ADDLESHAW GODDARD

Data Diaries - September 2024

26 September 2024

In the September 2024 issue of Data Diaries, guest editor David Hackett from Addleshaw Goddard highlights the accelerating changes and key developments in data protection, technology, and cyber security law as we approach Q4. Notable topics include Ireland's Data Protection Commissioner's action against X/Twitter for AI data training, the anticipation of new data protection legislation in the UK, the implementation of the NIS2 Directive in the EU, and significant focus on the protection of children online across multiple jurisdictions. Additionally, the complexities of international data transfers are underscored by a substantial fine imposed on Uber by the Dutch data protection authority, illustrating the ongoing challenges organizations face in navigating global data privacy requirements.

Guest editorial - David Hackett

We are fast approaching Q4 of 2024, and the pace of change in the areas of data protection, technology and cyber security law is only increasing. I'm pleased to be the guest editor for this latest issue of Data Diaries, which will give you a taster of some of the interesting developments that I, together with my colleagues in our other EU offices (France, Germany and Spain), the UK and Dubai are advising on.

In Ireland, our Data Protection Commissioner recently took action against X/Twitter in relation to its use of personal data to train an AI tool. Following action by the company, the DPC has concluded its proceedings, but similar action is now being continued by Max Schrems' privacy organisation noyb. This is an interesting time for my colleagues in the UK, who are awaiting the publication of the new Labour government's proposed reforms to the laws on data protection, cyber security and AI. In the EU, we are getting ready for NIS2 and the Critical Entities Resilience Directive becoming applicable in October, as well as awaiting the European Commission's first annual report on the operation of the EU-US Data Privacy Framework (DPF). Regarding transfers to the USA, the Dutch data protection authority's recent fine imposed on Uber illustrates the complexity organisations are facing around the issue of international data transfers. The protection of children online has become a key priority in the UK, EU, USA and worldwide, and we provide a round-up of some of the latest developments in this space.

I hope that you enjoy our bulletin – please get in touch with me or another member of our data team if you would like more information about any of the topics covered.

David Hackett is a partner in Addleshaw Goddard's IP/IT & Data Protection team, based in our Dublin office.

Irish DPC action against X/Twitter for using personal data to train Grok

In August the Irish Data Protection Commission (DPC) launched High Court proceedings against Twitter International Unlimited Company claiming that Twitter was using posts by X users, including personal data, to train Twitter's AI systems including its search tool "Grok". It also claimed that Twitter had refused the DPC's requests to cease processing the personal data in question and to defer the launch of the next edition of Grok.

On 8 August the DPC announced that X had agreed to suspend its processing of the personal data contained in X's EU/EEA users' posts, which it processed between 7 May and 1 August 2024, for the purpose of training Grok. As a result, the court proceedings concluded on 4 September.

However, privacy activist Max Schrems and his organisation noyb are not satisfied that the DPC went far enough, stating that it focused on mitigations and the fact that X started processing while in a consultation process with the DPC, rather than focusing on core violations of GDPR. On 12 August noyb announced that it had filed complaints against X's use of personal data for AI training with the data protection authorities in 9 EU countries (including Ireland, France and Spain), asking what has happened to the EU data that had already been used and how X can separate EU data from non-EU data. noyb alleges the following infringements of GDPR:

- Breach of the data protection principles
- Lack of a lawful basis for processing
- Lack of transparency
- Lack of an exception permitting the processing of special category data
- Inability to respect data subjects' rights to rectification, erasure, restriction of processing and to object
- Breach of the requirement for data protection by design and by default

On 13 August X announced that it had released beta versions of two new Grok tools.

On 12 September the DPC announced that it has launched an inquiry into Google's foundational AI model, Pathways Language Model 2 (PaLM 2). The inquiry relates to whether Google complied with its obligations to conduct a DPIA prior to processing the personal data of EU/EEA data subjects associated with the development of PaLM2.

While these claims concern large tech companies, all the issues highlighted are important core principles to bear in mind when any organisation uses personal data to train an AI tool or uses an AI tool that has been trained by a third party using personal data. If you would like advice on how to implement AI in your business in compliance with the law, please contact one of our data specialists.

EU cyber security legislation coming into force in October, plus new UK legislation on the horizon

The NIS2 Directive, which expands on the existing NIS (Network and Information Systems) Directive, becomes applicable on 18 October 2024. It applies to entities which operate in critical and highly critical sectors, including energy, transport, health, water, banking, financial market infrastructures, digital infrastructure, ICT service management, public administration, space and food. There is a size threshold, but member states can designate smaller entities which fall within the national risk assessment criteria set out in the Directive. NIS2 widens the scope of the obligations imposed by the original NIS Directive, requiring in-scope entities to:

- take appropriate and proportionate technical, operational and organisation measures to manage risks to the security of the network and information systems they use for their operations or to provide their services; and
- report incidents which have caused or may cause severe operational disruption of their services, financial loss or considerable damage.

The UK implemented the original NIS Directive in the NIS Regulations. It will not implement NIS2, but the King's Speech 2024 stated that the new UK government will introduce a Cyber Security and Resilience Bill, which will:

- expand the remit of the NIS Regulations to protect more digital services and supply chains;
- put regulators on a strong footing to ensure essential cyber safety measures are being implemented; and
- mandate increased incident reporting to give government better data on ransomware and other cyber attacks.

Digital Services Act enforcement activity

The provisions of the EU Digital Services Act (DSA) applicable to very large online platforms (VLOPs) and very large online search engines (VLOSEs) came into force in August 2023 and the remainder of the Act, applicable to smaller online platforms, hosting services and intermediary services, came into force in February 2024. The DSA's goal is to prevent illegal and harmful activities online and the spread of disinformation.

From the start of this year, the European Commission has been actively enforcing the DSA against VLOPs, focusing on the following issues:

- addictive design
- transparency of recommender systems, including options for users to opt out of being profiled
- protection of minors
- the prohibition on presenting advertisements based on profiling using special categories of personal data
- age assurance and verification methods

To date the Commission has mainly focused its attentions on VLOPs, but now that the DSA is fully in force, it may start to turn its attention to smaller online platforms and service providers. The issues identified so far give an indication of the potential infringements that concern the Commission. The DSA links closely to GDPR, as both laws include extensive obligations relating to transparency, profiling and the protection of children.

Protection of children online: update

Recent developments in the UK, EU, USA and Australia show that the protection of children online is a top priority in all these jurisdictions. Guidance and action in this area can be instructive for organisations involved in dealing with vulnerable individuals of any age.

UK: ICO Children's Code updates

On 2 August the UK Information Commissioner's Office (ICO) published three items relating to its Children's Code:

Children's Code Strategy progress update

This includes its findings following a review of 34 social media and video sharing platforms in relation to the following focus areas:

- default privacy and geolocation settings – these should be switched off by default and providers should not use nudge techniques to encourage children to switch off privacy protections
- profiling of children for targeted advertising - profiling should be switched off by default for children, unless the service can demonstrate a compelling reason, taking into account the child's best interests
- use of children’s personal information in recommender systems - profiling should only be used if there are measures in place to protect the child from any harmful effects
- use of personal information of children under 13 years old - online services should establish the age of their users with a level of certainty appropriate to the risks arising from their data processing, or otherwise implement protections appropriate to children to all their users

Warning to social media and video sharing platforms about children's privacy practices

This states that, following the review referred to above, the ICO is calling on 11 of the platforms reviewed to improve their children's privacy practices in respect of default privacy settings, geolocation, age assurance and targeted advertising.

Call for evidence

The ICO has called for views and evidence on two areas of the ICO's strategy:

- the use of children's personal information in recommender systems; and
- the use of personal information of children under 13 years old.

The ICO states that it will use this evidence to inform its ongoing work to ensure that platforms protect children's privacy.

European Commission launches call for evidence on the protection of minors online

On 31 July the European Commission launched a call for evidence to gather feedback for its upcoming guidelines on the protection of minors online, which will advise online platforms how to implement high levels of privacy, safety and security for minors online, as required by the Digital Services Act (DSA). The Commission is seeking feedback on the proposed scope and approach of the guidelines, as well as on good practices and recommendations related to mitigation measures to the risks that minors can encounter online. The call for evidence indicates that:

- The guidelines will apply to all online platforms, including those aimed at adults (such as adult entertainment platforms) but that still have underage users due to inadequate or non-existent age-verification tools.
- Online platforms accessible to minors should regularly conduct a child-specific impact assessment that is structured around the OECD's "5C" typology of risks: risks arising from content, conduct, contact, consumers and cross-cutting risks.
- The guidelines will factor in the Commission's ongoing work in developing a harmonised age-verification solution based on the EU digital identity wallet.

In the USA, legal action has been taken to enforce the Children's Online Privacy Protection Act of 1998 and the Children's Online Privacy Protection Rule, focusing on addictive design and age verification. Australia's eSafety Commissioner is also taking action to require tech companies to protect children online, showing that this is a top priority globally.

If you need advice on operating your services in line with the relevant law and guidance, please contact one of our data specialists.

EU-US data transfers: update

EU-US DPF: update on first annual review

The EU-US Data Privacy Framework (DPF) came into force in July 2023. While one legal challenge has been brought, and Max Schrems has stated that he will bring another, the DPF currently provides a valid

mechanism for the transfer of personal data from the EU to US companies that have self-certified under the DPF. When the European Commission adopted the DPF, its approval was subject to regular reviews, the first taking place after one year. On 9 August 2024 the European Commission published a call for evidence on the functioning of the DPF. This closed on 6 September and the Commission plans to publish its report in Q3 2024.

Dutch DPA fines Uber €290 million for transferring drivers' data to the US without using SCCs

On 26 August the Dutch DPA announced that it had fined Uber €290 million for transferring personal data from its EU subsidiary Uber BV to the US parent Uber Inc without putting in place standard contractual clauses (SCCs) during the period between the invalidation of the Privacy Shield in 2020 and the EU-US DPF coming into force in 2023. The decision has been widely criticised, and Uber has stated that it will appeal the decision.

Uber argued that:

- It did not need to put a safeguard in place because Uber Inc, as a joint controller of the personal data, is caught by the territorial scope of the GDPR.
- It was not appropriate to use the SCCs, because the European Commission's Q&As for the SCCs issued in 2021 state that the SCCs cannot be used for data transfers to controllers or processors whose processing operations are directly subject to the GDPR.
- It could rely on a derogation under Article 49(1)(b) and (c), because the transfers were incidental (under Recital 111), as most personal data was supplied directly from the driver to Uber Inc, not transferred by Uber BV, and the transfers were necessary for the performance of a contract.

The Autoriteit Persoonsgegevens (AP) disagreed, stating that "Uber could not in any case have deduced from these statements that SCCs or other transfer tools do not have to be used if the processing falls under Article 3 of the GDPR." The AP did not accept that the transfers were incidental or necessary, so Uber could not rely on a derogation.

The decision and its subsequent criticism demonstrate that international transfers, in particular those to jurisdictions like the US, which permit extensive surveillance by governmental authorities, are complex. While Uber is correct that there is, since publication of the updated SCCs in 2021, a gap in respect of transfers to organisations directly subject to the GDPR due to its territorial scope, a more prudent approach would have been to put alternative appropriate documentation in place. Late on 11 September the European Commission announced a planned public consultation in Q4 this year for SCCs where a data importer is in a third country but directly subject to GDPR. Once these SCCs are finalised and adopted, they will fill this gap.

Next steps

Addleshaw Goddard's data protection specialists have extensive experience of advising our clients on all aspects of data compliance, so please contact one of us if you would like our assistance in relation to any of the issues covered in this newsletter, including AI training, protecting children online, compliance with EU legislation including the Digital Services Act and NIS2, or international data transfers.