats to balance their obligations and interests with the rights of data subjects. It provides advice on: identifying the responsibilities of the various bodies involved in the processing operation; determining the lawfulness of data processing; understanding the extent of obligations in terms of informing data subjects; considering the rights of data subjects; and guaranteeing the relevance, proportionality, accuracy and security of the processed data.
2. **the re-use of data published on the internet** – these guidelines offer tailored advice in respect of: re-use of data for the purposes of distributing professional directories; re-use of data for the purposes of creating and enriching databases for commercial prospecting; re-use of data for non-

health-related scientific research; and extraction of data by public authorities as part of their missions.

Additionally, in response to questions raised during the public consultation, the CNIL clarified:

- Actors can generally rely on legitimate interest when re-using data disseminated by administrations under open data legislation. In the absence of email addresses, actors may only provide public communication regarding the processing's existence, characteristics, and the rights of data subjects.
- When re-using data to create a directory of professionals enriched with user ratings and comments, individuals should have accessible options to opt out or be removed from such directories. If a professional objects to the processing of their data, the potential harm to them should take precedence over their listing in the directory.
- Organisations can only collect personal data for commercial purposes without prior consent if individuals would reasonably expect it. The CNIL recommends considering the purpose of the re-use, the type of data involved, whether the source site allows individuals to object, the nature of the source site, any prohibitions in the privacy policy or terms of use, and the proposed canvassing purpose.

In light of the feedback from the consultation and referrals, the CNIL's work on the practical guide for re-using company data will continue. This guide, which was open for consultation, has not yet been adopted by the College and will therefore not be published at this stage. Over the coming months, the CNIL will continue its work on data sharing scenarios involving the circulation of data to specifically authorised third parties and whether or not they shall appear on a restrictive list.

Spain Updates

1. Gaming platform fined €10,000 for requesting a user's ID, profession, salary, and employment history

The Spanish DPA has fined the gaming platform Eurobox S.A. €10,000 for requesting unnecessary personal information from a user. In order to reactivate the user's suspended account, Eurobox requested his ID, profession, annual salary, and employment history and it was found that Eurobox failed to adequately justify the need for these details.

In its decision, the DPA emphasized the importance of the GDPR's data minimisation principle and Eurobox's lack of transparency, as the user was not clearly and precisely informed about the purpose of collecting this information and they were not referenced in Eurobox's privacy policy or required to be collected under current regulations. These factors led to the imposition of the fine.

This case serves as a reminder to companies of the need to strictly adhere to GDPR principles, ensuring that any request for personal information is properly justified, proportional to the purpose, and transparently communicated to users. Practices that do not meet these standards can result in significant fines and reputational damage.

2. School sanctioned for breach of rights of access and data deletion of the psychopedagogical evaluations of a student

The Spanish DPA recently published a resolution by virtue of which school Colegio Caude was sanctioned for not properly addressing the rights of access and deletion requested by the parents of a student. The parents requested access to and deletion of their daughter's psychopedagogical evaluations (a study linked to psychoanalysis and medicine), claiming they never gave explicit consent for such data to be stored in systems external to the school.

The school refused to provide such information to the parents as they took the position that assessments are not given to parents, as parents place their trust in the school and guidance counsellors. The school also claimed they were unable to delete the data from the digital platform as they were not responsible for that system.

The DPA concluded that the school did not adequately comply with the data deletion and the access request and emphasised that the school should have provided a more complete response or deleted the data from its own system. This case highlights the importance of educational institutions understanding and respecting data protection rights, ensuring adequate and timely responses to access and deletion requests. It also serves as a reminder of the need to review and update internal procedures for managing personal data, ensuring compliance with current regulations to avoid sanctions and protect individuals' rights.

Spotlight: Cybersecurity laws

Cyber security threats are real and on the increase: in 2023, the UK's National Centre for Cyber Security (**NCSC**) reported that cyber attacks were up 64% compared to 2022, and in continental Europe, it has been noted that there was a 57% surge of cyberattacks over a similar period. Hand in hand with that rise in cyber security attacks has been a significant increase in the numbers of laws and regulations that seek to impose cyber security obligations on companies. It can be hard to keep track of where these obligations sit and whether they apply to you. In this month's data bytes we turn our spotlight on some key pieces of current and upcoming legislation and guidance relevant to cyber security in UK and Europe.

Key Current laws and Guidance in the UK

- **UK GDPR**

Both the UK and EU GDPR require that personal data is processed securely using appropriate organisational and technical measures.

In recent years we have seen a trend from the ICO to refer to objective security standards when assessing compliance with this principle including expressly referencing ISO27000, PCI DSS and the US National Institute of Standards and Technology (NIST) standards. They also refer to publicly available guidance such as that from the ICO and UK National Cyber Security Centre (NCSC) on, for example, the appropriate use of multi-factor authentication, patch management and encryption, legacy protocol removal and endpoint protection, data protection training and streamlining incident response.

By referring to objective standards against which organisations will be held to account, the ICO brings welcome clarity and certainty to the security principle.

- **Directors' duties**

Directors in the UK are under a general duty to act in their companies' best interests and promote its success – this includes helping ensure a strong company reputation, and to consider the consequences of their decisions and their impact on a variety of stakeholders. Cybersecurity considerations form an important part of this duty and the NSCS has developed a useful toolkit for considerations that boards should take into account in respect of their cybersecurity duties.

Ashurst has previously written about the draft Cyber Governance Code of Practice. The Cyber Code has been designed by industry leaders in collaboration with the NCSC and is intended to formalise the government's expectations of directors for governing cyber risks, as they would with any other material or principal business risk.

- **Network Information Security Directive of 2018 (NIS 1)**

NIS 1, transposed into local law in each EU member state (including the UK at the time), is currently in effect but will be repealed and replaced by the NIS 2 Directive in October of this year (see the section below).

NIS 1's primary purpose is to provide a framework for the regulation of cybersecurity – to legislate for the implementation, monitoring and enforcement of cyber security measures across the EU. It requires EU member States to impose statutory obligations on 'operators of essential services' (or OESs) and 'relevant digital service providers' (or RDSPs). OESs are providers of a service that are essential for the maintenance of crucial societal or economic activities, whereas RDSPs are providers of online marketplaces, online search engines and cloud computing services. These entities are obliged to implement **appropriate and proportionate technical and organisational measures** to manage risks posed to the security of their network and information systems. Depending on the sector and regulated entity, certain regulators have jurisdiction to enforce compliance. OESs and RDSPs are under duties to report cyber security incidents to the relevant regulators.

- **Best of the Rest**

You will also find specific sector related security requirements in the Communications Act 2003, Privacy and Electronic Communication Regulations 2003, Computer Misuse Act, Electronic Identification and Trust Services for Electronic Transactions Regulations 2016, Telecommunications (Security Act 2021).

Upcoming Legislation Regarding Cybersecurity

Europe are currently leading the charge in putting more cybersecurity legislation on the statute book with the following key pieces of legislation imminent:

- **EU Critical Entities Resilience (CER) Directive**

The EU's CER Directive requires EU Member States to implement certain requirements into local law to ensure essential services are resilient and robust from a security risk perspective. Member States have until 17 October 2024 to adopt national legislation transposing the CER Directive, and they must each identify entities considered critical or vital for society and the economy. The named entities will then need to carry out risk assessments and take technical, security and organisational measures to enhance their resilience and notify the regulators of incidents.

- **EU Cyber Resilience Act**

The EU's Cyber Resilience Act, once it has completed its journey through the EU legislative system, will introduce new cyber security obligations on providers of hardware and software products containing digital elements. The proposed EU regulation has two main objectives: (i) ensure that hardware and software products are manufactured with fewer vulnerabilities and better security during the product's lifecycle; and (ii) allowing users to take cybersecurity into account when selecting and using products with digital elements.

- **Network Information Security Directive**

The EU's Directive 2022/2555 (the NIS 2 Directive) is due to take effect on 18 October 2024, which will repeal and replace the NIS 1 Directive.

NIS 2 Directive has been developed to expand the scope of cyber security regulation to a wider group of "essential entities" encompassing not just critical infrastructure sectors like energy and transportation, but also other important sectors like online marketplaces, food production, and certain manufacturers.

Entities regulated under NIS2 are categorised as ‘Essential’ or ‘Important’ depending on factors such as size, industry sector and criticality. In addition to implementing appropriate and proportionate cyber security measures and complying with similar obligations that were contained in NIS 1, the NIS 2 Directive will oblige essential entities to pro-actively take steps to prevent cyber security attacks (as opposed to acting after the fact) and will be subject to a higher level of regulatory fines (e.g., a penalty capped at the greater of €10m and 2% of annual global turnover). See below for some further analysis on this point.

Meanwhile although the UK have published proposals to update The Network and Information Security Regulations of 2018 (NIS Regulations) (the UK's implementation of the NIS 1 Directive they have not yet come to fruition and at the time of writing, we predict the likely change in government to place more uncertainty on this direction of travel. For now, NIS 1 will remain the primary source of cyber security legislation in the UK for the specified sectors and will not be replaced by the NIS 2 Directive and therefore we will have a divergence in the regulation of cybersecurity in the UK versus the EU. The most apparent distinction is the difference between proactive and reactive regulation.

As noted above, the NIS 2 Directive introduces an obligation on 'essential entities' to **proactively** takes steps to prevent cybersecurity incidents from occurring, as opposed to implementing appropriate and proportionate security measures but only reporting to regulators after an incident occurs. This is a key difference to observe in practice. We anticipate that organisations, particularly those with a continental European presence, will implement security measures and the associated practice of monitoring compliance and engaging with regulators to align with the requirements under the NIS 2 Directive as opposed to NIS 1. The requirements of the NIS 2 Directive will therefore likely become 'best practice'.

Authors: *Rhiannon Webster, Partner; Nicolas Quoy, Partner; Alexander Duisberg, Partner; Andreas Mauroschat, Partner; Cristina Grande, Counsel; Shehana Cameron-Perera, Senior Associate; Tom Brookes, Senior Associate; Antoine Boullet, Senior Associate; Matthew Hewitson, Senior Associate; Lisa Kopp, Associate; David Plischka, Associate; Carmen Gordillo, Associate; Julia Bell, Associate; Emily*

Jones, Associate; Nilesh Ray, Junior Associate; Hana Byrne, Junior Associate; Saba Nasrolahi, Trainee Solicitor; Muriel McCracken, Trainee Solicitor; Melvin Chung, Trainee Solicitor