Data protection newsletter - Issue 9

As this most challenging year comes to a close, we consider how civil sanctions are being settled; proposed updated standard contractual clauses; accountability and data protection by design and default.

Civil actions

Its more than 2½ years since the GDPR came fully into force and it feels like gradually organisations are becoming more and more compliant. The fear that big fines and sanctions would be imposed quickly has proven incorrect. However, GDPR is embedding its way into organisational systems and thinking. It is difficult to find a single source of judgements from civil actions, it seems that most organisations are settling complaints quietly rather than potentially being a test case and paying expensive legal fees.

A search around the internet indicates that Germany and the Netherlands are the jurisdictions that have had the highest number of civil judgements. In Germany civil actions where the data subject didn't suffer any material damage were not awarded any compensation by the courts. Data subjects have been more successful in the Netherlands where they have received judgements in the order of a few hundred euro for non-material damages.

When we feed this into our thinking as DPOs and privacy professionals, it would indicate that systemic errors that impact many data subjects are a high risk, especially given the opportunity for these subjects to come together in one case. The decision to pay out on ad-hoc individual issues may appear sensible given the cost and management effort of fighting these. However, by doing so we create culture of pay-outs that will ultimately add costs to all our organisations.

New draft standard contractual clauses

The EDPB is inviting feedback on the new draft standard contractual clauses. The feedback opportunity will end on December 21st.

Once published, organisations will have one year to migrate from the old SCCs to the new ones. The SCCs include a response to the Schrems II finding including:

- Refusing where possible and minimising where mandatory the sharing of personal data with government agencies.
- Providing transparency reports (as much as legally possibly) to notify on data shared with these agencies
- Conducting transfer impact assessments to assess the risk of the data transfer
- Providing systems to support all of the data subject rights defined in the GDPR

mazars

In addition, the draft SCCs help deal with some of the legacy issues as they can be extended to processor to sub-processor relationships and can be agreed and signed by multiple parties that are jointly delivering an end-to-end process.

Schrems II update

Following the Schrems II judgement in the European Court of Justice which struck out privacy shield, the legal cases keep coming with both Facebook and Max Schrems having court proceedings with the DPC.

However the EPDB has established a task force to review Schrems complaints against 101 data controllers in the EEA which transfer data to Google and Facebook in the use via cookies.

While the legal wrangling goes on, it appears that EEA organisations are taking account of the Schrems II judgement when establishing new data transfers but that legacy transfers will only be addressed over time. I suspect that this will probably happen as part of the migration project to the new SCCs when they are published.

New EDPB guidance on DPbDD

The European data protection board adopted new guidelines on data protection by design and default on October 20th 2020. The document is 30 pages long and breaks down the definition of DPbDD into its component parts with some additional guidance A couple of points I took from it on the first read are:

Cost is a factor when considering DPbDD but it cannot justify not implementing DPbDD.

DPbDD needs to be taken on early in projects and maintained through the process.

DPbDD needs to be periodically reviewed once the process is live to ensure that the controls remain adequate as technology and the environment changes

In addition, it provides advice on the DPbDD considerations under each of the GDPR principles. This is useful and would be worth building into the DPIA process.

The final words of advice in the guidelines are “get professional advice and help.” We anticipate the requirement to conduct reviews of change lifecycles in the coming months to assess adherence with the guidelines.

ICO guidance on accountability

The UK’s ICO has developed a sub-website on meeting the accountability principle. The content can be viewed online or downloaded as a 100-page document.

It’s very good and many organisations will find that despite the scale of the requirements they are largely compliant and can take something from it to further mature their compliance. The information is also a useful tool to develop or update a GDPR compliance audit programme that could be used to meet the DPO obligations.

Mazars rebrand

You may have noticed that Mazars rebranded in October 2020. The branding doesn’t so much change our message but clarify in a more concise way what 7000 staff and clients communicated to the brand team over the last two years. Its highlights both what we are and what we aspire to be. The key pillars of the brand are: empowered expertise, seamless integration, balanced perspective and social conscious.

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

Sarah Hipkin
Director
T: +353 (01) 449 4419
shipkin@mazars.ie