GDPR in Context: Internal Privacy Audit and Gap Analysis

Background

The General Data Protection Regulation (the "**GDPR**") will come into effect on 25 May 2018. The GDPR will be directly effective in each EU member state, with the aim that the same rules will be applied uniformly within the EU. This marks a shift in the approach to data protection at a European level, which until 25 May 2018 will rely on national implementing legislation in each EU member state.[1]

The period between now and 25 May 2018 is therefore the de facto transition period, during which organisations will need to assess their current approach to data protection, to undertake a gap analysis between that current approach and the requirements under the GDPR, and to implement any changes and improvements which are required to achieve demonstrable compliance with those GDPR requirements.

The privacy audit

The significant strengthening of data protection rules which is inherent in the GDPR, and in particular the sanctions under the GDPR, emphasise the need to ensure that each organisation has full insight into the data flows concerning the customer, employee and other personal data which it controls, and that it puts appropriate notifications, consent capture arrangements, processing agreements, transfer arrangements and security arrangements in place.

The starting point for any GDPR compliance project is therefore an understanding of the "what, why, how and where" of current personal data processing by each organisation, and where appropriate by department or business line within the organisation. What personal data is held and used, why the organisation needs and uses it (which may not necessarily be the same thing), how the personal data is processed and shared, where it is stored and from where it is accessed – all of these are important questions to be answered before it will be possible to undertake the necessary gap analysis.

Organisations should therefore commence with an audit of their existing databases and uses of personal data, which can be framed around a detailed fact finding questionnaire. The purpose of the questionnaire is to assist the organisation in understanding its current universe of data and of data processing, as a first step to identifying remedial actions which will need to be taken to ensure GDPR compliance. The questionnaire should ideally be framed in a broad manner, to elicit as much information as possible in relation to potential uses (which is to be understood in its broadest sense) of personal data by an organisation. This is reflective of the fact the GDPR is broadly drafted, both as to the information caught within the definition of personal data and the many processing activities which can be applied to the personal data.

Large organisations should consider whether it is appropriate to answer the questionnaire at a legal entity level, or at a business unit or department level. There may be a benefit in obtaining information at a business unit or department level, as this may result in identification of assumptions or misapprehensions of other business units or departments as to uniform treatment of personal data across the organisation, and / or additional training requirements.

---

[1]There will be national implementing legislation with regard to certain elements, in particular the sanctions regime. However, the general principles which govern the processing of personal data by both controllers and processors will apply automatically from 25 May 2018.

Internal Privacy Audits and Gap Analysis

The key elements of the privacy audit

Personal data – scope, uses and disclosures

The GDPR reformulates the data protection principles which are set out in the DPA, with greater emphasis on transparency and accountability, requiring that data controllers implement privacy "*by design and by default*" and in a manner which enables them to demonstrate compliance with the GDPR. In practice, this means that organisations will need to be in a position to show that they have considered the privacy impacts of their collection, use and sharing of personal data, and that they have factored those impacts, and the associated risks to individuals, into the development and ongoing procedures relating to their products, services and systems.

Under the GDPR the definition of personal data has also been clarified. Personal data essentially captures all information from which an individual can be directly or indirectly identified, and the GDPR includes express reference to identifiers, including location data, online identifiers etc and factors specific to eg, the cultural or social identity of an individual. For this reason, the questionnaire should request a broad range of information relating to various categories of individuals, so that the organisation can establish as broad a view as possible of the personal data which is holds. All possible processing operations which can be applied to the personal data will be caught under the GDPR, and "use" in the context of the questionnaire should therefore be considered as including all forms of use, including for example and without limitation, recording, amendment / adaptation, sharing and deletion, etc.

Transparency as regards the use (in the broad sense referenced above) of personal data is a key element of the GDPR, and therefore the questionnaire should seek to identify how and from whom personal data is gathered, as well as the information which is given to individuals in relation to the organisation's use of the personal data. Because an organisation may hold personal data relating to different categories of individuals (eg, employees, customers etc), and because the manner in which the personal data relating to the various categories is collected and used, and the manner in which individuals within the category are informed of the use, may all vary, the questionnaire should distinguish between, and seek to elicit the relevant details by reference to, categories of individual.

Security is another key pillar of the GDPR, and is inherent in the "by design and by default" philosophy underpinning it. Therefore, the questionnaire should include specific queries aimed at both the specific security measures which are applied to personal data or categories of personal data in practice, as well as overall security policies and procedures. In this and other regards, the questionnaire may approach important issues from a number of perspectives, which should assist the organisation in assessing its activities holistically and in identifying gaps between policy and practice.

Rights of individuals

While individuals have a number of data protection rights under the DPA, the GDPR will extend the number and scope of individual rights. While none of these rights are absolute, it is necessary to understand what, if any, processes and procedures the organisation has in place to consider and manage requests to enforce these rights, as well as the extent to which individuals are already aware of existing rights in order to assess changes which may be required to ensure compliance with the GDPR. The questionnaire will therefore need to interrogate the processes and procedures which are already in place, so that changes to existing and / or additional procedures can be identified.

Systems and security

In order to ensure compliance with the "by design and by default" principles in the GDPR, it will be necessary to assess and understand where information is currently held, how it can be accessed, used on and shared through, and, very importantly, how it is protected on, networks and IT systems and devices. Accordingly, these details should be sought through the questionnaire.

Internal Privacy Audits and Gap Analysis

Data protection officer

Under the DPA, the appointment of a Data Protection Officer ("**DPO**") is not mandated. Under the GDPR, the appointment of a DPO will be required, however, where (i) the processing is carried out by a public authority or body (with the exception of the courts); (ii) where the core activities of the organisation consist of (a) processing operations which require regular or systematic monitoring of data subjects on a large scale; or (b) processing large amounts of special categories of personal data. The responses in relation to the scope and uses of personal data will help establish whether a DPO will be required under the GDPR. However, it will also be necessary to identify whether a DPO has already been appointed, and if so, the terms of reference for the DPO.

Policies, procedures and documentation

In line with the accountability principle under the GDPR, each organisation, whether acting as a controller or processor of personal data, should document and retain records in relation to relevant processing activities, and implement appropriate policies and procedures which will assist in demonstrating compliance. The questionnaire should therefore seek details of existing policies and procedures which may be leveraged for GDPR compliance, and should also enable the organisation to identify additional policies and procedures which may be of benefit to it in seeking to demonstrate compliance going forward.

Next steps

The scope of any privacy audit required by an organisation will clearly be a function of the nature of the business conducted by that organisation, including the extent to which it uses and processes personal data in the course of its business. However, it is unlikely that any organisation will be fully immune from the scope of the GDPR, and while the risks will increase incrementally with the scale of personal data processing use and processing, every organisation should have GDPR compliance on its radar. Undertaking an internal audit of existing databases and uses of personal data, framed around a detailed questionnaire, should be the starting point for understanding the potential implications for, and actions required by, an organisation.

Contacts

Anne-Marie Bohan
PARTNER
D +353 1 232 2212
E anne-marie.bohan@matheson.com

Deirdre Kilroy
PARTNER
D +353 1 232 2231
E deirdre.kilroy@matheson.com

Chris Bollard
PARTNER
D +353 1 232 2273
E chris.bollard@matheson.com

Carina Lawlor
PARTNER
D +353 1 232 2260
E carina.lawlor@matheson.com

Christine Woods
ASSOCIATE
D +353 1 232 2147
E christine.woods@matheson.com

12.10.17