Ashurst

Data Bytes 44: Your UK and European Data Privacy update for February 2024

08 March 2024

Welcome to our second edition of Data Bytes in 2024, where the Ashurst UK and European Data Privacy and Security team look to summarise the key privacy legal and policy developments of the previous month.

In this months' edition you'll see some interesting contrasts in the approach of regulators across Europe. Whilst the ICO appears to be having a rest from fines, preferring to take action through enforcement notices and reprimands, both the CNIL in France and AEPD in Spain have had a busy month, issuing monetary penalty notices on organisations for breaches.

Keep scrolling down for our "spotlight section" which this month covers the UK's approach to regulating AI. For all its talk on taking a hands-off, "pro-innovation" approach, the UK Government's non-statutory regime is not the same as nor as simple as no regulation at all. Whilst we will be waiting a number of years for the EU's broad risk based AI Act to be fully implemented and enforceable, there are several regulatory initiatives in the UK which will be impacting how organisations develop and use AI in different contexts over the next 12 months.

Get your byte sized digest here.

The Ashurst UK and European Data Privacy and Cyber Security Team

UK developments

1. ICO issues enforcement notices and guidance on biometric data processing

On 23 February, the ICO issued enforcement notices ordering Serco Leisure and seven community leisure trusts to stop using facial recognition technology and fingerprint scanning to monitor workers attendance and destroy all related biometric data. The ICO found that employees were not offered a clear alternative to having their faces and finger prints scanned for the purpose of attendance checks and subsequent payment of their time. Serco failed to show why it is necessary or proportionate to use people's biometric data, when there are less intrusive means available such as ID cards or fobs.

On the same day, the ICO also issued new guidance outlining how organisations can comply with data protection law when using biometric data to identify people. Both the enforcement notices and guidance put organisations on notice that the ICO now expects any organisation deploying biometric technologies

to clearly evidence how they are being used proportionately including how potential risks, such as errors or bias, are mitigated.

2. ICO publishes content moderation guidance

On 16 February 2024 the Information Commissioner's Office (ICO) published new guidance to help organisations use content moderation technologies and processes in compliance with data protection law. The guidance is aimed at all organisations undertaking content moderation, but has a particular focus on those using content moderation in order to comply with requirements under the Online Safety Act 2023. The ICO highlights in the guidance that a data protection impact assessment must be carried out prior to undertaking content moderation and draws particular attention to the harms that can be caused to individuals if incorrect decisions are made.

3. ICO enters into MOU with FCC on Predatory Marketing Practices

The ICO announced on 29 February 2024 it has signed a joint Memorandum of Understanding (MoU) with the US Federal Communications Commission (FCC) which details how they will collaborate to combat unwanted nuisance calls, spam messaging and the misuse of private and sensitive data. The MOU demonstrates how the ICO is seeking to deliver on its ICO2025 commitment to tackle predatory marketing and builds on existing collaboration between the regulators through the Unsolicited Communications Network (UCENet). Non-compliance with direct marketing laws is already a common area of enforcement for the ICO and this collaboration with the FCC suggests this trend is likely to continue.

4. ICO urges all app developers to prioritise privacy

Following its review of period and fertility apps (see our September 2023 Data Bytes here), on 8 February 2024 the ICO released a statement reminding all app developers to protect users' privacy. As part of the review, the ICO contacted several app providers to find out about their privacy practices and emphasised in the statement that all that app developers need to ensure compliance with transparency and lawful basis obligations. Over the coming weeks the ICO also plans to outline steps app users can take to protect their privacy. In light of the continued focus on apps by the ICO, organisations should consider reviewing their own app privacy information and any in-app consent mechanisms.

5. DSIT publishes guidance on "Smart Products" Security Regime

The Department for Science, Innovation and Technology (DSIT) published, on 26 January, guidance on the UK Product Security and Telecommunications Infrastructure (Product Security) regime. The regime comprises of: Part 1 of the Product Security and Telecommunications Infrastructure (PSTI) Act 2022 and the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 which will both come in effect on 29 April 2024. From that date, the law will require manufacturers of UK consumer connectable products (or ‘smart’ products) to comply with the relevant obligations set out in the regime, which include ensuring they and their products meet the relevant minimum security requirements. The guidance provides an overview of who exactly the regime applies to, what are their relevant duties and how enforcement will be undertaken.

EU developments

1. EDPB publishes its Coordinated Enforcement Action Report on Data Protection Officers

On 16 January 2024, the European Data Protection Board ("EDPB") has published its results on its "Coordinated Enforcement Action" ("CEA") in its report titled "Designation and Position of Data Protection Officers". With its "Coordinated Enforcement Framework" ("CEF") the EDPB aims to streamline enforcement and cooperation among the member state data protection authorities ("DPAs"). With its CEA, the EDPB wants to shed light on whether data protection officers appointed in accordance with Art. 37 GDPR have the role, organizational position and resources necessary to fulfil their tasks.

To that end, the EDPB had asked the supervisory authorities in 2023 to conduct an extensive inquiry. Based on a total of 17,490 responses to its questionnaire, controllers, processors, and DPOs have shared valuable insight, allowing the EDPB to present its CEA report with a summary of main challenges and recommendations. According to the report, DPOs and their organisations articulate a strong need for further guidance on "the role of the DPO". The report provides recommendations how DPOs could be enabled to fulfil their duties more efficiently, and at the same time reduce the burdens on resourcing the DPO that exist in many organisations. The CEA report emphasizes the existing guidance and other types of support provided by the supervisory authorities (e.g. enforcement actions, guidelines, conferences and trainings), however, also clearly recognises the strong need for updated and comprehensive guidance for all DPOs.

2. EDPB adopts opinion on main establishment of a controller

On 13 February 2024, the European Data Protection Board ("EDPB") has adopted its "Opinion 04/2024 on the notion of the main establishment of a controller" (Article 4 No. 16 lit. a GDPR. With its opinion, the EDPB has replied to the questions raised by the French data protection authority ("CNIL"), providing further clarity in relation to its previous Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority (Art 56 GDPR). The "one-stop-shop" enables organizations operating in several EU Member States to benefit from a single point of contact with the lead supervisory authority (LSA) for cross-border processing (Art. 4 no. 23 GDPR).

In its new opinion 04/2024, the EDPB holds that a controller's place of central administration within the EU provides a starting point to identify the main establishment, but supervisory authorities must still assess whether it constitutes a main establishment. To that end, the central administration must take "t*he decisions on the purposes and means of processing of personal data and it [must have the] power to have these decisions implemented*." Further, the controller must provide evidence that one of its establishments in the EU takes such decisions and implements them. Consequently, a controller located outside the EU cannot claim a "main establishment" where an organisation takes the decisions on the purposes and means of processing outside the EU. As a result, that controller cannot take advantage of the one-stop-shop mechanism and, in case of a breach, will necessarily need to notify each data protection authority of a member state individually where one or more data subjects are affected by the breach.

3. EDPB publishes digest on one-stop-shop mechanism for data breach notifications

On 18 January 2024, the European Data Protection Board ("EDPB") has published its case digest "Security of Processing and Data Breach notification", providing guidance on the specific challenges with the "one-stop-shop" mechanism ("OSS") when controllers need to deal with data security and breach notifications in multiple locations across the EU. Under the coordinated approach inherent to the OSS (Art. 56 GDPR), the lead supervisory authority (LSA) leads the investigations and needs to consult with other concerned supervisory authorities ("CSA"), in the process of reaching a coordinated decision between the supervisory authorities. In the digest, the EDPB analyses a selection of final OSS decisions on data security and data breach notification (Art. 32 - 34 GDPR).

The digest offers valuable insights on how LSAs have interpreted the GDPR in diverse scenarios in consultation with the other CSAs, such as in regard to technical and organizational measures ("TOM", Art. 32 GDPR), the root-causes of personal data breaches (e.g. malicious attacks by external entities, insufficient company practices and systems, human error), and data breach notifications (Art 33, 34 GDPR). The digest offers valuable insight through personal data breach analyses, including whether or not certain TOMs were found to be appropriate.

4. CJEU rules on non-material damages

On 25 January 2024, the Court of Justice of the European Union ("CJEU") has issued a further (preliminary) ruling on non-material damages. The CJEU held in "BL v MediaMarktSaturn Hagen-Iserlohn Gmbh" (C-687/21) that a data subject's fear about possible future misuse of personal data may constitute a non-material damage, provided that the claimant is able to prove such damage and a causal link to a breach of GDPR rules. With this ruling, the CJEU has clarified its position taking in "VB v. Natsionalna agentsia za prihodite" (C 340/21) where it had considered that a purely subjective sensation of fear about possible misuse of personal data could already result in a compensation for non-material damages.

In its recent case, an employee of MediaMarktSaturn had accidentally transmitted a customer's sales contract and credit agreement to another MediaMarktSaturn customer. The employee promptly noticed the error and retrieved the documentation within thirty minutes; by that time the other customer had demonstrably not taken notice of the personal data contained in the documents. Nevertheless, the customer alleged non-material damages arguing that he feared the other customer could make a copy of the documentation before returning it, and thereby losing control over his personal data. The CJEU rejected the argument, ruling that the claimant must establish a (non-material) damage based an infringement of the GDPR, and demonstrate the causal link between the infringement and the damage. Against that background, the CJEU confirmed that "*a purely hypothetical risk of misuse by an unauthorised third party cannot give rise to compensation*."

Updates from France

In France, the CNIL has announced its priority investigations for 2024, which are Data collection for the Olympic and Paralympic Games, Data collected online from minors, Loyalty programmes and electronic till receipts; and Data subjects' right of access. For further information click here.

Meanwhile, the CNIL fined De Particulier à Particulier ("PAP"), the publisher of the real estate advertisements website pap.fr, €100,000 after conducting two investigations which revealed the multiple violations of the GDPR, including being particularly critical of overly long data retention periods for customer account data. For further information click here.

Updates from Spain

In Spain, the AEPD has imposed a number of large monetary penalties in the last few months. In its second highest sanction to date, it has imposed a fine on gas company Endesa, for 6.1 million euros for a security breach affecting the data of millions of gas customers. For further information click here.

It has also fined Openbank 2.5 million euros for insufficient security measures, even though no actual loss of data had occurred. An Openbank customer had claimed for a mechanism to submit the requested information encrypted or through direct upload on the web portal. The only valid option was to send it via email, as the customer was asked to declare the origin of several amounts received in their bank account according to anti-money laundering regulations. After an investigation, the AEPD concluded that email was the only communication channel offered to customers at that time, which was not suitable given the potential threat to the rights and freedoms of the data subjects. For further information click here.

Finally, The AEPD has imposed a five million euro fine on CaixaBank for a security breach that allowed its customers to view data on transfers made by others with whom they had no relationship. For further information click here.

Spotlight

"Non-statutory" doesn't mean "non-regulatory" for UK approach to AI

One of the biggest takeaways from the UK Government's February 2024 response to its AI consultation was the intention to continue holding off on issuing any AI legislation. This approach can be sharply contrasted to the EU, where Member States recently gave the EU AI Act their stamp of approval, marking a significant step towards the establishment of an EU AI Office and EU AI Board for implementation and oversight (for more on the EU AI Act, please see our article here).

For all its talk on taking a hands-off, "pro-innovation" approach, the UK Government's non-statutory regime is not the same as nor as simple as no regulation at all. Whilst we will be waiting a number of years for the EU's broad risk based AI Act to be fully implemented and enforceable, there are several regulatory initiatives in the UK which will be impacting how organisations develop and use AI in different contexts over the next 12 months.

The noteworthy UK developments which have caught our attention include:

- On 15 February, the government issued a request for regulators (including the ICO but also others industry bodies such as the MHRA (for medicines and healthcare), Ofgem (for gas and electricity) and Ofsted (for education)) to publish updates on their strategic approach to AI by the end of April 2024. Unlike the EU's new AI regulatory function, these regulators are already up and running and could implement any new AI regulatory strategies potentially more quickly and with less hiccups

than the new EU governing body could. The government also announced a £10 million package to boost regulators' AI capabilities.

- In addition to the current cross-regulatory approach, the consultation response announced the establishment of a new steering committee to support coordination across the AI governance landscape. According to the response, the government has already recruited a new multidisciplinary team to undertake cross-sectoral risk monitoring within the Department for Science, Innovation and Technology (DSIT).
- In its consultation response, the government announced triggers for legislating on AI, including reviewing the plans published by regulators. The government said that binding measures or legislation would be considered by looking at factors including the adequacy of current mitigations, the ability of any new mitigating measures to mitigate risks in a targeted way, and if the risks could not be effectively mitigated using existing legal powers. They have also done preliminary analysis on initial thresholds for such legislation including "compute" used to train the model and "capability benchmarking" for high risk areas.
- Following an announcement last September, the DRCF is preparing to launch its AI and Digital Hub pilot in the spring to support AI and digital innovators with queries that span regulatory remits. In its consultation response, the UK government said that insights from the pilot will also inform the implementation of its regulatory approach.
- According to the consultation response, the UK's data protection framework, which is being reformed through the Data Protection and Digital Information Bill (DPDI), will complement its pro-innovation, proportionate, and context-based approach to regulating AI. Therefore, although the government said that it's not currently proposing any AI legislation, the government can still incorporate AI governance requirements through other pieces of legislation, and the space where this could happen is the DPDI biill.
- In February 2024 the Department for Science, Innovation & Technology (DSIT) issued guidance on techniques for AI assurance. The guide aims to support organisations to better understand how AI assurance techniques such as algorithmic impacts assessments and bias audits can be used to ensure the safe and responsible development and deployment of AI systems.

Despite the current UK Government's stated intention to refrain for the time being from implementing new legislation on AI, as shown by the above regulators are not and will not be sitting around twiddling their thumbs waiting for a legislative mandate before they start taking action. The Government has also stated that while its current non-statutory approach offers adaptability, it will be kept under review.

With the 2024 general election looming later this year, it remains unanswered whether a new government would pursue the same strategy and approach to regulating AI – however with Labour seemingly supportive of tougher AI regulation and with the current government's approach to AI supportive of further regulations and guidelines, it's a topic that can't be ignored.

Watch this space as we will be closely watching for new developments from both the UK central government and individual regulators throughout 2024.

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