May 25, 2018

GDPR is here: the dawning of a new era?

May 25, 2018. The sun rose as usual, the clocks did not stop, the sky did not go Armageddon-black, and, of course, GDPR became effective. Were you ready? Any loose ends? All GDPR-compliant contracts with processors in place? All pre-GDPR consents to processing checked and, if necessary, renewed? All data protection impact assessments done for current processing operations likely to result in a high risk? Breach notification procedures drawn up, staff trained, the DPO who had a nervous breakdown replaced? Are you granular and transparent? Are you fully "accountable". If not, perhaps you've left it too late. But now it's a case of better late than never and those still striving to be fully GDPR-compliant are unlikely to be publicly pilloried or the first to be fined up to 2% or 4% of global turnover. When it comes to compliance priorities, high risk operations take precedence as they will for the national data protection authorities when enforcing the new laws. In view of this, it helps to appreciate what those priority areas are. We consider some of these below.

Of course, GDPR has a defined territorial scope, and many organizations outside of Europe may not fall within its purview. For those controllers and processors subject to GDPR, the past 18 months have likely been spent processing the guidance of the national data protection authorities and Article 29 Working Party, proposed or final, and assessing their relevance to their data processing and gearing up in terms of technical capacity and appointment of personnel to deal with the new laws.

Impact assessments

DPIAs, for example, are mandatory for certain types of processing and for any other processing that is "*likely to result in a high risk to the rights and freedoms of natural persons*". The UK's data protection authority, the ICO, has stated it will expect a DPIA to be carried out by any organisation that plans to use new technologies to process personal data, or to match data or combine datasets from different sources, for example. For organisations that already carry out PIAs in accordance with the ICO's PIA Code, the ICO reassuringly suggests "the new process will be very familiar". Data controllers are encouraged to see DPIAs not only as an insurance policy against reputational damage resulting from failure to identify risks that ultimately become realities, but also against being seen not to care sufficiently in the post-Cambridge Analytica world about individuals' fundamental rights. DPIAs can therefore also be a means of fostering trust and potentially gaining competitive advantage.

Legitimate interests

The concept of legitimate interests is also not new and while the GDPR provides more detail, the rules are essentially the same as under the previous data protection regime. The main change is that any decisions taken on using legitimate interests as a basis for processing should be documented, and information on the decision should be set out in the privacy policy. GDPR transparency dictates that individuals should be made aware of the basis for processing and their rights, including their right to object to the processing. In light of the potential difficulties obtaining valid consent may present, data controllers may see legitimate interests as the go-to justification for the processing of personal data. The basis should not, however, be seen as a general panacea and should be balanced not only against the rights, but also the expectations of the individual.

Consent

As regards consent, the GDPR sets higher standards in relation to "regular" and "explicit" consent, which may require data controllers to alter their practices and change the way they request consent for data processing. Consent under GDPR requires a clear affirmative action. If a controller finds that the consent previously obtained under the Data Protection Directive is not GDPR-compliant, then it may want to assess whether the processing may be based on a different lawful basis under the GDPR. This can be done on a one-off basis as controllers move to the new regime. Otherwise, non-compliant consents may need to be refreshed. Under GDPR, a controller relying on consent as its basis for processing should be able to demonstrate that valid consent was obtained: presumed consents of which no references are kept will need to be renewed for further processing. The Article 29 Working Party (WP29), which will become the European Data Protection Board, has discussed some golden rules: consent should not be bundled up as a non-negotiable part of terms and conditions; several purposes for processing require separate "granular" consents; consent for special category data must be "explicit"; withdrawal of consent should be as easy as giving it; employee consent is unlikely to be valid in many circumstances.

Data breach notification

The WP 29 advises both controllers and processors to have in place processes to be able to detect and promptly contain a personal data breach, to assess the risk to individuals, and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate any high risk breaches to the individuals concerned. Failure to notify could mean a substantial fine. And beware the knock-on effect: failure to notify a breach could reveal either an absence or an inadequacy of security measures which might attract a further sanction.

Joint controllers are required to determine their respective responsibilities for GDPR compliance and contractual arrangements; joint controllers may need to include provisions that determine which controller will take the lead or be responsible for breach notification. A controller may need a breach response plan that caters for potential breaches affecting the personal data of individuals in more than one Member State, by assessing the lead supervisory authority that it would notify. While the controller has ultimate responsibility for assessing risk associated with a breach, a processor who becomes aware of a breach must notify the controller without undue delay.

Controller and processor

Also not new is the requirement for a contract between controller and processor. The level of detail and mandatory terms under the GDPR, however, represent a significant change. Controllers were urged by regulators last year to check contracts with processors, negotiate and implement changes where necessary. For those with large numbers of non-EU processors, this may not have been as straightforward a task as some regulators appeared to suggest.

Transparency

Transparency is key. Information or communication with individuals should be concise, transparent, intelligible, easily accessible and in clear and plain language. Changes to the contents or conditions of existing privacy notices, the WP29 suggests, should be communicated by way of an appropriate modality, the emphasis being on the layering of information and the use of "push" and "pull" notices such as ad hoc just-in-time notices and privacy dashboards. In particular, data controllers who carry out profiling and automated decision-making should consider proactively engaging with individuals whose data they are processing by providing clear information about how their data is being used and how the processing might affect them.

Accountability

Closely linked to transparency is the new GDPR principle of accountability which in broader terms requires controllers and processors to demonstrate GDPR compliance. In many larger organisations, the embodiment of the principle will be the DPO and the privacy management framework that the DPO oversees. Although, for example,

recording processing activities and maintaining clear records of consent are specifically called out by GDPR, failure to keep such records could also indicate a lack of accountability, as could undue delay in dealing with subject access requests or failure to carry out a DPIA when necessary.

Data portability

The GDPR, as everyone knows, brings with it new rights for the individual including a right to data portability which applies to processing operations that are based on consent or a contract with the individual concerned. For controllers, the right is potentially onerous insofar as it requires technical capabilities not just to identify and retrieve personal data efficiently, but to allow onward transmission to another controller while guaranteeing the security and integrity of that data, something that will require a degree of standardisation and cooperation within organisations and the particular sectors in which they operate.

What now?

One can only hope that the GDPR compliance frenzy now abates but there may be concerns that we are only entering the eye of the storm with national data protection authorities poised to unleash a typhoon of massive fines on non-compliant organisations. This is of course unrealistic. Fears may not subside until one or more of the regulators has shown its hand in that regard, but as the UK's Information Commissioner has said repeatedly and as echoed in the ICO's draft Regulatory Action Policy currently open to consultation, regulatory action will be targeted and proportionate focussing on the most serious cases involving high-impact, intentional, wilful, neglectful or repeated breaches. Additionally, the ICO has openly acknowledged, recently through James Dipple-Johnstone, Deputy Commissioner for Operations at the ICO, that its ability to levy fines will be hampered "unless we have the powers to move at pace and obtain the information and evidence to determine what's happened", so the regulators have their challenges too as GDPR takes hold for all.