GDPR in Context: Data Controller Accountability

Background

The General Data Protection GDPR (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.

Overview

The GDPR does not, for the most part, introduce wholly new compliance principles on data controllers. What it does, for the most part, is build on existing principles to form the backbone of a more robust statutory framework as a means of ensuring that data protection is given the attention and importance that the EU institutions and data protection supervisory authorities believe it deserves.

Perhaps the biggest shift introduced by the GDPR is that accountability is the new compliance, and much of the preparation for controllers for May 2018 is to adopt accountability measures to achieve greater security and trust around processing. The principle of accountability pervades all of the primary obligations of controllers under the GDPR and the objective is to implement a holistic compliance programme for their data processing activities.

Controller compliance requirements - common elements

Before considering some of the specific compliance requirements, it is worth noting certain common themes or elements. These advocate a risk based approach with the data subject at its centre, so controllers will need to assess any risks to individuals posed by their processing activities and what measures they need to take to address them. The requirements also identify common factors for controllers to take into account when making those assessments, like the state of the art, the cost of implementation and the nature, scope and purposes of data processing. It is clear, therefore, that there is no 'one-size fits all' and that controllers are given a wide discretion as to how to achieve compliance.

[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.

Data Controller Accountability

Data protection by design and by default

The principle of data protection (or privacy) by design, is that privacy controls are to be embedded in the design of business operations, processes, products and services. The principle of data protection by default contemplates controllers applying the strictest privacy settings, for example, to a product or service. The aim is that controllers prevent, as far as possible, privacy risks occurring.

Ideally all aspects of the data lifecycle within an organisation (the collection, use within the business, disclosure to third parties, retention and ultimately destruction of data) should be designed around data subjects. Controllers should analyse whether their systems, processes and procedures are appropriate to allow data subjects to exercise their rights. This would include, for example, reviewing the means of data collection, whether marketing preferences are respected and whether data can be easily identified and packaged to enable data portability.

Standards based approach

A common theme that runs through the GDPR compliance obligations is that adherence to codes of conduct or approved certifications can be used as a factor in demonstrating compliance. Consistency of laws across Member States was the primary driver for the new regime being implemented through a regulation rather than a directive, so it would seem likely that there will be an emphasis at the EU and supervisory authority levels on developing and adopting uniform codes and certifications (at least in regulated sectors and those businesses that are either significant data users or data producers).

Data protection governance

Looking at the various requirements on controllers 'in the round', the aim of the GDPR (and what supervisory authorities will likely expect to see) is for organisations to implement a formal data protection programme within their organisation. This will include (in addition to the actions outlined below) staff education, identifying key stakeholders to support the programme, allocating responsibility for compliance and identifying formal data protection reporting lines up to the top level of management level.

Among the key controller obligations which controllers need to consider are:

- the more explicit obligations on controllers to **communicate** with data subjects regarding the processing of their personal data, and their rights in relation to that processing, in a **transparent manner**, in concise, intelligible and easily accessible for, and using clear and plain language;

  This will require comprehensive review of subscription and application forms, prospectus disclosures and any relevant website terms and conditions, as well as a consideration of any other methods through which personal data is collected;

- the additional and specific requirements relating to the manner in which **consent** is collected from a data subject, such that consent must be obtained on a purpose by purpose basis, using clear and plain language, in circumstances where in order to be valid, the consent must be an **unambiguous** indication of the individual's wishes, by a statement or clear and affirmative action, and individuals must be informed that they **may withdraw** their consent at any time. Accordingly, the circumstances in which consent may be relied upon to legitimise processing will be narrower, and where consent is to be relied upon, there will be an impact of how this is communicated to individuals when collecting information, etc;

- where a **legitimate purpose** of the controller is relied upon as a legitimate processing ground, the requirement that the individual be told of the justification for the processing and of his or her additional **rights to object**, to restrict processing and to have data erased;

- the continuing obligations to implement appropriate technical and organizational measures, which may include pseudonymisation and encryption, to ensure a level of security appropriate to the risk to the rights and freedoms of individuals associated with the processing activities, the controller having undertaken a risk assessment as the varying likelihood and severity of the risks which considers the state of the art, the costs of implementation of the measures, and the nature, scope, context and purposes of the processing.

  The GDPR gives some colour as to the factors controllers can take into account when assessing risks posed by their processing activities and the measures they can adopt to address them. They include pseudonymisation and encryption of data, proper diligence of processing systems and services and having embedded processes for regular testing, assessing and evaluating security measures. While there may be a tendency to focus on IT related security and protections against cyber attacks, it is worth keeping in mind that the vast majority of data security breaches still result from human error. An equal focus should be kept on having appropriate processes and regular training as a result. Steps controllers can take in order to move toward compliance with security requirements under the GDPR include regular updating of firewalls and software penetration testing, stricter user access control management, encrypting portable devices, greater emphasis on compliance and enforcement of internal policies and assessing physical security for premises and IT hardware;

  - increased focus on the responsibility of controllers in **choosing processors** which provide sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the GDPR requirements are met and the rights of data subjects are protected, and in ensuring ongoing compliance by those processors;

  - the additional requirements in relation to **processing contracts**, which will necessitate a review of all processing arrangements (including, in particular, administration agreements) currently in place, to ensure all newly mandated provisions are incorporated;

Data Controller Accountability

- the continuing restrictions on the transfer of data from the EU combined with a clear statement that only the European Commission may determine whether a third country or international organisation ensures an adequate standard of data protection.

  Organisations will still be able to rely on model clauses as a valid means of transfer and the GDPR provides a list of other valid transfer mechanisms, including the potential for approved codes of conduct and certification mechanisms, provided there are binding and enforceable commitments of the controller or processor in the third country. Helpfully, the GDPR also mentions the possibility of model clauses between data processors, which do not exist at present. The GDPR also specifically sets out clear provisions on requirements and procedures in relation to binding corporate rules ("**BCRs**") for the first time, which may simplify the current lengthy approval process with data protection authorities;

- the additional and / or expanded **data subject rights** under the GDPR, including rights to object, to restrict processing, data portability and the "right to be forgotten", as well as **shorter timeframes** for compliance with data subject access requests;

- **mandatory data breach notifications** to the supervisory authority, within 72 hours, unless the breach is unlikely to result in risk to the rights of individuals, and to individuals without undue delay, where the breach is likely to result in a high risk; and

- the requirement, in most circumstances, to maintain more **extensive records** of processing activities, including the purposes of the processing, the categories of data subjects, personal data, recipients (including in third countries), any transfers of personal data abroad, including documentation of suitable safeguards, timelines for erasure of data, and where possible, a general description of the technical and organisational security measures applied to the processing activities. To comply with the record-keeping requirements, controllers should aim to have a centralised data processing register that gives a fuller picture of the controller's internal and external processing activities. This would include, for example, a map of data flows through the data lifecycle, an inventory of the types and uses of data, and the preparation and implementation of relevant policies for each of them (including contract management for data processors).

In appropriate circumstances, controllers may be required to:

- undertake pre-processing data protection or privacy impact assessments ("**PIAs**"), which are required if the processing is likely to result in a high risk to an individual's rights, and which may require pre-processing consultation with the relevant supervisory authority. Such high risk processing includes profiling, large scale processing of sensitive categories of personal data, and may arise where there is innovative use of technological solutions;

  In addition, transfers of personal data outside the European Economic Area ("**EEA**"), while not specified in the GDPR as high risk per se, have been identified by the Article 29 Working Party as amongst the factors which may be indicative of high risk. Whether a PIA may be required will therefore be a relevant consideration in the context of any offshore outsourcings by service providers; and

- appoint a data protection officer ("**DPO**"), which will be required, inter alia, where the processing: (i) requires regular and systematic monitoring of data subjects on a large scale; or (ii) involves processing large amounts of sensitive data or personal data relating to criminal convictions and offences.

  Organisations are free to appoint DPOs even if not required to do so under the GDPR, but if they chose to do so, all DPO related provisions in the GDPR will apply.

Data Controller Accountability

Next steps

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 customer data and other personal data which it controls, and that it puts appropriate notifications, 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. At a minimum, for controllers, this will require a review in advance of 25 May 2018 of all data collection methods and terms, the basis upon which they legitimise their collection and use of data, privacy policies and statements, website terms, processor and data transfer agreements, and procedures to comply when individuals exercise their rights, to enable controllers to demonstrate compliance with their obligations under the GDPR.

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