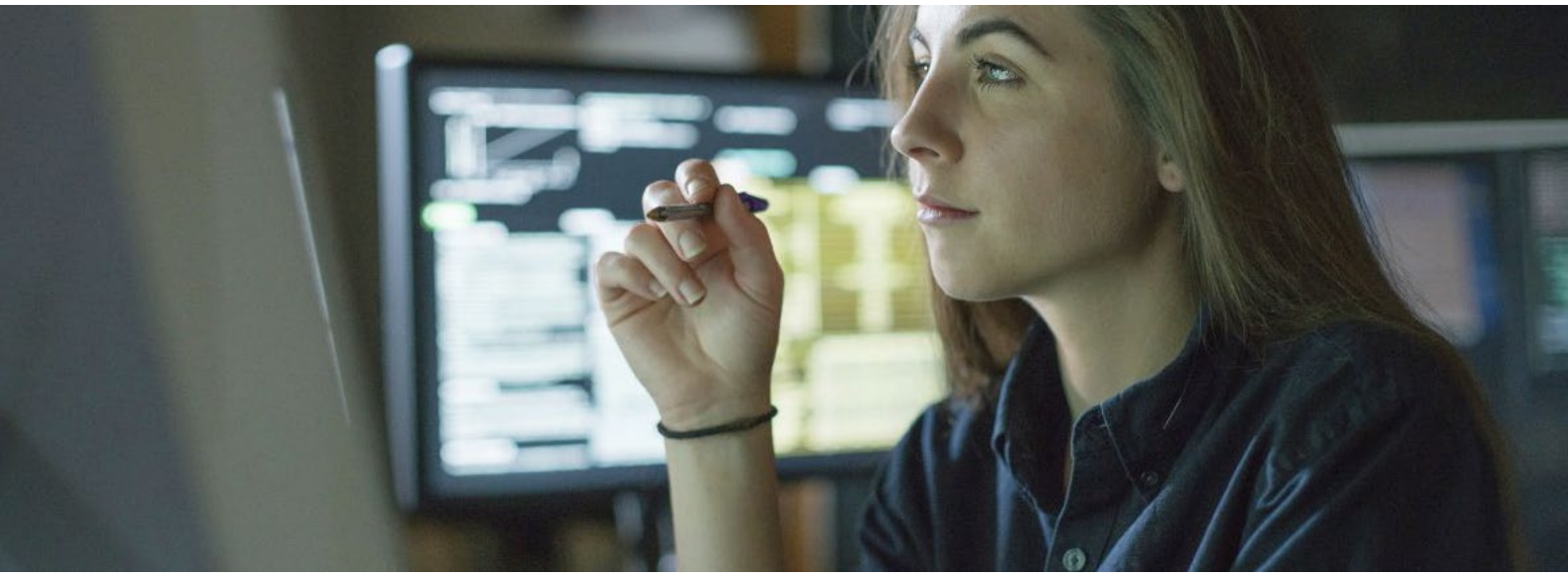

Data protection newsletter
Issue 11

As we approach the end of the year, we have reflected on five of the most significant data protection topics to date in 2021, and we supply you with a "key action" to take from the issue.

1. Data Protection Commission moving from guidance to enforcement

In July, the Irish Joint Committee on Justice published a report that included a series of recommendations on the work of the DPC. The recommendations in the report address concerns raised about the Irish DPC's oversight and enforcement of the GDPR.

The recommendations state that the DPC should:

- urgently move from emphasising guidance to emphasising enforcement;
- increase the use of its sanctioning powers – particularly orders stopping infringers from processing data, in addition to dissuasive fines – to ensure effective implementation of GDPR;
- streamline its complaint-handling processes;
- clarify its written procedures and rules with fellow regulators;
- publish the exact processes it follows when handling complaints and clarify its definitions on when cases have been "concluded" or "resolved";

- Ensure staffing levels and resource allocation are appropriate (this has led to an increase of €4.1 million funding in the latest budget)

This transition to enforcement will likely lead to a higher risk of fine or other action by the DPC, which should be reflected in data protection risk registers.

Key action: review your risk acceptance decisions in the context of increased risk of fines or sanctions and ensure that these decisions remain within your risk appetite.

2. Standard Contractual Clauses

The European Commission ("EC") adopted two sets of Standard Contractual Clauses ("SCCs") on the 4th of June:

- The first for use between controllers and processors within the EEA under Article 28;
- The second is for the transfer of personal data to third countries under Article 46.

They reflect new requirements under the General Data Protection Regulation ("GDPR") as previous SCCs had been under the older Directive and consider the Schrems II judgment.

Controllers and processors currently using the previous sets of standard contractual clauses for international transfers have until December 2022 to replace legacy SCCs. All new transfers from the end of September are required to use the new SCCs. You can find more information on SCCs **here.**

As seen in the Schrems II ruling and subsequent guidance from the EDPB, a Transfer Impact Assessment is required for all transfers to third countries that do not have an adequacy decision. The EC reinforced this in the implementing decisions for the new SCCs. A recent survey indicates that many organisations find TIAs challenging, with 67% of those surveyed indicating that completing a TIA would influence the decision to transfer data to a third country. For more information on TIAs and how to implement the SCCs see our webinar **here.**

Key action: Ensure you have a robust list of third country transfers, prioritise these and progress TIAs and new SCCs

3. WhatsApp Ireland & Facebook fines

In September, we saw a record fine imposed on WhatsApp Ireland of €225 million. To date, this is the largest fine imposed by the DPC. This came after a proposed €50 million fine was rejected by the DPCs counterparts in the EDPB, and the revised figure was enforced.

The DPC investigation examined whether WhatsApp had met its obligations regarding providing information and its transparency to both users and non-users of WhatsApp's services. We can conclude from the fine that Privacy Notices need to clearly outline all processing and the legal basis in detail. There should be no confusion or uncertainty as to the processing taking place and the legal basis relied upon by companies.

The DPC has recommended that Facebook Ireland be fined up to €36 million over breaches of its transparency obligations, according to a draft decision. As the lead supervisory

authority for Facebook in Europe, they must now share their draft decision with other EU regulators before a final decision can be reached. This adds strength to the reasoning for updating privacy notices!

As with the WhatsApp fine, we can expect other EU regulators to object to what may be perceived as the low value of the fine and that this will be increased to indicate in the severity of the non-compliance. NOYB has more information on their website.

Key action: Review and update your privacy notice to reflect the requirements identified in the judgement

4. UK adequacy decision

On the 28th of June, the EC announced that it had adopted two adequacy decisions for the UK, one under GDPR and one under the Data Protection Directive with Respect to Law Enforcement. The EC has now formally recognised that UK data protection rules are "adequate" and that personal data can flow from the EU to the UK.

The UK's data protection system continues to be based on the same rules that applied when the UK was a Member State of the EU, and the UK has fully incorporated the principles, rights, and obligations of the GDPR and the Directive into its post-Brexit legal system.

The EC noted that both adequacy decisions include strong safeguards in case of future divergence, including a sunset clause, which limits the duration of adequacy to four years. But as we begin to learn that the UK wants to overhaul its data protection regulations, any major changes could jeopardise their adequacy.

Key action: if you transfer data to the UK keep an eye on the UK GDPR changes and their impact, e.g. the potential need to implement both UK and EEA SCCs.

5. Data Protection Officers

With an increasing number of privacy and data related laws, guidance and regulations coming into effect, organisations have come to rely heavily on the experience and expertise of their appointed Data Protection Officer ("DPO"). DPOs play a crucial role in keeping organisations compliant and accountable concerning data protection. The role of the DPO is complex, acting as the point of contact between the organisation and the DPC, identifying data protection risks, advising on data protection compliance and ensuring the rights of data subjects are met. Since the introduction of the GDPR, it's not surprising that there has been a shortage of qualified DPOs. It's not simply enough to promote someone with an IT or legal background. A solid understanding of the GDPR is vital. The ability to interpret complex regulatory requirements and provide useful advice is key. Through outsourcing, the role of the DPO organisations can get all this and more. Through greater insight into how other organisations are implementing the principles of GDPR, access to external resources and specialised consultants, industry expertise, the understanding of how to apply the GDPR in practice, and the ability to promote a culture of data protection compliance throughout an organisation are just some of the unique selling points of an **outsourced DPO**

Key action: Be good to your DPO!

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 90 countries and territories around the world, we draw on the expertise of 42,000 professionals – 26,000 in Mazars' integrated partnership and 16,000 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