Ashurst

Data Bytes 45: Your UK and European Data Privacy update for March 2024

09 April 2024

Welcome to our March 2024 edition of Data Bytes. This month, the UK and European Data Privacy and Cyber Security team at Ashurst have looked at recent data protection law developments in the UK, including the latest ICO consultations on the 'consent or pay' model and generative AI and the ICO's long-awaited fining guidance. We also provide updates on the latest legislative and case law developments in the EU which are continuing at pace and recent enforcement decisions in Spain and France.

Keep scrolling for our 'Spotlight' section, where this month we consider the rapidly evolving data protection landscape in the US. There are a host of states passing comprehensive privacy legislation, which will make privacy considerations even more important for clients with operations in these states.

UK Developments

1. ICO consults on the 'consent or pay' model

Following Meta's adoption of its subscription model in Europe (whereby users have the choice to pay to use Facebook and Instagram without ads) and the regulatory scrutiny that ensued, including the most recent investigation by the European Commission under the Digital Markets Act, it is no surprise that the ICO has issued a consultation on its 'emerging thinking' on such models. The consultation closes on 17 April 2024. Responses will inform and help develop the ICO's final regulatory positions which will be reflected in its upcoming guidance update on cookies and similar technologies to be published after the Data Protection and Digital Information Bill receives Royal Assent.

The ICO is intentional in its decision not to provide a definitive view and interestingly refers to mechanisms such as cookie walls that are unlikely to comply with the consent threshold. It highlights that whilst data protection laws do not prohibit the 'consent or pay' business model, reliance on consent for personalised advertising must take into account factors such as: power balance; equivalence (are the ad-funded service and the paid-for service the same?) and fee amounts (consent for personalised ads is unlikely to be freely given when the alternative is an unreasonably high fee).

2. ICO releases new data protection fining guidance

Following a consultation process in 2023, the ICO published its new fining guidance on 18 March 2024. In this guidance, the ICO helpfully (and for the first time) provides insight and transparency into its fining

approach under the UK GDPR and the DPA 2018 going forward. In particular, this guidance provides insights on:

- the concept of an 'undertaking', which is a key term when determining fine amounts;
- factors the ICO will consider when determining whether a penalty notice is appropriate, including: (i) the seriousness of the breach and whether it was intentional (e.g. senior management authorised the unlawful processing) or arose as a result of negligence; (ii) aggravating factors (such as costs saved as a result of a failure to invest in appropriate measures) and mitigating factors; and (iii) whether the imposition of the fine would be effective, proportionate and dissuasive; and
- the ICO's five-step approach to calculating a fine amount. This is particularly interesting as it sets out 'starting points', 'indicative ranges' and adjustments in the form of calculations and figures which bring to life how the ICO will ultimately reach a decision on the fine amount.

3. ICO releases second call for evidence on generative AI

On 26 February 2024, the ICO released its second call for evidence as part of its consultation series regarding generative AI, with a focus on purpose limitation in data processing. This update emphasises the necessity for organisations to define clear, specific and legitimate purposes for processing personal data in the context of generative AI models. It also underscores the importance of transparency and alignment with individuals' expectations throughout different stages of the AI model lifecycle, including training, adaptation and application development.

This consultation also highlights the need for compatibility assessments when reusing training data and stresses the significance of establishing new purposes if further processing diverges from the original intent. By providing guidance on purpose limitation principles, the ICO is delivering on its promises to 'not miss the boat' on AI and to proactively share with stakeholders its early emerging thinking on data protection challenges associated with generative AI. The consultation closes on 12 April 2024.

4. House of Lords launches inquiry into UK-EU data adequacy arrangement

On 15 March 2024, the House of Lords European Affairs Committee launched an inquiry examining the UK's EU data adequacy arrangement. Following Brexit, this adequacy arrangement is relied on by organisations for transfers of personal data under the GDPR from the EU to the UK without the need for additional safeguards such as standard contractual clauses. The Committee will assess the existing adequacy arrangement, including the challenges for its renewal by the EU Commission in 2025 and the implications of adequacy not being renewed. The inquiry is taking place against the backdrop of potential legislative change in the UK in the form of the UK Data Protection and Digital Information Bill. The Committee is accepting written evidence until 3 May 2024 and is due to release its findings in July 2024.

5. ICO releases guidance to assist employers in mental health emergencies

Data protection laws do not inherently prohibit or 'block' the sharing of personal data and this is particularly true in urgent emergency/vital scenarios, such as in a mental health emergency. In recognition of the same, the ICO recently published guidance for employers on what they 'must', 'should' and 'could' do when sharing their workers' personal details in a mental health emergency.

The guidance encourages employers to think in advance about when and how it is appropriate to share information and also suggests that employers give workers the opportunity to identify separate emergency contacts for general emergencies and mental health emergencies on an emergency contact form.

European Updates

1. European Parliament publishes final text of the AI Act

On 13 March 2024, the European Parliament endorsed the AI Act by 523 votes in favour, 46 against and 49 abstentions. Following the political agreement in December, this is the next important step on the way to the adoption of the AI Act in this legislative period. The regulation must now be formally endorsed by the Council, which will most likely occur in April 2024. The AI Act will enter into force 20 days after its publication in the Official Journal of the European Union and will be fully applicable 24 months after its entry into force. In the meantime, familiarise yourself with what businesses need to know and do next to prepare for the introduction of the AI Act here.

2. Council and European Parliament reach provisional agreement on the European Health Data Space ("EHDS")

On 15 March 2024, the Council and the European Parliament reached a provisional agreement on a new law which paves the way for the easier exchange of, and access to, health data at an EU level. The Council and the Parliament will now need to endorse this agreement. The proposed regulation aims to improve access and control for individuals regarding their personal electronic health data, whilst also enabling the reuse of certain data for the public interest and scientific research. The EHDS will mean that individuals will have easier access to their health data, regardless of whether they are in their home member state or another member state (for example, patients could have their prescriptions fulfilled in a pharmacy in another member state and doctors would be able to access the health data of a patient from another member state). The EHDS will also provide researchers and policy-makers with wider access to specific health data, enabling them to utilise the enormous potential of a large database in the public interest. To improve control, individuals can exclude or restrict access to their health data, by healthcare professionals or for further use.

The EHDS is one of nine European sector and domain-specific data spaces set out by the Commission in its 2020 communication entitled "A European strategy for data". The Commission is aiming to establish further data spaces in agriculture, manufacturing, energy, mobility, finance, public administration, skills and the European Open Science Cloud with the overarching priority of meeting the Green Deal objectives. Ashurst is among the very few law firms with distinct expertise in the field of data spaces, having created Catena-X (www.catena-x.net), the first collaborative data space for the automotive industry.

3. CJEU rules on joint controllership in TCF marketing-related data processing

On 7 March 2024, the Court of Justice of the European Union ("CJEU") issued a preliminary ruling in "IAB Europe (C-604/22)" on joint controllership and the definition of personal data. The CJEU held that IAB

Europe and its members were joint controllers with respect to the processing of marketing-related consent declarations under the "Transparency and Consent Framework" ("TCF") set up by IAB Europe.

TCF is a GDPR consent management solution for targeted advertisement cookies in the EU. With the TCF, IAB Europe aims to promote compliance with the GDPR when advertisers use the OpenRTB protocol. The OpenRTB protocol is one of the most widely used protocols for Real Time Bidding, an instant and automated online auction system of user profiles for the purpose of selling and purchasing advertising space on the internet ("RTB"). IAB Europe presented TCF to publishers, advertisers and vendors as a solution capable of bringing RTB into conformity with the GDPR.

Please see a more detailed description of the judgment and its consequences here.

4. CJEU strengthens corrective powers of data protection authorities ("DPAs")

On 14 March 2024, the CJEU issued a preliminary ruling on the corrective powers of DPAs to erase personal data. The CJEU held that a DPA can exercise its corrective powers under Article 58(2)(d) and (g) of the GDPR on its own motion and does not need a prior data subject request to: (a) order the controller or processor to bring processing operations into compliance with the GDPR; or (b) order the rectification or erasure of personal data or the restriction of processing.

In the case, the Hungarian Újpest administration obtained personal data of Hungarian residents as part of its efforts to verify whether individuals were eligible for a financial support program during COVID-19. However, the administration failed to fulfil its transparency obligations, including by failing to inform data subjects on how they could exercise their rights. The Hungarian DPA ordered the administration to erase the personal data of data subjects who were entitled to the right to erasure under Article 17(1) of the GDPR, but who had not requested it. The court held that the DPA had the corrective power to order the erasure of the data collected on its own motion. The CJEU went even further and specified that DPAs have the power to order the erasure of unlawfully processed personal data, even if the data was collected directly from the data subject itself.

Updates from France

1. CNIL fines FORIOU €310,000 for using data supplied by data brokers for commercial prospecting without valid consent

On 5 March 2024, the French data protection authority (CNIL) published its decision SAN-2024-003 relating to the investigation of FORIOU's telephone marketing activities, which resulted in a €310,000 fine (1% of the company's turnover) being imposed by the CNIL.

The CNIL found that the data FORIOU obtained from brokers for its cold calling campaigns lacked a lawful processing basis under Article 6 of the GDPR. Although the brokers collected the data through participation forms in competitions or online product tests, the CNIL held that FORIOU could not rely on legitimate interests as a legal basis for the collection of such data given that the forms did not consistently mention FORIOU as a potential contact.

Furthermore, the CNIL found that FORIOU failed to ensure valid consent was obtained from individuals despite imposing contractual requirements on data suppliers. The CNIL identified a significant proportion

of non-compliant prospect files, indicating inadequate downstream control.

Updates from Spain

1. Opinion 2/2024 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the TELEFÓNICA Group

In March 2024, the Spanish Data Protection Agency (AEPD) approved the Binding Corporate Rules ("BCRs") of the Telefónica Group following the consistency mechanism regulated by Article 63 of the GDPR, in which European data protection authorities and the European Data Protection Board participated.

In accordance with Article 46 of the GDPR, these approved BCRs enable the international transfer of data from Telefónica Group companies located in the European Economic Area to Telefónica Group companies located outside the European Economic Area. The BCRs represent a commitment and a guarantee of good privacy governance within the Telefónica Group. This guarantee enables the international transfer of data between its companies.

The Opinion emphasizes that the approval of BCRs by the BCR Lead does not imply automatic approval of specific data transfers and outlines the conditions under which the applicant can modify or update the BCRs, including updates to the list of group members covered by the BCRs.

2. The AEPD fines Eurocollege Oxford English Institute €90,000 for data protection violations

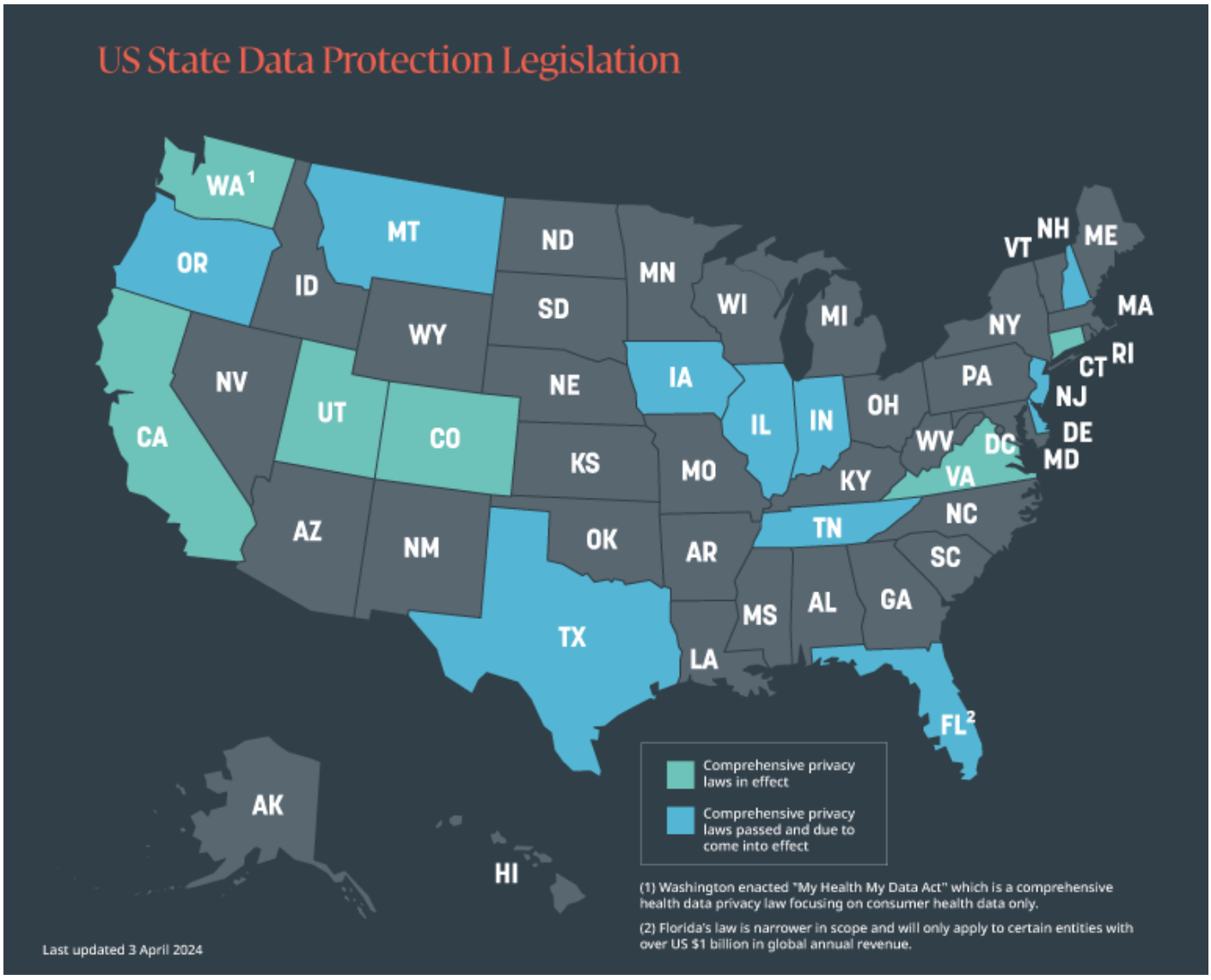
In November 2023, the AEPD imposed a fine of €90,000 on Eurocollege Oxford English Institute S.L. ("Eurocollege") following an individual's complaint.

The complainant signed a training contract with a school named CEAE and before enrollment, CEAE required the individual to: (i) undergo a medical check-up and provide a medical certificate; (ii) fill out a health declaration; and (iii) provide a criminal record certificate. Following an investigation, the AEPD found that: (i) the personal data requested by CEAE was neither necessary nor a legal requirement; (ii) CEAE had violated Article 6(1) of the GDPR by processing the complainant's personal data without a legal basis; (iii) CEAE had failed to comply with the data minimisation principle; and (iv) CEAE's collection of health data from the complainant was neither proportional nor necessary, contrary to Article 9(2) of the GDPR. As Eurocollege absorbed CEAE in 2023 by way of a merger, it was deemed the responsible party and was issued the fine.

Spotlight - A United States of Privacy?

Although we are by no means short of interesting data protection law developments in the UK and Europe, one region that is catching our eye lately is the United States. Whilst the US is yet to develop an omnibus federal piece of data protection legislation similar to the UK GDPR or EU GDPR (though we note that in the last few days, two members of US Congress have released a draft bipartisan, bicameral federal privacy bill, so it may be on the cards sooner than we think), a flurry of new legislative developments have been springing up at state level across the pond.

It goes without saying that the US data protection landscape has evolved significantly since the California Consumer Privacy Act was passed in 2018 (otherwise known as the CCPA). In 2023 alone, the number of state privacy laws more than doubled, going from just five to twelve. Several of these laws will take effect in 2024, making data protection considerations increasingly relevant for a growing number of states. See the map below to view the progress of US state privacy laws (accurate as of 3 April 2024):



Here is a flavour of key stateside developments we're keeping a close eye on:

- **California:** The first US jurisdiction to implement comprehensive privacy legislation, the Golden State is a hotbed of legal and regulatory activity in relation to data protection. The California Attorney General has now issued two pieces of enforcement action under the CCPA – a $1.2 million settlement with Sephora relating to the sale of customer data, and a $375,000 settlement with DoorDash relating to the provision of consumer personal information to a marketing cooperative. Other privacy-related enforcement action includes a $93 million settlement against Google in relation to the use of location data for profiling and advertising purposes. We have also seen the California Attorney General carry out "investigative sweeps" targeting businesses including streaming services and mobile applications. 2023 also saw the California Privacy Rights Act come into effect, amending and strengthening the CCPA. Alongside this development, California has also issued draft rules relating to the performance of cyber security audits and risk

assessments, including additional requirements where AI and/or automated decision-making technologies are used.

- **Colorado, Connecticut, Utah, Virginia**: Data privacy laws in each of these states came into effect throughout the course of last year, but do not generally govern individual or employee data or offer consumers as much protection as their Californian counterpart. The Utah Consumer Privacy Act in particular is much narrower in scope than its Californian counterpart, with multiple thresholds that must be met in order for a business to fall within its remit.
- **Texas, Oregon, Florida, Montana, Iowa, Delaware, New Hampshire, New Jersey, Tennessee, Indiana, Hawaii, Kentucky, Maryland, Pennsylvania, Minnesota, Vermont, Georgia, Wisconsin, New York, Illinois, Rhode Island, West Virginia, Missouri and Oklahoma**: Data privacy laws in Texas, Oregon, Montana and Florida are due to come into effect later this year (in July 2024 for Texas, Oregon and Florida and October 2024 for Montana). Iowa, Delaware, New Hampshire, New Jersey, Tennessee and Indiana each have laws coming into effect in 2025 or 2026. The remaining states have started rolling out bills which are at the committee and/or legislative chamber stages, and we expect at least some of these to be passed later this year. Watch this space.

In the US, we are also following more broadly:

- **Federal Trade Commission ("FTC") enforcement:** Although the US does not have a national data protection regulator like the ICO in the UK or an oversight body like the European Data Protection Board in the EU, the FTC is not afraid of using its authority to protect consumers against unfair trade practices. It has investigated companies for failing to adequately protect consumer information and for making inaccurate and misleading statements in privacy notices, amongst other things. A few key enforcement trends we've seen in the US are investigations relating to sensitive consumer data (such as health, location and genetic data), unfairness and targeted advertising and enforcement actions include fines (including for the purpose of issuing customer refunds), prohibitions against using customer data for advertising purposes and requirements to implement and document formal privacy programmes.
- **A federal privacy law?** In Biden's October 2023 Executive Order on AI, he specifically called on Congress to pass bipartisan data privacy legislation to protect all Americans, especially children. He also directed Congress to prioritise federal support for accelerating the development and use of privacy-preserving technologies, to strengthen privacy-preserving research and technologies such as cryptographic tools and to develop guidelines for federal agencies to evaluate the effectiveness of privacy-preserving techniques (including those used in AI systems). Looking back to 2022, there was a push to pass a piece of federal data protection legislation known as the American Data Privacy and Protection Act ("ADPPA"). However, one of the main controversies surrounding the Bill was its express pre-emption clause, which would have prohibited individual states from enforcing state laws that, subject to certain exceptions, governed anything covered by the ADPPA. California (with its existing state privacy laws) was outspoken on this point, urging lawmakers to create a "floor, not a ceiling" and allow states to continue to build on existing state privacy laws to offer stronger individual protection. Time will tell whether we see the ADPPA (or another form of it, such as the draft bipartisan, bicameral federal privacy bill released on 5 April 2024) and the pre-emption debate resurface as a result of Biden's order.

The developments summarised above demonstrate that there is an increasingly complex web of data protection laws to navigate across the US and it is clear that data protection compliance will look different for companies operating exclusively in the UK and EU compared to those also operating stateside. Businesses with a US presence will need to identify where any changes to their data protection compliance programme are required, prepare for compliance with new laws and continue to keep an eye on emerging developments in state legislation.

Ashurst has an established working relationship with US law firm BakerHostetler and is therefore well positioned to help you navigate the complex transatlantic data protection environment.

Authors: Rhiannon Webster, Partner; Alexander Duisberg, Partner; Andreas Mauroschat, Partner; Nicolas Quoy, Partner; Cristina Grande, Counsel; Shehana Cameron-Perera, Senior Associate; Antoine Boullet, Senior Associate; Tom Brookes, Associate; David Plischka, Associate; Carmen Gordillo, Associate; Julia Bell, Associate; Lisa Kopp, Junior Associate; Chelsea Kwakye, Junior Associate; Emily Jones, Junior Associate; Nilesh Ray, Junior Associate