


Data Protection Day: Expectations for 2024 & 2023 Look Back

January 2024

William Fry LLP is celebrating the Council of Europe's annual Data Protection Day, which is an opportunity to take stock of 2023's key data protection highlights and forecast the trends that 2024 is likely to bring. In this update, we explore:



Highlights and forecast

Part 1

Our expectations and trends for the year ahead in the ever-evolving and expanding data protection space.

Key trends include the GDPR's interplay with the EU Digital Reforms package.

Part 2

A look back on the insights from the multitude of developments in 2023, a year of many "firsts" in GDPR regulation and from which, we have an even richer body of regulatory guidance and decisions, in addition to decisions from national courts and the Court of Justice of the European Union (**CJEU**).

PART 1: 2024 Expectations & Trends

We have many expectations for 2024 and the trends that will take the main stage in data protection regulation, including:

A new data protection regulator



Europe will see the end of Helen Dixon's trailblazing term as Ireland's data protection regulator on 19 February 2024. After her ten years at the helm of European data protection regulation, a new commissioner or commissioners (currently unknown) will be appointed to the Data Protection Commission of Ireland (**DPC**). Given Ireland's location as the lead privacy regulator for many EU-based tech companies, this anticipated development is being closely monitored, particularly to gauge whether it will mark a new approach and appetite to data protection supervision and enforcement in Ireland and the European Union (**EU**).

Understanding the interplay between GDPR and the EU's Digital Reforms package



This package covers the areas of AI, content, data, cyber and platforms. In some areas, the EU is introducing "first-of-a-kind" laws (e.g. AI, content and platforms); while in others, it is building on existing rules (e.g. cyber and data protection). Each of these laws interplay with, and indeed reference, the GDPR – meaning businesses will need to assess the implications of the package both generally and from a GDPR perspective. As with the EU's flagship privacy law, the GDPR, these new laws are expected to lead the way in influencing new global standards. The net of regulation for businesses doing business in and through Ireland/the EU is getting wider, particularly when it comes to processing both data and personal data. We also expect guidance to be issued from the European Data Protection Board (**EDPB**) on the interplay between the GDPR and these new laws, which, based on its most recent plenary agenda, is a work in progress for the EU's Artificial Intelligence Act (**AI Act**) and the Digital Services Act.

A final text of the EU's AI Act



With the final text of the EU AI Act leaking on 22 January 2024 (review our initial thoughts [here](#)), it appears that it is on track to being finalised by summer 2024 – at which time it will be applicable and become effective within six months for prohibited AI systems and 24 months for high-risk AI systems, along with other transition periods. Organisations need to be cognisant of GDPR compliance when they deploy or develop AI systems given the reliance of such systems on data (including, personal data). For further analysis on the interplay between AI and data protection read our guide to AI law in Ireland [here](#).

Data protection authorities (DPAs) will continue to focus on regulating AI



As 2023 showcased, the rapid scaling and development of AI resulted in the DPAs in Europe and beyond stepping in to regulate the use of AI systems to protect the fundamental right of individuals to the protection of personal data. We expect ramped up supervision and enforcement by DPAs in 2024, particularly as the AI Act becomes applicable.

Protection of children's data online



Online safety and the protection of children's data will remain a steadfast priority for European data protection regulators, with expected EDPB guidelines anticipated on the processing of children's data. Echoing the significant fine placed on TikTok in 2023 by the DPC for the misuse of children's data, controllers and processors of personal data will be under increased regulatory scrutiny regarding: parental consent and parental controls; age assurance and age verification; children's privacy; and content regulation for children (including under the Online Safety and Media Regulation Act 2022).

DPAs implementing a framework for the EU-US Data Privacy Framework (DPF)





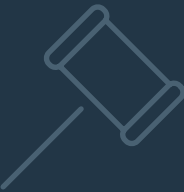

The DPF will have its first review in July 2024. The European Commission and the US Department of Commerce have been adamant that the DPF is "here to stay" (given the weight of President Biden's Executive Order) and that it is a framework that is being co-managed and co-owned by each party to the deal, meaning it will be continuously tested and assessed. The DPF's two-tier redress mechanism is operational in the US; while in Europe, 2024 will see a focus on EU DPAs getting the systems in place for the complaints mechanism go live and raising awareness for individuals that they can file complaints with the DPAs in Europe – it is important to note that the redress mechanism is for all individuals, irrespective of whether a US-based company they want to file a complaint against is certified under the DPF.

More Adequacy Decisions



Following the restoration of EU-US transfers, the Commission is set to continue making adequacy decisions in 2024, with adequacy decisions for Brazil and Chile expected.

On 15 January 2024, the Commission concluded its review and confirmed the adequacy of the 11 existing adequacy decisions, allowing for personal data to continue to flow freely to the relevant countries. Read more [here](#).

<p>Increased privacy litigation</p> 	<p>Businesses can forecast a persistence in privacy-related litigation by individuals seeking damages against them for breaches of the GDPR. While damages awarded by national courts have (to date) been low, the legal costs and associated reputational impacts are issues for which businesses need to be cognisant of as we move towards this next era of data protection regulation.</p>
<p>Coordinated enforcement</p> 	<p>The new “GDPR Procedural Regulation” is also on the table of proposed legislation in 2024. Almost six years into the GDPR’s regime, this regulation is intended to streamline enforcement of the GDPR by standardising cooperation between the EU’s privacy regulators in cross-border cases (e.g. data subject complaints and investigations) – an often-thorny issue, as showcased in 2023, due to certain tensions created by the GDPR’s “one-stop-shop” mechanism.</p>
<p>Extended jurisdiction of District Court</p> 	<p>Following commencement of the relevant provision of the Courts and Civil (Miscellaneous Provisions) Act 2023 (amending section 117 of the Data Protection Act 2018 (DPA 2018)) on 11 January 2024, the jurisdiction to rule on data protection claims has been extended to the District Court (DC). The DC has monetary jurisdiction to hear claims up to €15,000. In Kaminski v Ballymaguire Foods Limited [2023] IECC 5, the modest sum of €2,000 was payable for non-material damages, greenlighting considerably lower costs awards. Although this legislative amendment brings a welcome further possibility of redress for data protection claims, the DC does not deliver written judgments and it could therefore be more difficult to discern trends in the assessment of data subject actions.</p>
<p>More data subject access request (DSAR) guidance</p> 	<p>Since the GDPR came into effect in May 2018, DSARs have played a complex and prominent role in DPA decisions and guidelines. On 17 October 2023, the EDPB announced that the topic selected for its third Coordinated Action in 2024 will concern the implementation of the right of access by controllers, stating that, “[F]urther work will now be carried out to specify the details in the upcoming months and the action itself will be launched in 2024”. As a result, we expect that several organisations of varying sizes and from various sectors/ industries will be asked to engage in a voluntary consultation (like the EDPB’s Coordinated Action for data protection officers).</p>

If you would like to learn more about the EU’s Digital Reforms Package, read our insights [here](#).

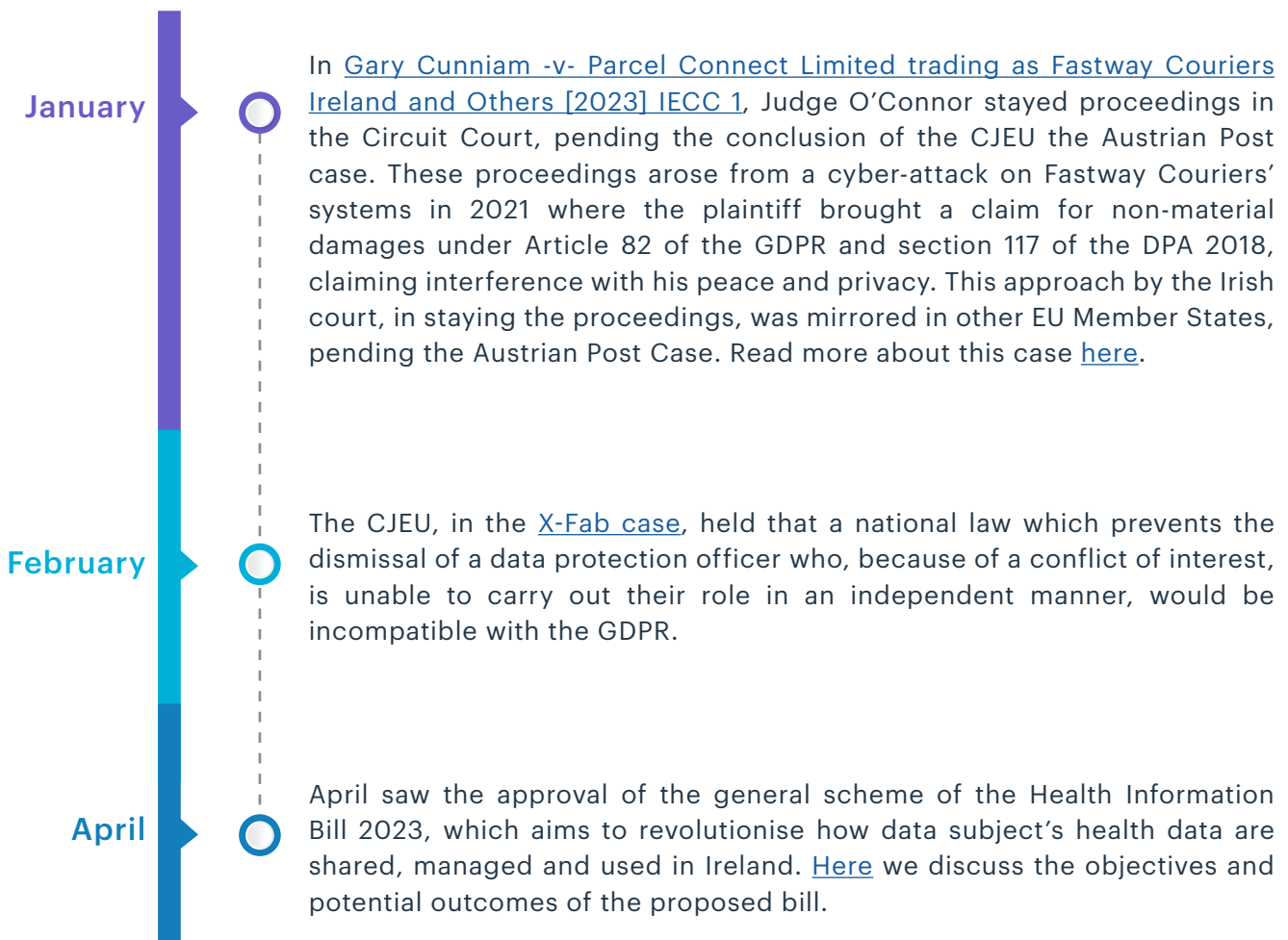
PART 2: 2023 Look Back

2023 was an unprecedented year for the number of regulatory decisions and guidance, in addition to decisions by national courts and the CJEU. The categories of regulatory developments in 2023 can be broken down as follows:

- **Data Subjects Rights & Privacy Litigation**
- **Interplay between Data Protection & AI**
- **GDPR Enforcement Ramp-Up**
- **International Data Transfers**

Given the practical takeaways stemming from these developments, a summary of the key points as they happened (by way of practical guidance), is set out below.

1. DATA SUBJECT RIGHTS & PRIVACY LITIGATION



May

The CJEU ruled in the [Austrian Post](#) case. This was the first CJEU decision dealing with an individual's right to compensation for non-material loss under the GDPR. The CJEU determined that:

- mere infringement of the GDPR will not of itself give rise to a right to compensation for material or non-material damage;
- there is no *de-minimis* standard of loss to be suffered for an individual to recover compensation under the GDPR;
- there must be a causal link between an infringement of data protection law and damage suffered to recover compensation under the GDPR.

The CJEU stated that it is for national courts to interpret this decision and apply it to data protection claims on a national basis. To read more about this case, see [here](#).

The CJEU, in [the CRIF case](#), provided welcome clarity on the obligations of controllers when responding to DSARs and the right of individuals to access their personal data under the GDPR. The CJEU held that Article 15(3) of the GDPR confers a right on individuals to receive a "*faithful and intelligible reproduction*" of their personal data which is to be understood in a "broad sense". We explore the decision [here](#).

The Irish Court of Appeal (**CoA**) agreed in [McVann](#), that there was a reasonable expectation that CCTV could be used in an investigation of a breach of security. The CoA held that personal data, captured via CCTV footage, was lawfully used in disciplinary proceedings. To read more about this case, see [here](#).

July

In [Kaminski v Ballymaguire Foods Limited \[2023\] IECC 5](#), following the decision of the CJEU in the Austrian Post Case, the Circuit Court Judge O'Connor awarded €2,000 in compensation to a plaintiff who claimed non-material damages arising from a breach of rights under Article 82 of the GDPR and section 117 of the DPA 2018. To read more about this case, see [here](#).

October

The CJEU confirmed the long-standing position that an individual is not required to inform a controller about their reasons for making a DSAR under Article 15 of the GDPR. Read our case debrief [here](#).

2. INTERPLAY BETWEEN DATA PROTECTION & AI

April

The Italian DPA temporarily banned ChatGPT when it launched in Europe, voicing GDPR compliance concerns. The DPA gave OpenAI, the developer of ChatGPT, until 30 April 2023 to address its concerns regarding ChatGPT's transparency obligations; legal basis to process personal data; and age verification measures (or else to pay a fine of either €20 million or up to 4% of its annual global turnover). On 28 April, ChatGPT was reinstated in Italy after OpenAI implemented features such as a personal data removal request form, enabling users in the EU to opt out of their data being collected, and a tool to verify users' age in Italy.

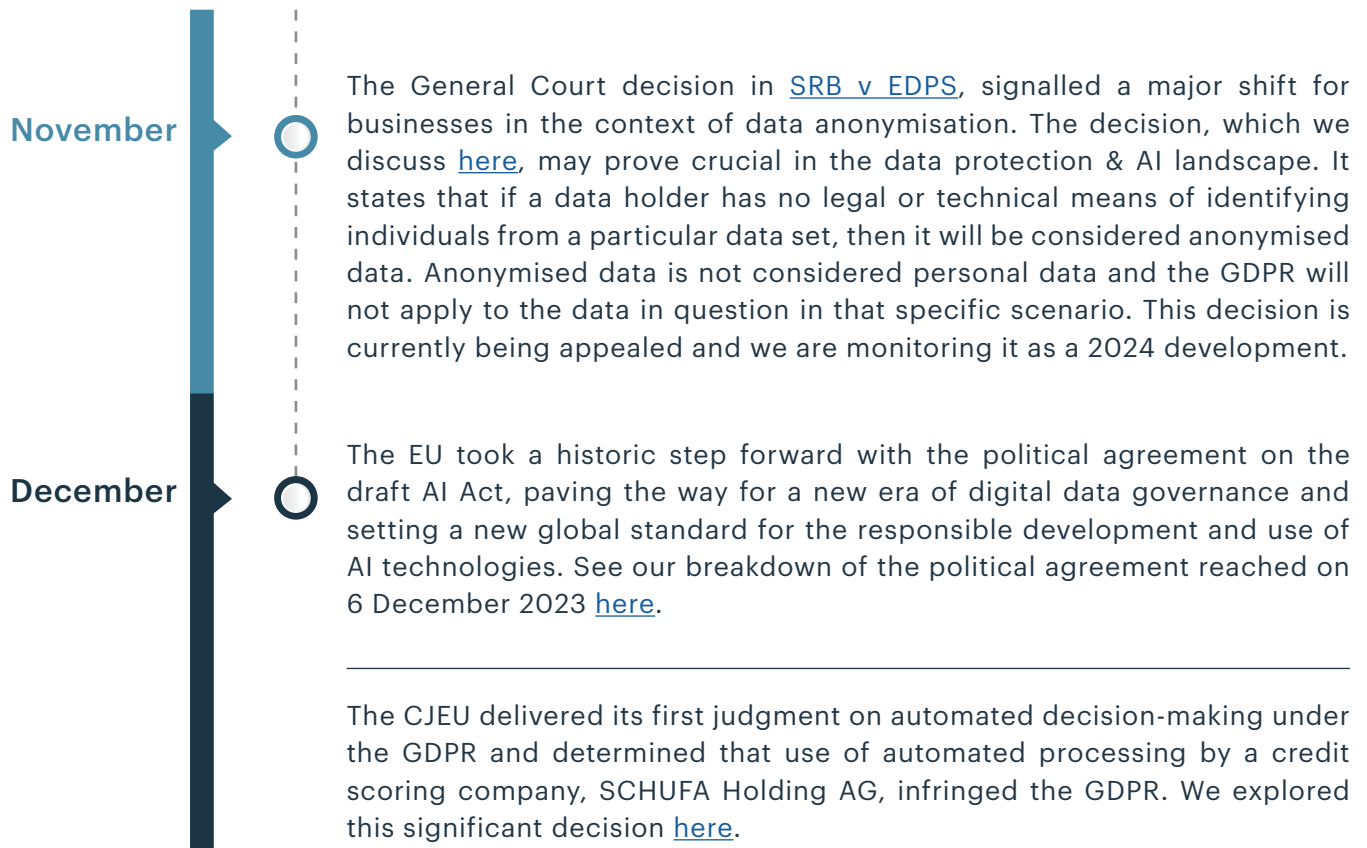
On 13 April 2023, the EDPB launched a dedicated task force on ChatGPT to foster cooperation and to exchange information on possible enforcement actions conducted by DPAs.

August

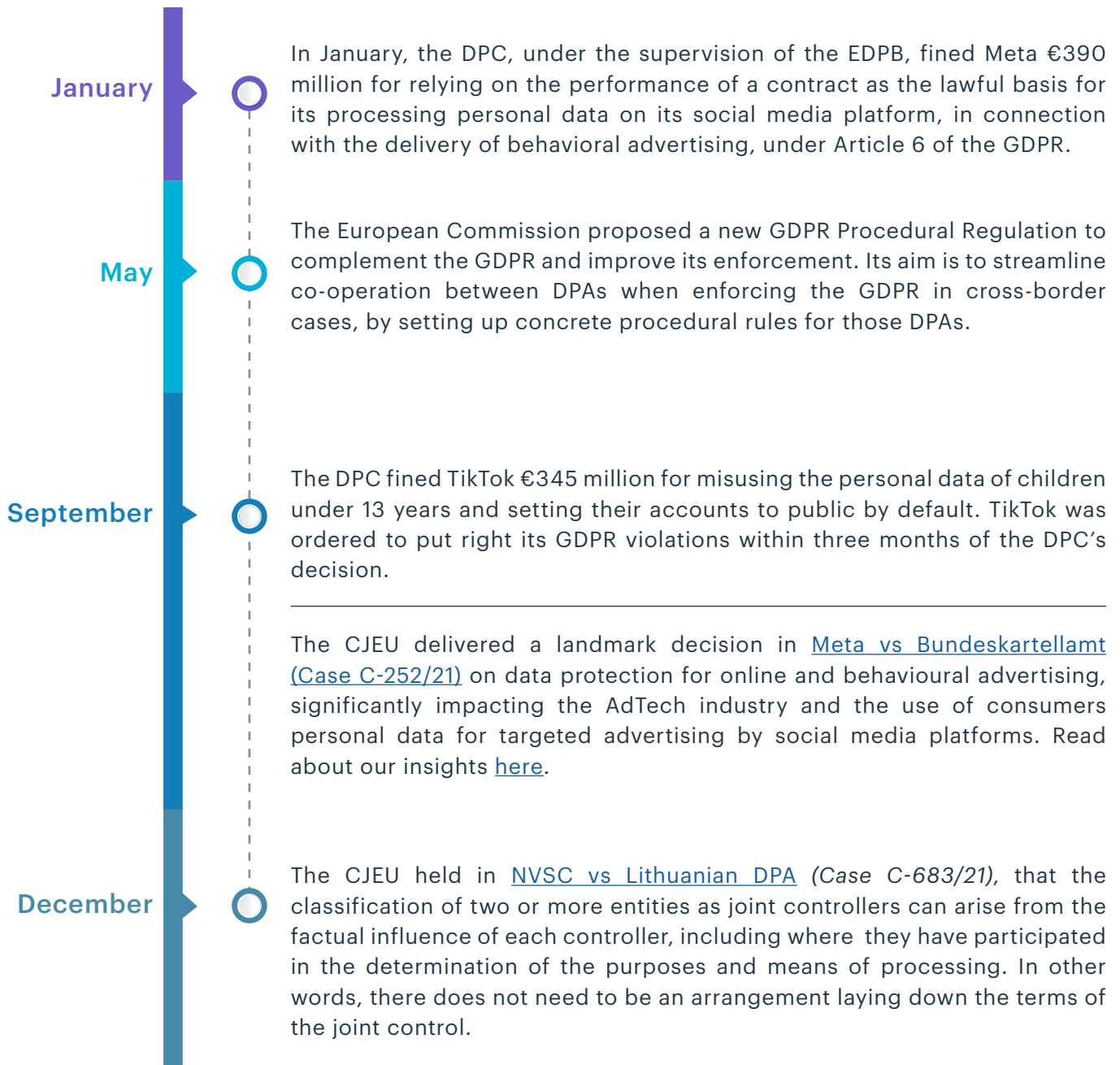
In August, 12 international data protection and privacy regulators issued a joint statement on safeguarding against unlawful data scraping. Notably, the DPC and EDPB were not signatories to the statement. Data scraping gives rise to data protection concerns when personal data are scraped and harvested without a legal basis (or knowledge of the individuals to whom such data relates). Data scraping in this manner is likely a breach of the GDPR and led to unlawful processing of personal data. For further information, see [here](#) our discussion on the main impacts of the joint statement.

October

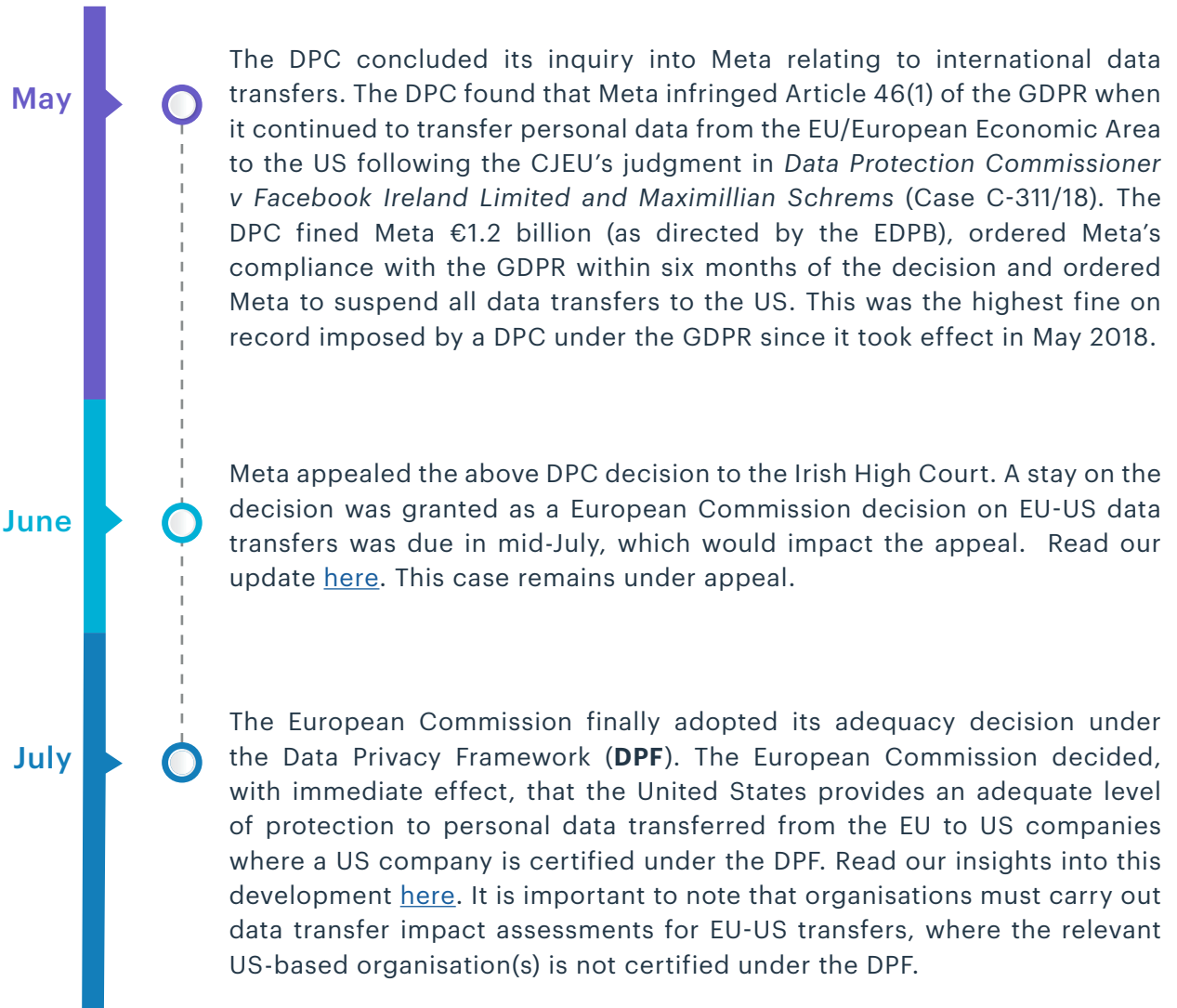
October saw the European Data Protection Supervisor (**EDPS**) submit its final recommendations on the EU's draft AI Act. The EDPS reiterated that it would be "*paramount that the use of AI systems that pose unacceptable risks to individuals and their fundamental rights are prohibited*", including the use of AI systems for automated recognition of human features and classifying people based on their biometric features. It also outlined its view that the DPAs should be the competent authorities to supervise and enforce the AI Act owing to their expertise and experience with protecting fundamental rights, the GDPR and other data protection rules.



3. GDPR ENFORCEMENT & EU DIGITAL REFORMS PACKAGE



4. INTERNATIONAL DATA TRANSFERS



Contact us

For more information on any of these developments or data protection advice, please contact Leo Moore, Rachel Hayes, or your usual William Fry contact.



Leo Moore

PARTNER
Head of Technology,
Co-lead of Tech, Data & Comms
+353 1 639 5152
leo.moore@williamfry.com



Rachel Hayes

SENIOR ASSOCIATE
Technology
+353 1 639 5218
rachel.hayes@williamfry.com



Jordie Sattar

ASSOCIATE
Technology
+353 1 489 6533
jordie.sattar@williamfry.com

WILLIAM FRY

DUBLIN | CORK | LONDON | NEW YORK | SAN FRANCISCO

William Fry LLP | T: +353 1 639 5000 | E: info@williamfry.com

williamfry.com