July 9, 2019

GDPR: One Year On

Attorneys
Clare Sellars

The Information Commissioner's Office has published GDPR: One Year On, describing its experiences and giving insights into the impact of the GDPR since 25 May 2018. The document reaffirms the ICO's risk-based approach to enforcement focussing on GDPR breaches involving highly sensitive information, large groups of individuals and vulnerable individuals. A key message, however, is that there is "*still a long way to go to truly embed the GDPR and to fully understand the impact of the new legislation.*"

The Information Commissioner's Office has published GDPR: One Year On, describing its experiences and giving insights into the impact of the GDPR since 25 May 2018. The document reaffirms the ICO's risk-based approach to enforcement focussing on GDPR breaches involving highly sensitive information, large groups of individuals and vulnerable individuals. A key message, however, is that there is "*still a long way to go to truly embed the GDPR and to fully understand the impact of the new legislation.*"

The Multistakeholder Expert Group (MEG), which supports the application of the GDPR and which was established in 2017 to assist the Commission in identifying potential challenges in GDPR application, also published a report contributing to the stocktaking exercise of June 2019 on one year of GDPR application. This notes various interesting issues, some of which are summarised below.

GDPR Awareness

According to the ICO, "*people have woken up to the new rights the GDPR delivers, with increased protection for the public and increased obligations for organisations*". Generally, the first year of GDPR has seen people realise the potential of their personal data, with 64% of recently surveyed DPOs stating that they had seen "*an increase in customers and service users exercising their information rights*". The increased understanding of and engagement with GDPR rights and responsibilities seems to have been reflected in the volume and nature of the ICO's contact and engagement with businesses, organisations and individuals.

The MEG notes that organisations have appointed DPOs where required and sometimes also voluntarily. Often SMEs are not required to appoint DPOs under the GDPR, but may be legally obliged to do so in some Member States (e.g. Germany) for other reasons, while in the pharmaceutical sector, health authorities tend to assume that DPOs will be appointed, regardless of the GDPR's requirements. Generally, organisations' experiences with appointing DPOs have been positive, although the market for experienced DPOs is immature and many non-experts are becoming DPOs very quickly thanks to the proliferation of new training courses. The ICO notes that in larger organisations, the GDPR has placed significant responsibility on DPOs. Most seem to feel that they have received good support within their organisations; however, almost 50% said they faced "unexpected consequences" resulting from the GDPR. Nonetheless, more than 90% had an accountability framework in place, and 61% reported that their framework is well understood in their organisation.

The ICO also acknowledges that "*it hasn't been easy for small organisations to become GDPR compliant*" and intends to establish a one-stop shop to support SMEs.

GDPR Guidance

The ICO is committed to updating its Guide to the GDPR, as required and to developing four statutory codes for data-sharing, direct marketing, age-appropriate design and data protection and journalism to support GDPR implementation. The age-appropriate design code, currently under consultation, sets out 16 standards which providers of online services and apps must meet when apps are likely to be used by children or when they process children's personal data. The data-sharing code will update the ICO's 2011 data-sharing code of practice (a draft will be subject to formal consultation this summer and laid before Parliament in autumn). Similar timetables will apply to the direct marketing and journalism codes. The former will be subject to review and updating, if required, once the new EU e-Privacy Regulation is

ATTORNEY ADVERTISING

completed. The latter will build on the ICO's previous guidance developed in response to the Leveson Inquiry and will involve input from press regulators.

Additionally, following its July 2018 Democracy Disrupted? report and subsequent guidance, the ICO favours a wider statutory code of practice for all organisations processing personal data for political campaigning purposes.

Enforcement

"*Enforcing the GDPR is not just about big fines; it's about using all the tools set out in our Regulatory Action Policy*" – the ICO says it will respond swiftly and effectively to breaches, focusing on those involving highly sensitive information, adversely affecting large groups, or impacting vulnerable individuals. Its aim is to be "*effective, proportionate, dissuasive and consistent*" in its application of sanctions, targeting organisations and individuals suspected of "*repeated or wilful misconduct*" or "*serious failures to take proper steps to protect personal data*".

The ICO also promises to be proactive in mitigating new or emerging risks arising from technological and societal change (e.g. relating to social media companies, political parties and data brokers). The ICO also intends to cooperate with other regulators regarding enforcement and regulatory action.

The ICO can now issue formal assessment notices to any organisations and has issued 15 so far in connection with its investigations into data analytics for political purposes, political parties, data brokers, credit reference agencies and others. It has also issued reprimands and warnings across various sectors (e.g. health, retail and finance). Eleven information notices have also been issued, allowing the ICO "*to progress our investigations and inform our action*". "No-notice" assessment notices should mean that the ICO can access companies' data protection practices faster and "urgent" information notices will "*assist with all fast-moving investigations*".

Incidence of Personal Data Breaches

The ICO confirms that, since 25 May 2018, it has received around 14,000 personal data breach (PDB) reports, compared with around 3,300 the previous year. Over 12,000 of these have been closed, only around 17.5% required action from the organisation and less than 0.5% led to either improvement plans or civil monetary penalties. The ICO believes this demonstrates that "*businesses are taking the requirements of the GDPR seriously and it is encouraging that these are being proactively and systematically reported to us*", although assessing and reporting breaches within the statutory time scales remains challenging. The PDBs have led to various outcomes. In some cases no further action was taken, while in others action was required from the organisation or the ICO.

Public Concerns

From 25 May 2018 to 1 May 2019, over 41,000 data protection concerns from the public were raised with the ICO compared to around 21,000 in 2017/18, indicating increased GDPR awareness. All categories of complaint have risen in proportion with the overall increased number of complaints. Subject access requests remain the most frequent complaint category, representing around 38% of complaints received. Inevitably, higher numbers of breach reports and concerns arise in some sectors than others, especially the health sector. The MEG also notes that there may be challenges in meeting deadlines regarding data subjects' rights requests and that responding to requests can be time-consuming.

The MEG observes that not-for-profit organisations entitled to enforce data subjects' rights under the GDPR have started bringing representative actions for infringements. Many are based on mandates from affected individuals and include both complaints to DPAs and requests for injunctions and compensation claims through courts. Some procedural hurdles to NGOs' bringing complaints apparently remain.

EU Figures

According to the EDPB, from 25 May 2018 to 1 May 2019, there were around 240,000 cases across the EU involving data protection complaints, breaches, proactive investigations or similar issues. The ICO received approximately 23% of these and is currently the lead supervisory authority on 93 such cases, while working on behalf of UK citizens to uphold

their information rights in 58 other cases. The ICO notes that its international strategy commits it to maintaining strong global links and continues to strengthen its ties with the EU supervisory authorities.

Enabling Innovation

The ICO notes that it will encourage innovation through its approach to regulation and engagement to help organisations comply with the GDPR. In March 2019 the ICO opened the beta phase of its regulatory Sandbox, a new service designed "*to support organisations using personal data to develop products and services that are innovative and have demonstrable public benefit*". This should help participants to work through how they use personal data in their projects to ensure GDPR compliance. Last year the ICO also introduced a Research Grants Programme to promote good practice and support independent, innovative research and solutions focused on privacy and data protection issues to help deliver long-term improvements to information rights (in 2018, grants were awarded to four organisations).

The MEG observes that some aspects of the GDPR (e.g. data protection by design) may encourage innovation, but others and the threat of administrative sanctions may discourage it if applied strictly. Some organisations are concerned that strict interpretation of the GDPR regarding automated individual decision-making and profiling and applying the GDPR to new technologies (e.g. blockchain or AI) may impede innovation. The MEG also notes that the GDPR's impact on the pharmaceutical sector will depend on interpretation of fundamental provisions regarding scientific research and processing of health data and also whether Member States will differ in their implementation of significant issues regarding processing of health data.

Data Subjects' Rights

The MEG observes that, while many organisations have taken considerable steps to implement the GDPR's transparency and information requirements, it remains hard to know how detailed privacy notices should be and how to provide the information. The report notes failure to comply with information obligations and lack of clarity in data protection notices in some cases.

Some individuals request copies of their personal data plus the original documents on which such data are based, and the exercise of access rights in employer-(ex)employee relationships can be difficult. Verifying data subjects' identities can be challenging, and clarification regarding age verification for children would be welcome. Some organisations have also reported malicious use of rights.

Consent

The MEG notes that certain miscommunications have led to individuals erroneously believing that consent is required for all data processing. Many organisations now choose to rely on a legal basis other than consent for future processing, if available. Not all consents obtained in online environments fulfil the GDPR's requirements, and some companies continue to track users online and through devices without valid consent.

The GDPR's parental consent requirements remain a concern, with information provided to data subjects who can consent often being unclear. Some organisations allow children to consent themselves where possible, or rely on a different legal basis for processing (this raises concerns in the context of digital platforms, as there is a risk that this may effectively sidestep the GDPR's requirements regarding children's consent in respect of information society services, and lead to unintended fragmentation across Europe).

The MEG notes that the finance/insurance industry has specific difficulties on requesting explicit consent for processing health-related data in insurance contracts where such processing is necessary to execute the contract correctly, leading to different approaches between Member States on the legal basis for processing health data in a reinsurance context and for fraud prevention/detection. The MEG also observes that small enterprises are not yet adequately aware of the need for free consent and the consequences of tied consent. In particular, forced consent or contractual bundling of consent appears to arise in the tech industry.

ATTORNEY ADVERTISING

Accountability and Risk-Based Approach

The MEG confirms that many organisations have tried hard to implement the GDPR. This requires considerable initial effort, but contributes to improved data management and structure and can make data protection a brand asset. Some SMEs and public bodies especially have struggled with implementing accountability, which requires greater human resources and work to implement compliance mechanisms and provide staff training. Documentation can become administratively burdensome, with requirements not being explicit regarding content, level of detail or form.

Generally, the risk-based approach has been received positively and awareness of the need for DPIAs is growing; however, some organisations can only process these at a limited rate and are unclear as to when they are required.

The MEG observes that many organisations have made significant investments to upgrade and implement their IT and data management systems to comply with GDPR requirements (e.g. regarding security) and in GDPR-related human resources and staff training.

The Controller/Processor Relationship

The MEG notes that some organisations believe the distinction between controllers and processors is still unclear, with some former processors now wanting to become controllers or joint controllers (sometimes, contractual designation of controllers and processors appears to be determined by the preference of the strongest company, rather than who decides the purposes of processing). Further, the scope of what constitutes a processor can be unclear and further EDPB guidance would be welcomed.

Re-negotiating controller-processor contracts is often time-consuming and depends on the contracting parties' understanding of the GDPR. Some organisations have included provisions going beyond those required by Article 28, included additional commercial provisions, or changed the parties' liability positions.

Some organisations recommend adopting standard contractual clauses for processor contracts (this could assist especially SMEs who lack resources to negotiate individual processor contracts). Others support non-mandatory standard contractual clauses or templates of minimum requirements for data-processing agreements. Some organisations believe standard contracts are unnecessary, while others favour various possible clauses to be selected to best reflect the parties' commercial relationship, or standard clauses for specific processing situations. Organisations also appear divided over the content of standard contractual clauses. Some organisations are seeking clarification of various additional issues, and some favour new standard contractual clauses for the processor/sub-processor relationship, or at least clarification of certain issues through clauses. Some recommend a flexible structure, while others recommend adapting the existing standard contractual clauses for international controller to processor transfers.

Standard Contractual Clauses for International Transfers (SCCs)

The MEG observes that many organisations believe that the SCCs could be improved and made more flexible and would welcome clarity on specific aspects (e.g. onward transfers). Sector-specific clauses have also been suggested. Many believe that the existing SCCs should be amended to better reflect the GDPR, especially to take into account the controller-processor relationship while providing for flexibility to reflect the circumstances and relationship between the parties. Processor to sub-processor clauses are highlighted, as well as clauses for other situations (e.g. EEA processors to non-EEA controllers). Various issues requiring further clarification have been suggested (e.g. relations with sub-contractors). Many organisations view SCCs as essential to justify international personal data transfers and are concerned about their possible invalidation (various improvements have been suggested to guard against this).

Comment

The GDPR has clearly increased citizens' awareness and understanding of data protection. Not surprisingly, many organisations appear to have appreciated the significance of the new legislation, although possibly not always its full impact. The ICO notes that the focus for the second year of the GDPR "*must be beyond baseline compliance – organisations need to shift their focus to accountability with a real evidenced understanding of the risks to individuals in*

ATTORNEY ADVERTISING

the way they process data and how those risks should be mitigated. Well-supported and resourced DPOs are central to effective accountability." Although the MEG notes concerns that some DPAs may lack effective resources to perform their new tasks, the ICO at least has developed to accommodate its new powers and responsibilities (e.g. expanding its workforce significantly and increasing its fee income by 86%). Going forward, the ICO will focus on various regulatory priorities (e.g. cyber-security) and acknowledges the UK's ability "*to take on a leadership role within the global privacy and information rights community*". While the ICO appreciates what has been achieved since 25 May 2018, clearly there is still much left to do.

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have. © 2019 Ropes & Gray LLP

ATTORNEY ADVERTISING