GDPR series: new obligations on data processors

Laura Dietschy, Associate with Cooley (UK) LLP, considers how organisations will need to change their existing data processing practices to comply with the new obligations on data processors under the GDPR

From 25th May 2018, the General Data Protection Regulation ('GDPR') will impose statutory obligations on processors and give data protection regulators direct enforcement powers against them, with potentially serious fines for non-compliance. Data subjects will be able to issue claims against processors for any damage caused by a breach of the GDPR. This will be quite a contrast with the current regime of the Data Protection Directive (95/46/EC) ('EU Directive'), which is mostly aimed at data controllers who are responsible for ensuring their data processors' compliance with data protection laws through contractual obligations.

In view of the broad definition of personal data under the GDPR and the fact that a processor is defined as anyone who handles personal data under the instructions of a controller, these obligations will affect a great number of organisations and entities ranging from Software-as-a-Service and cloud providers to marketing and payroll specialists. This article considers how such organisations may need to change their existing data processing practices, and what steps they should take to comply with the new obligations on processors under the GDPR.

Current legal framework

The EU Directive established data protection principles governing the way personal data should be handled. Under the EU Directive, processors (and sub-processors) were prohibited from processing personal data except in accordance with the instructions of the controller or the requirements of applicable law, and subject to appropriate security measures. Whilst these obligations and principles remain under the GDPR, they have been greatly expanded upon and strengthened. Categorised below are the key new processor obligations under the GDPR

Accountability and transparency

The GDPR emphasises the need for all organisations to be transparent and accountable in their data processing operations and to keep a record of their processing practices. In practice, this will mean detailed and adapted policies and procedures must be established to illustrate processors' data flows and processing practices and to document any decision-making reasoning relating to personal data. This may include putting in place internal data protection policies, staff training, internal audits of processing activities, and reviews of internal HR policies.

The record keeping requirement will include documenting the processor's processing purposes, data sharing and retention of data, as well as security measures in place.

Article 30(2) of the GDPR requires processors to keep an up-to-date record of all categories of processing activities carried out on behalf of a controller. These records should contain the name and contact details of the controller on behalf of which the processor is acting, any sub-processor (and their respective representatives, if applicable), and the categories of processing carried out for each controller by each (sub-)processor. The record should also document any transfers of data outside of the European Economic Area ('EEA') and the appropriate safeguards in place in relation to such transfers.

Governance and data security

Having comprehensive but proportionate governance measures in place will help demonstrate a processor's compliance with the requirements of the GDPR.

Processors have to implement 'appropriate technical and organisational measures' to ensure a level of security for personal data that is appropriate to the risk. The ways in which processors implement data protection by design and by default will depend on a case-by-case analysis of their processing activities.

These practices are likely to include data minimisation, pseudonymisation (where possible), allowing individuals to monitor the processing, and enhanced and up-to-date security features (e.g. encryption, confidentiality, integrity and resilience of processing systems and ability to restore personal

data in a timely manner in the event of an incident).

Processors should conduct regular security testing, assessments and evaluations of the effectiveness of their technical and organisational measures to ensure their processes evolve alongside the types of processing and data they process. Enhanced requirements apply to processors who process special categories of data and/or criminal conviction and offence data.

Processors should audit their systems and security measures and review their risk mitigation plans to ensure the appropriateness of their systems, networks and business practices in view of the type of data processed. They should set up, or update if already in existence, disaster recovery procedures to restore personal data in case of data breach or other security incident.

Adherence to an approved code of conduct or certification scheme will have a strong probative value in demonstrating that a processor has met its good governance and security obligations under the GDPR. No such codes or certification schemes have yet been approved and/or published by the relevant authorities, but some controllers (particularly in heavily regulated industries) may make them a condition-precedent to their contracting with processors in future.

"Adherence to an approved code of conduct or certification scheme will have a strong probative value in demonstrating that a processor has met its good governance and security obligations under the GDPR... some controllers (particularly in heavily regulated industries) may make them a condition-precedent to their contracting with processors in future."

Processors might then find that such schemes not only provide them with an efficient way of demonstrating their GDPR-compliance and therefore accelerating their sales cycles, but also give them a competitive edge on the market.

As part of the general overhaul of their data protection practices and processes, processors should review their template agreements with controllers and expect controllers to require that their current arrangements be updated by 25th May 2018, to ensure that they satisfy the new requirements imposed by the GDPR, as further detailed below.

Contractual requirements

Under the GDPR, processors must only process data upon the documented instructions of the controller (unless required to do so by Member State law), and immediately inform the controller in the event that they believe that such instructions conflict with the requirements of the GDPR (or other European Union ('EU') or Member State laws). Where a processor contravenes such obligations and determines the purposes of any processing activity itself, that processor will be treated as a controller in respect of that processing activity.

There must be a written agreement between the controller and processor, and the GDPR is rather prescriptive about what the agreement must contain. Processors should review their template agreements with controllers to ensure that they cover the following compulsory provisions: the subject matter and duration of processing; nature and purpose of processing; type of personal data and category of data subject in question; and the obligations and rights of the controller.

Under such data processing agreements, processors will have to impose confidentiality obligations on their authorised personnel processing the personal data; ensure the security of the personal data processed; implement measures to assist the controller in complying with data subjects' rights; return or destroy personal data when the agreement is terminated (upon the controller's instructions); and provide the controller with appropriate information for the controller to demonstrate compliance with the GDPR (which will often take the form of audit rights of the controller).

Under such an agreement, controllers will also ensure that processors abide by the rules relating to the appointment of sub-processors, as set out below.

Appointment of sub-processors

The processor must not appoint a sub-processor without the prior written consent of the controller. Any sub-processors must be appointed on the same terms as are set out in the contract between the controller and the processor and comply with the requirements set out above.

The original processor remains liable to the controller for the performance of the sub-processor's obligations. Processors who use sub-processors should therefore perform appropriate due diligence on sub-processors prior to contracting with them to ensure that the sub-processors are able to satisfy the contractual obligations in the agreement with the controller.

Data transfers to countries outside of the EEA

Under the GDPR, obligations relating to transfers of personal data outside

(Continued on page 8)

(Continued from page 7)

of the EEA will apply directly to processors, who can now have direct statutory liability in that regard. As stated above, processors can only process data on the instructions of the controllers, and this includes transfers of personal data to countries outside of the EEA (unless required to do so by Union or Member State law). Processors may only transfer personal data outside of the EEA to countries which have been determined by the European Commission to have adequate levels of protection.

If, upon the controller's instructions, processors wish to transfer personal data outside of the EEA to countries which are not recognised by the European Commission as having adequate levels of protection, they must put in place appropriate safeguards and ensure that data subjects can enforce their rights appropriately. This can be done for instance, either through the implementation of Binding Corporate Rules or standard data protection clauses (it is anticipated that the current form of Model Clauses will remain valid under the GDPR until repealed, amended or replaced). Approved codes of conduct and/or certification methods may also be implemented in future, therefore offering further safeguards processors might use to legitimise their transfer of personal data outside of the EEA.

Data breach notification

Processors must notify controllers without undue delay after learning of a data breach. It is recommended that the timeframe for, and circumstances giving rise to, the report of such breach be set out in the agreement between controller and processor. Processors should also set up mechanisms by which they can detect and report data breaches, including by implementing a security breach response plan and creating a response team. In line with their accountability and transparency obligations, processors should document any security incidents and breaches, and any action taken as a result, as well as the reasoning that led to this action being taken.

Data processing impact assessment, EU representative and Data Protection Officer

It is worth noting that under certain circumstances, processors may have to assist controllers in conducting data processing impact assessments and/or designate a representative in the EU if they are not established there. Processors should appoint a Data Protection Officer if they conduct regular and systematic monitoring of data subjects, or process special categories of personal data on a large scale.

Cooperation with supervisory authorities

Processors (and their representatives, if any) are required to cooperate, on request, with supervisory authorities in the performance of their tasks. Under the current regime, processors are not required to interact with data protection authorities.

Conclusion

Processors acting in breach of their new obligations under the GDPR may be subject to civil and administrative or criminal penalties, and/or damages in proceedings brought by supervisory authorities or data subjects. Fines imposed by supervisory authorities may be as onerous as 20 million euros, or four per cent of total annual worldwide turnover (whichever is greater).

The extent to which supervisory authorities will enforce processors' obligations under the GDPR is yet to be seen. However, updating personal data processing standards in line with the spirit of the GDPR, and in particular setting up record keeping habits and good governance measures now, is likely to provide processors with a definite competitive advantage in any event.

Laura Dietschy
Cooley (UK) LLP
ldietschy@cooley.com