THE BIGGEST GDPR MISTAKES SIX MONTHS ON

Written by Robert Wassall / First published: 21st November 2018

"With many organisations already far behind on compliance, we are likely to see a large wave of fines and disciplinary action from the ICO in the next six months if organisations don't take the spirit of the GDPR to heart."

Six months on from its introduction, the GDPR has done much to shake up the way organisations collect, secure and use people's personal data. However, while the ambitious legislation has succeeded in many of its original goals, there are other objectives which may be longer in the making.

On the positive side, the GDPR has certainly achieved its primary aim of harmonising data protection laws across the European Union. Similarly, it has also successfully overseen sweeping modernisation, brought data laws up to date, and made them fit for purpose.

However, the GDPR has yet to truly change the culture around data privacy and security. This is perhaps the greatest challenge, and it means overcoming the longstanding attitude that data protection is not a significant business risk nor a particularly important business priority – an attitude that has been ingrained over many years.

As a result, many organisations have failed to understand the significance of the GDPR and what it represents. This means we still commonly see organisations either trying to take shortcuts or, crucially, misunderstanding key elements of the law. As a Lawyer and in my capacity as a virtual Data Protection Officer (vDPO) working with multiple organisations, I have first-hand experience of how this can leave organisations exposed.

Misunderstanding Data Protection Officers

As a vDPO, I fulfil the Data Protection Officer role for organisations ranging from charities and schools to large manufacturers and pharmaceutical firms based overseas. With this breadth of experience, I have found that, generally, most organisations do not understand the role of the DPO.

The GDPR recognises that DPOs are key players in the new data protection regime. The Information Commissioner's Office (ICO), says that a DPO's primary focus should be compliance with the GDPR and playing a key role in fostering a culture of data protection within the organisation. Additionally, whilst an ability to 'influence' is not listed in the GDPR as a criterion for a DPO, given the seniority of the role and DPO's overarching objective to ensure compliance, the DPO should be involved in difficult conversations regarding business

requirements versus compliance. The ability to influence effectively in such situations can be paramount to the success of the DPO's role.

Half a year after the GDPR came into force, I still get frequent enquiries from organisations asking me if they 'need' a DPO. In most cases what they are really asking is if they are legally required to have one. In fact, appointing a DPO is not mandatory in most circumstances. Upon hearing this, many organisations will simply discount the idea of appointing a DPO.

However, even when not legally required, a DPO would still be a very beneficial addition to virtually any organisation, by helping to improve their security stance as well as more easily maintaining compliance. Bodies such as the Information Commissioner's Office and European Data Protection Board strongly recommend organisations give serious consideration to appointing a DPO. In fact the ICO says: "even if you're not obliged to appoint a DPO, it is very important that you have sufficient staff, skills, and appropriate reporting structures in place to meet your obligations under the GDPR". Those that opt not to take on a DPO are urged to make a note of why they did not do so.

Conflicts of interest

The GDPR says that a DPO may fulfil other tasks and duties provided these do not result in any conflict of interest. The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. In each organisation, this has to be considered case by case.

As a rule of thumb, conflicting positions within the organisation may include senior management positions such as the CEO or Directors, and heads of marketing, HR, and IT. These roles have been identified as being non-compatible with the role of DPO.

How DPOs can help understand regulatory demands

Another of the most common points of confusion about the GDPR is what counts as a data breach and what must be reported to the authorities. Ironically, despite many organisations still trying to get away with the bare minimum activity to comply with the GDPR, the ICO has been inundated with breach reports.

At the Confederation of British Industry's (CBI's) fourth annual Cyber Security Conference in September, the ICO stated that it had been receiving around 500 calls a week from organisations that believed they needed to report a breach. However, as many as a third of these reports were completely unnecessary, with the organisations misunderstanding what constituted a breach.

Furthermore, the ICO found that organisations often tended to leave out crucial details in their reports, or else go the other way and write exhaustive and over-inflated reports that were full of unnecessary detail. Either way, this lack of understanding about the requirements serves to slow down the reporting process and creates more work for the ICO.

Alongside breach reporting, organisations have often been labouring under false pretences about data permission requirements. There was a great deal of press coverage about how the GDPR would impact marketing operations, and the common consensus was often that organisations would need to obtain permission for all their contacts or else delete their databases. This is not true in most cases. For example, it is perfectly fine to contact an existing customer with something that is legitimately likely to be of interest, if they are given a clear and easy path to unsubscribing.

Perhaps more importantly, the idea of consent for marketing contacts was not actually introduced by the GDPR. This is a requirement of the Privacy and Electronic Communications Regulations (PECR), which was put into law as far back as 2003.

Having an objective and experienced individual in the DPO role – whether as a fulltime in-house position or an external vDPO – can help organisations to understand their obligations and ensure they aren't needlessly hampering their business activities in ways the GDPR doesn't actually call for.

The race to catch up

Many organisations are still running through a backlog of activity required for compliance even so many months after the GDPR entered into law. For example, I am still routinely being asked to look over contracts made before the GDPR came into effect, to ensure that they comply. This can be very slow work and requires an experienced DPO with both legal and technical expertise. The ICO seems content to give these latecomers a bit more time to catch up, but with half a year already passed, it seems unlikely stragglers will be given much more leeway.

With many organisations already far behind on compliance, we are likely to see a large wave of fines and disciplinary action from the ICO in the next six months if organisations don't take the spirit of the GDPR to heart.