Data Dispatch - September 2024

02 October 2024

Welcome to the sixth edition of Data Dispatch from the Data Advisory team at RPC. Our aim is to provide you on a regular basis with an easy-to-digest summary of key developments in data protection law.

Please do feel free to forward on the publication to your colleagues or, better still, recommend that they subscribe to receive the publication directly.

If there are any issues on which you'd like more information (or if you have any questions or feedback), please do let us know or get in touch with your usual contact at RPC.

ICO Concludes Gen AI Consultations

The UK Information Commissioner's Office (ICO) has wrapped up a series of consultations focused on data protection and generative AI. The consultations covered the following –

1. The lawful basis for web scraping to train generative AI models
2. Purpose limitation in the generative AI lifecycle
3. Accuracy of training data and model outputs
4. Engineering individual rights into generative AI models
5. Allocating controllership across the generative AI supply chain

The consultations aimed to address key challenges related to the responsible use of personal data in AI systems, ensuring compliance with UK GDPR and the Data Protection Act. The discussions highlighted concerns about transparency, fairness, and bias in AI-driven decision-making. The ICO plans to release updated guidance to help organisations deploy generative AI systems whilst maintaining compliance with privacy laws.

In parallel with the ICO's consultation, a number of companies developing generative AI systems have paused the training of their systems on user data in response to concerns raised by data protection regulators. This includes X's suspension of personal data processing for it's AI "Grok" in response to action from the Irish Data Protection Commission, and LinkedIn's decision to suspend training of its AI models on UK user data following discussions with the UK ICO.

(Source)

Uber Fined €290 Million by Dutch DPA Over Data Transfers

On August 26, 2024, the Dutch Data Protection Authority (Dutch DPA) published its record €290 million fine imposed on Uber for violating the GDPR's rules on international data transfers. The Dutch DPA argues that Uber transferred personal data of European taxi drivers to the US without using an appropriate transfer tool between 2021 and 2023. This relates to the period between the "Schrems II" judgement, which invalidated the EU-US Privacy Shield and the implementation of its replacement, the EU-US Data Privacy Framework.

The Dutch and US Uber entities in this matter qualify as joint controllers and both fall under the scope of application of the GDPR. In 2021, Uber removed the Standard Contractual Clauses (SCCs) from its Data Sharing Agreement between these two entities. With regard to the period between 2021 and 2023, Uber argues that transfers were necessary to perform contracts with the European drivers. However, the Dutch DPA held that this derogation under Article 49 GDPR could not be applied, as the conditions of the transfers being "occasional" and "necessary" have not been met.

Uber has confirmed it will appeal the fine, describing the decision as "flawed" and the fine as "completely unjustified". It will be interesting to see how the appeal progresses and whether other enforcement actions are taken in relation to the period during which there was no EU-US arrangement in place for transatlantic data flows. During this period, according to the EU Commission SCCs were not available for transfers to importers who are themselves directly subject to the GDPR (as confirmed in Q.24 of the EU Commission's FAQs) – such as Uber's US entity in this matter.

The EU Commission will shortly commence a consultation on a new version of the SCCs that will cover transfers to controllers or processors that are directly subject to the GDPR.

Article written by Kennedy Van der Laan (KVDL), our partner firm in the TerraLex Group.

ICO Reprimand to Labour Party

On 28 August 2024, the ICO issued a formal reprimand to the Labour Party for repeatedly failing to respond to data subject rights requests within the legally required timeframe.

Further to a security breach the Labour Party experienced in October 2021, it received a significant increase in data subject access requests, which, by November 2022, had resulted in a backlog of requests numbering 352. Of these, 78% were not addressed within the three-month limit, and over half faced delays exceeding a year.

The ICO's investigation, prompted by over 150 complaints, also uncovered hundreds of additional subject access and erasure requests in an unmonitored inbox, to which there was no evidence that responses had been provided.

In issuing a reprimand, the ICO recognised that since engaging with The Labour Party, the Labour Party had made improvements, including assigning extra staff and putting in place additional procedures to clear the backlog.

The reprimand highlights the importance for organisations of ensuring they deal with subject access requests in compliance with the law, including responding to all such requests within the required time limits.

(Source)