Data Dispatch - November 2024

28 November 2024

Welcome to the eighth 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.

Data Protection Supervisory Authorities' new Joint Statement on Data Scraping

The Information Commissioner's Office (**ICO**), together with fifteen other data protection supervisory authorities around the world, have released a follow-up joint statement (**Joint Statement**) to their initial August 2023 call (**Initial Statement**) for social media companies (**SMCs**) to adopt proactive measures to deal with data scraping. The Statement reflects discussions with SMCs and other stakeholders about the Initial Statement and the recommendations outlined in it.

In brief, the Initial Statement (i) flagged that publicly-available personal data is subject to data protection law in most countries, (ii) SMCs and website operators that host publicly-available personal data have a duty to protect the personal data on their platforms from unlawful data scraping (and should do so using multiple techniques), (iii) mass personal data scraping could require reporting as a data breach and (iv) users of social media platforms can take measures to protect themselves from data scraping, and SMCs have obligations to assist users to implement these measures.

The Joint Statement outlines additional expectations and best practices for SMCs and website operators that host publicly-available personal data. These include:

- using a range of protective measures to ward against unlawful data scraping and carrying out regular reviews of, and updates to, these measures to match the advances in scraping

techniques (which include the mimicking of real user activity);

- complying with data protection and AI laws (and other relevant guidance), including when using scraped data from third parties or their own data to develop artificial intelligence large language models (LLMs);
- harnessing AI where appropriate to help protect against unlawful data scraping and using APIs for greater oversight and control over large-scale data scraping; and
- ensuring that, where data scraping is permitted, it is done fairly, lawfully and transparently and that any contracts with third parties relating to data scraping contain terms which are compliant with the law (and compliance with these terms should be monitored and enforced).

The Joint Statement notes that many of the measures set out in the Initial Statement have been put in place by SMCs. The Joint Statement stresses that it is addressed to both the large SMCs, as well as smaller players, and that some tools to protect against unlawful data scraping are available at accessible cost levels. It also notes that many of the measures outlined in the Joint Statement are required by law/regulation in the jurisdictions of the signatories.

The Joint Statement reflects increasing concerns about the privacy risks of data scraping and evidences a trend towards constructive engagement between regulators and industry in respect of data protection issues.

(Concluding Joint Statement on Data Scraping)

(ICO press release on Joint Statement)

Further reading:

(Initial Statement on data scraping and the protection of privacy)

(ICO press release on Initial Statement)

Irish DPC fines LinkedIn €310 million for data protection breaches relating to behavioural analysis and targeted advertising

The Irish Data Protection Commission (**DPC**), acting as the lead supervisory authority for LinkedIn Ireland Unlimited Company (**LinkedIn**), the Microsoft-owned social media platform, has imposed a €310 million fine on LinkedIn for data protection law breaches. In addition to the fine, the DPC issued a reprimand and has mandated that LinkedIn revises its data processing practices to achieve compliance with data protection law. This enforcement action stems from a complaint originally filed with the CNIL, the French data protection supervisory authority.

Whilst the DPC has not yet released its detailed decision, it found that LinkedIn lacked a lawful basis for processing the personal data of members for the purposes of behavioural analysis and

targeted advertising (breaches of Articles 5(1)(a) and 6 GDPR). The DPC determined that:

- Under Article 6(1)(a) GDPR, which concerns consent, LinkedIn had failed to obtain the freely-given, informed, specific, and unambiguous consent of its users to use third party data (i.e. data about its members obtained from third parties) for behavioural analysis and targeted advertising;
- Article 6(1)(f) GDPR (legitimate interests) was not available as a lawful basis because LinkedIn's interests were outweighed by the interests and fundamental rights and freedoms of its members – both in respect of first party data (i.e. data obtained directly from members themselves) for behavioural analysis and targeted advertising and third party data for analytics; and
- Article 6(1)(b) GPDR, concerning contractual necessity, was also not a valid lawful basis for processing users' first-party data for behavioural analysis and targeted advertising.

The DPC also found that LinkedIn had violated its transparency obligations under the GDPR (Articles 13(1)(c) and 14 (1)(c) GDPR) and fell short of fairness requirements (Article 5(1)(a)).

LinkedIn has brought a High Court of Ireland action to contest the fine.

At the IAPP conference in Brussels this month, Dale Sutherland, DPC Commissioner, gave some insight into the decision. He explained that LinkedIn had demonstrated that it had a legitimate interest in the processing and it was necessary for those purposes. However, LinkedIn did not demonstrate that LinkedIn's interests overrode "*the interests or fundamental rights and freedoms*" (Art 6(1)(f) GPDR) of its members. He stressed that it was important to show that a detailed legitimate interest assessment has been carried out and that it was "*really robust*".

The DPC's action against LinkedIn highlights the importance of getting the lawfulness, fairness and transparency principles of data protection law right when it comes to potentially privacy-intrusive activities, such as behavioural analysis and targeting advertising. Further, although legitimate interests may appear to be readily available as a lawful basis, controllers must ensure they have thoroughly assessed and balanced their interests and those of the relevant data subjects.

(DPC Press Release)

(High Court filing)

ICO releases Audit Outcomes Report on the use of AI recruitment tools

The ICO has released its AI tools in recruitment audit outcomes report ("**Audit Report**") which sets out recommendations for both AI providers and developers to ensure their AI recruitment tools protect job seekers' privacy rights.

The recommendations in the Audit Report are based on an audit of a number of AI recruitment tool developers and providers. Although AI tools can provide significant benefits to the recruitment

process, they can create unfairness and negative impacts for individuals when not used lawfully.

The audit report includes a summary of the results of the audit, as well as a series of recommendations. It also contains some examples of how to put these recommendations into practice and uses case studies to demonstrate the points.

The ICO found that some AI tools were leading to unfair data processing, such as enabling the filtering of candidates for certain protected characteristics and inferring protected characteristics from the candidate names. Further, some tools were not audited for accuracy and some collected significant amounts of data on individuals without their knowledge to create large databases. The ICO also identified occasions where AI providers incorrectly badged themselves as processors when they were actually controllers, leading to the incorrect application and implementation of data protection obligations.

Key recommendations include:

- processing personal data **fairly;**
- being **transparent** to job candidates about the use of AI by providing detailed and clear **information** to them;
- keeping the data processed via AI to the **minimum** necessary for recruitment purposes and implementing appropriate retention periods and ensuring the data isn't used for other **incompatible purposes**;
- carrying out **data protection impact assessments** early in the process to assess the privacy risks of the AI tool;
- being clear on the **data protection roles** of the parties (controller, processor or joint controller) and the parties' relevant obligations;
- recruiters setting "*explicit and comprehensive written processing instructions*" for the AI provider (and checking from time to time that these **instructions** are being followed); and
- identifying the applicable **lawful basis** for the processing (when acting as a controller) and (if applicable) the relevant condition for processing any special categories of personal data.

The recommendations from the ICO as set out in the report were either accepted or partially accepted by these companies and steps were taken to address them.

The ICO has also published a list of questions that those procuring AI recruitment tools can use to interrogate the AI tool. These questions relate to DPIAs, lawful bases of processing, data protection roles and responsibilities, checking for fairness, accuracy and bias, transparency, data minimisation and purpose limitation.

A webinar will be hosted by the ICO for recruiters and AI developers at **10am on Wednesday 22 January 2025**, where you can learn about the audit and how to implement the recommendations.

(ICO - AI tools in recruitment - audit outcomes report)

(ICO press release on AI recruitment tools (including link to sign up for ICO webinar))

(ICO news - Thinking of using AI to assist recruitment? Our key data protection considerations)

Data (Use and Access) Bill

If you'd like to know more about the UK's Data (Use and Access) Bill, please see the article on our website here.