



Data protection newsletter Issue 10

It has been almost three years since the GDPR came fully into force, and it feels like we have achieved a lot. Still, the challenges of greater digitisation coupled with increased awareness of the topic by people have resulted in no easing of the workload for organisations and data protection teams.

Some organisations have made enormous strides in embedding a culture of data protection, which is evident in their approach to change. However, despite this, there are two areas where cultural weaknesses most commonly show themselves:

1. Legacy skeletons in the cupboards: old contracts, relationships and technology that were not addressed as part of the initial GDPR project continue to blow up intermittently. When I talk to senior management teams, I still sense that some people want to keep their head down and fingers crossed.
2. Change processes: DP considerations not being fully incorporated into the change process. We have data protection by design and default build into our change approach, complete DPIAs and address the risk associated with third

parties we transfer data. However, it sometimes feels like the approach is a tick box exercise. Where this is the case, the DP team are brought into the conversation late, and changes the DP team suggest that would have been simple and impactful if considered earlier in the process are perceived as barriers to deadlines by the project teams.

It is critical for us as DPOs to show ourselves to be practical in our approach, encourage our colleagues to engage with us early and protect the organisation from making costly mistakes. Engaging often and having access to the most senior management is critical to addressing this challenge.

Transfer Impact Assessments

When Safe Harbour was invalidated as a method of legalising the transfer of personal data to the US in 2015, nothing meaningful changed.

Organisations took a chance and were quickly rewarded with Privacy Shield in 2016.

Since Privacy Shield was deemed inadequate for GDPR purposes in mid-2020, there has been a change to third country transfers. It seems this time we are taking the decision seriously! The result is the new standard contractual clauses that are in the process of being ratified and the completion of Transfer Impact Assessments. The approach to compliantly conduct third country transfers is addressed in detail in our [International data transfers webinar](#).

When completing the TIA, there is a need to consider if the four essential guarantees required by the EU are present in the third country and the specific measures implemented by the target organisation. So, they do become easier, e.g. we assessed India's essential guarantees last month, and this reduces the effort in any further India related TIA.

EDPB guidance on breach assessment and notification

In January, the European Data Protection Board published [guidelines on examples regarding breach notifications](#).

This is a very helpful document. It goes through 18 specific examples of breaches from snail mail and human error on emails to sophisticated attacks. It outlines what would be reportable both to the DPC and the data subjects.

COVID-19

Last year organisations spent time designing compliant ways to bring staff back to their offices. Many wrote about the legality of temperature checks, the minimisation of data collected on return to work forms etc. This year the concerns have become more fundamental, i.e. if you don't want to be vaccinated, does your employer have a right to know this and could it impact their assessment of your performance or ability to do your job?

The EU has proposed a [Digital Green Certificate](#).

The initial press release recognises the privacy and security concerns. It will be interesting to see how these are delivered in practice in the coming months.

Brexit and data transfers

On February 19th, the EDPB provided a positive opinion on granting an adequacy decision to the UK. The EU Commission now has to complete the process of formalising the adequacy decision.

Until the end of June, transfers from the EEA to the UK continue to be legal under the EU-UK Trade and Cooperation agreement. The last adequacy decision that the EU granted to Japan took four months to get through the EC process, and so the likelihood is that the EC will meet the deadline of June 30th.

EEA organisations that process data of UK residents still need to consider if they have addressed the other outstanding items, e.g. have a representative in the UK, have updated breach processes to consider the need to report to the ICO. Our [Conducting GDPR compliant operations with the UK webinar](#) cover the requirements.

Contacts

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