Data protection newsletter

Issue 14

2022 was a year of significant data protection landscape updates. The Data Protection Commission (DPC) is working towards more enforcement than guidance. Non-material damages have also been a topic of discussion across the EU, and we saw the first GDPR certification being approved and ready for candidates. There was also a continued focus on international data transfers and more fines and actions.

2023 will bring more challenges as we see the introduction of a new draft adequacy decision between the EU and the US and a DPC with two more commissioners aiming to increase enforcement.

€390m fine for breach of transparency obligations and unlawful processing

The first big fine of 2023 from the DPC was for Meta's breach of GDPR. Specifically, its unlawful processing of user's data, relying on the performance of a contract for most of its processing operations, and a breach of its transparency obligations for not clearly outlining the lawful basis it relies upon to users. The DPC has stated that Meta's basis for seeking user permission to process personal data for personalised advertising is invalid.

The European Data Protection Board has outlined that Meta is not entitled to rely on the performance of a contract as a lawful basis for behavioural and targeted advertising as part of its service. Therefore, users will be required to be provided with a

consent option to use their personal data for targeted and behavioural advertising.

Key action: Review your processing activities and ensure you have a valid lawful basis; ensure you are meeting your transparency (privacy notices) obligations. If you are using any targeted advertising based on personal data, whether on social media or other digital media, ensure you have valid consent.

€265m fine for inadequate data protection by design and default

Meta has been fined, yet again, due to data scraping that was carried out on Facebook and Instagram.

It was found that the data scraping was made possible due to Meta not implementing data protection by design and default from Article 25 GDPR. The fines are directly attributed to Articles 25(1) and 25(2). Interestingly though, Article 25(3) states that the presence of a Certificate (Europrivacy) can be used to demonstrate compliance with the other provisions.

Key action: Ensure you take data protection by design and default seriously.

.

Cookie banner taskforce report

In September 2021, the European Data Protection Board (EDPB) set up a Taskforce in response to the hundreds of cookie banner complaints filed by NOYB across Europe. The Data Protection Authorities of Europe agreed on the interpretation of the ePrivacy Directive and the GDPR in relation to cookie banners.

A draft report of the taskforce findings was published in January.

In the table below we have illustrated the key points outlined in the draft report.

Concern	Outcome
Type A – No Reject button on the first layer	The absence of refuse/reject/not consent options constitutes an infringement.
Type B - Pre-ticked boxes	Pre-ticked boxes to opt-in do not lead to valid consent.
Type C - Practice	Website owners must not design cookie banners in a way that gives users the impression that they have to provide consent to access the website content.
Type D & E – Deceptive button colours & Deceptive button contrast	Contrast and colours of buttons used must not be misleading or prompt users to choose one option over the other.
Type H – Legitimate interest claimed, list of purposes	Where no valid consent is obtained, subsequent processing is not compliant with the GDPR. The legal basis for the placement/ reading of cookies cannot be the controller's legitimate interests.
Type I – Inaccurately classified ‘essential’ cookies	Specific tools may be used to analyse a website and create a report showing cookies that were placed while visiting. Website owners are responsible for maintaining such lists and providing them to the competent authority where requested to demonstrate the essentiality of the cookies listed.
Type K – No withdraw icon	Website owners should implement easily accessible solutions allowing users to withdraw their consent at any time, such as an icon hovering and permanently visible or a link placed on a visible and set place.

Key Action: Review your cookie banner and make any necessary changes.

Recent Data Protection Commission inquiries lead to no fines

Two insurance companies operating in Ireland were subject to DPC inquiries about the number of breaches they had incurred. Neither company was fined despite reporting multiple data breaches impacting several individuals. This is due to the measures taken to safeguard the data and the ability to demonstrate accountability.

One insurance organisation notified 49 personal data breaches to the DPC between June and December 2020, with roughly 60 individuals impacted. The other insurance company notified the DPC of 156 personal data breaches between December 2018 and May 2020. In both cases, it was determined that they had implemented several measures to ensure the safety and security of personal data, such as ongoing training and awareness, defined data breach management policies, process-specific SOPs, the appointment of data champions throughout the organisation, double-factor authentication, data retention policies etc. In October, the European Data Protection Board released guidance on personal data breach notification, which will assist organisations when faced with a breach and when notification is necessary.

Key Action: Review your assessment of breaches, ensure you have robust controls in place to help mitigate risks.

.

First approved GDPR certification scheme - Europrivacy

The European Data Protection Board has officially approved the first GDPR certification scheme, Europrivacy. It is the only official GDPR certification recognised across all EU member states. Europrivacy will assess and certify the compliance of an organisation's data processing activities with the GDPR and national data protection regulations. Organisations can identify and reduce risks by demonstrating compliance while enhancing and improving their reputation and market access.

GDPR certification comes with a wide range of benefits, including:

- Enhanced competitive advantage.
- It demonstrates an organisation's dedication to data protection compliance.
- It is recognised across Europe.
- It will allow organisations to build trust and confidence with all relevant stakeholders.

Mazars is a global implementing partner with Europrivacy (more information here). We have the expertise to enable you to demonstrate your commitment via GDPR certification.

Key Action: Contact us to get started

EU-US Adequacy Decision

The European Commission on 13 December launched the process towards adopting an adequacy decision recognising the essential equivalence of US data protection standards with those in the EU.

The draft adequacy decision is now with the European Data Protection Board, the Council of the European Union and the European Parliament for its opinion. We expect to see a decision on this by mid-2023.

If the adequacy decision is adopted, EU companies will be able to transfer personal data to US companies without putting additional data protection safeguards in place. However, they should still carry out a risk assessment. A key point to note is that this is only concerning US transfers. Data Transfer Impact Assessments and SCCs will still be required for all other third-country transfers.

This draft adequacy decision follows an executive order signed in October 2022 by US President Joe Biden committing to overhauling foreign intelligence agencies access to personal data. Access to European data by US intelligence agencies will be limited to what is necessary and proportionate to protect national security. EU individuals will benefit from an independent and impartial redress mechanism, which includes a newly established Data Protection Review Court, regarding the processing of their personal data by US intelligence agencies. This court will independently investigate and resolve complaints.

Companies in the US will be able to join the EU-US Data Privacy Framework by committing to comply with a detailed set of privacy obligations and to ensure the continuity of protection of personal data when shared with third parties.

Key Action: DTIAs and SCCs are still a requirement. The deadline was 27th December 2022.

International transfers

The deadline for having the new Standard Contractual Clauses (SCCs) of December 27th 2022, has now passed. Older SCCs should now be removed, and the new ones should be in place. Failure to comply could result in complaints, fines, or instructions to cease the transfer.

Remember, data subjects can request a copy of or access your SCCs. We are expecting these types of requests to increase in 2023.

Key action: If gaps remain, prioritise highest impact SCCs (editable versions available here).

Contacts

Liam McKenna, Partner
T: +353 (01) 449 6454
lmckenna@mazars.ie

David O'Sullivan, Manager
T: +353 (01) 449 6444
DOSullivan@mazars.ie

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 95+ countries and territories around the world, we draw on the expertise of 47,000 professionals – 30,000 in Mazars' integrated partnership and 17,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.
*where permitted under applicable country laws.

www.mazars.ie

mazars