Challenging times ahead for data processors

Bridget Treacy, Partner at Hunton & Williams, ***discusses the obligations on data processors as set out in the draft Data Protection Regulation, including the challenges for processors presented by the Regulation as currently drafted***

Much has already been written on the proposed EU Data Protection Regulation, but there has been very little focus on the fundamental changes to the responsibilities and liabilities that the Regulation seeks to impose on data processors. Currently, a processor has no direct responsibility or liability under the Directive (95/46/EC); the new Regulation introduces direct obligations and subjects processors to the same enforcement mechanisms as a data controller, including the possibility of substantial administrative fines of up to 24% of their worldwide turnover.

The essence of a processor's role

Determining whether a party is a 'processor' or a 'controller' is a fundamental distinction in European data protection law, not least because the Directive imposes direct responsibility (and liability) on a controller, not on a processor. The controller will usually allocate responsibility to a processor as a matter of contract.

Whether a party is a controller or processor can be a difficult assessment, frequently involving fine distinctions. In February 2010, the Article 29 Working Party published a widely anticipated 'Opinion on the Concepts of Controller and Processor' (www.pdpjournals.com/docs/88016). The Opinion's focus is on the role of the controller in ensuring data protection and therefore much of it is devoted to explaining how to determine controllership. The Working Party characterises the role of the processor as subsidiary to that of a controller, and emphasises that the existence of a processor is wholly dependant on a decision taken by a controller to delegate data processing activities to a third party. Thus, a processor needs to be a separate legal entity, and to undertake data processing activities on behalf of another, the controller. The Opinion is clear that whether or not a party is a processor is fact specific and depends on 'concrete activities in a specific context'.

Given the level of debate over the years as to the roles and responsibilities of a data controller versus a data processor, there was speculation that, in reforming data protection law, EU law-makers might remove the distinction altogether and instead impose responsibility on parties for the data processing activities they conduct. This has happened in many of the jurisdictions that form the Asia-Pacific Economic Cooperation. However, the current draft of the Regulation does not do this. Instead, it seeks to require the parties to establish the limits of their authority and authorisation, and to adhere to them.

Obligations imposed on processors

Chapter IV of the draft Regulation sets out the obligations imposed on both controllers and processors. Article 26 sets out the specific requirements where a controller seeks to delegate processing to a processor. These requirements, which must be imposed contractually, are similar to, but extend beyond, what is currently required under the Directive. Unsurprisingly, a key focus is on data security and a controller must chose a processor that provides sufficient guarantees to implement appropriate technical and organisational measures and procedures.

However, the security objective is expanded with the requirement that guarantees must be given 'in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'. This amendment apparently seeks to ensure that processors are able to deliver compliance across a broader range of rights, which are set out in further detail in Article 26(2). Yet the role of a processor is different to that of a controller and clearly there are aspects of the Regulation that processors cannot generally be expected to comply with. This provision is just one of several in which the role and responsibility of the processor require further consideration.

Contractual requirements

Article 26 also sets out requirements that must be reflected in the contract between the controller and processor.

(Continued on page 4)

(Continued from page 3)

These are more extensive that those currently required by the Directive.

There is a subtle difference between the wording of the draft Regulation and the Directive on the subject of whether a contract need be entered into between a controller and processor. The Regulation states (at Article 26(2)) that "*the carrying out of processing by a processor* shall be governed by a contract" (italics added); this can be contrasted with the requirement under the Directive that all data controllers must put in place processing contracts with their 'data processors'.

The significance of this distinction becomes apparent when you consider that processors can be penalised directly by data protection authorities for failure to comply with Article 26. The administrative sanctions in Article 79(6) impose the highest level of fine (up to 2% of annual worldwide turnover) for breach of the provision. These fines may be imposed on those who carry out processing, which includes the processor. Specifically, Article 79(6) permits the imposition of a fine not just on a controller but on anyone who, intentionally or negligently 'processes…personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26…'. Therefore, a processor could be subject to a sanction of the highest level if the controller fails to enter into a contract with it.

"There are many hundreds of thousands of services agreements and outsourcing contracts in the EU, most of which are unlikely to comply with the enhanced contractual requirements set out in the Regulation. Renegotiating such contracts to ensure compliance would take a lengthy period, certainly longer than the two year implementation period envisaged for the Regulation generally."

The specific requirements listed in Article 26 require that the processor will:

- act only on the instructions of the controller, in particular where the transfer of personal data used is prohibited;
- employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
- take all measures required in relation to the security of processing, as set out in Article 30;
- enlist another processor only with the prior permission of the controller;
- create, in agreement with the controller, the necessary technical and organisational requirements to enable the controller to comply with individuals rights set out in Chapter III (which deal with transparency, information, rights of access, rectification, the right to be forgotten, erasure, portability, the right to object and profiling);
- assist the controller in complying with Articles 30 to 34 (which deal with data breach notification, data protection impact assessments ('DPIAs') and prior authorisation);
- hand over results at the end of processing and not to process data otherwise; and
- make available to the controller and supervisory authority all information necessary to control compliance with the obligations laid down in Article 26 (see further below).

In addition, the controller and processor must document the controller's instructions and processor's obligations. If the processor processes personal data other than as instructed, the processor shall be considered a controller and subject to the rules on joint controllers, set out in Article 24.

Article 24 simply provides that where a controller determines the purposes, conditions and means of the processing jointly with others, the joint controllers shall determine their respective responsibilities for compliance under the Regulation. Thus, if a controller failed to give proper processing instructions, Article 26(4) may have the effect of transforming a processor into a controller. This may also occur where a processor inadvertently processes personal data, for example, because the processor does not realise that data contain personal data elements. It seems difficult to imagine that these consequences were intended.

The meaning of the last subsection of Article 26(2)(h), which refers to making available 'all information necessary to control compliance', is unclear. It appears to extend far beyond a general obligation to provide information, which sits awkwardly with the separate obligations in the Regulation that require the parties to maintain documentation recording processing operations, and permitting the supervisory authority to require information.

Overall, the Regulation envisages very detailed contractual provisions which would create a significant additional burden in many cases. A number of the issues listed in Article 26 are issues that will be covered by due diligence investigations between the parties in most cases, but which seem inappropriate as detailed contractual terms. Further, where data processing arrangements are complex, the relevant level of specificity may not be available at the time the contract is entered into, so that these provisions will need to be supplemented as the contract evolves.

At a practical level, the Regulation does not address the position of existing contracts, or make specific arrangements for transition. There are many hundreds of thousands of services agreements and outsourcing contracts in the EU, most of which are unlikely to comply with the enhanced contractual requirements set out in the Regulation. Renegotiating such contracts to ensure compliance would take a lengthy period, certainly longer than the two year implementation period envisaged for the Regulation generally. Further, as inevitably happens, once an agreement is re-opened, one or other of the parties will invariably seek to negotiate other terms; a process which could be very expensive for organisations. It is hoped that, at the very least, existing contracts will remain valid until the data processing activities changed, at which point new provisions could be negotiated.

"As a general observation, the Regulation does not clearly set out which provisions are applicable to controllers, which apply to processors, and which apply to both. The position is confused because some obligations are not attributed to either controller or processor, some are attributed to the controller, but then the supervisory authority can serve notices in respect of them on the processor, and others are referred to as being exercised by the processor 'on behalf of' the controller."

Maintain documentation

Both controllers and processors are obliged to maintain documentation of all processing operations for which they are responsible (Article 28(1)).

In particular, the Regulation sets out the following minimum requirements:

- name and contact details of the controller/joint controller/processor/representative;
- name and contact details of the Data Protection Officer ('DPO');
- purposes of the processing (including the legitimate interests pursued by the controller, where the processing is based on legitimate interests);
- description of categories of data subjects and categories of personal data relating to them;
- recipients or categories of recipients of the personal data;
- transfers of data to a third country or international organisation;
- general indication of the time limits for erasure of different categories of data; and
- description of the mechanisms referred to in Article 22(3), namely, the mechanisms that the controller uses to verify compliance with its obligations set out at Articles 22(1) and (2). In particular, these include documentation required under Article 28, data security requirements (Article 30)), DPIAs (Article 33), prior authorisation/prior consultations with supervisory authorities (Article 34) and designated DPO (Article 35).

There is also a general obligation on both the controller and processor to make the documentation available on request to the supervisory authority. There is an exemption to complying with this obligation for organisations with fewer than 250 employees whose data processing activities are ancillary to its main activities, and for natural persons processing data without a commercial interest.

A key difficulty here is that much of the information listed in Article 28(2) will be commercial information of the controller, not the processor, yet the obligation to maintain the information rests with both parties. Further, supervisory authorities may impose a fine of up to 1% of an enterprise's annual worldwide turnover where it intentionally or negligently fails sufficiently to maintain the documentation required by Article 28.

Processors' obligations unclear

The key obligations under the Regulation — i.e. the 'principles relating to personal data processing' listed in Article 5 — are clearly responsibilities of a controller. The grounds for processing (Articles 6 —10) also make clear that any basis for processing must be attributed to the data controller and not to the processor. The obligations of transparency (Articles 11—13) are imposed on the controller alone. The rights to information, access to data, rectification and erasure and other individual rights (Articles 14 — 21) are only exercisable against the controller. Yet, processors (as well as controllers and representatives, if any) are required to cooperate with the supervisory authority (Article 29 (1)), in particular, in connection with alleged breaches of the Regulation reported to the supervisory authority and the exercise of data subject rights.

Both processors and controllers are obliged to reply to requests of the supervisory authority relating to the exercise of data subjects' rights within a 'reasonable period' (to be specified by the supervisory authority) (Article 29(2)).

Thus, as a general observation, the Regulation does not clearly set out which provisions are applicable to controllers, which apply to processors, and which apply to both. The position

(Continued on page 6)

(Continued from page 5)

is confused because some obligations are not attributed to either controller or processor, some are attributed to the controller, but then the supervisory authority can serve notices in respect of them on the processor, and others are referred to as being exercised by the processor 'on behalf of' the controller. Clarity around which responsibilities are attributable to the processor would assist.

An example of this confusion may be seen in the context of subject access. Supervisory authorities may serve notices on processors where controllers fail to provide subject access. Yet none of the individual rights are exercisable directly against the processor, and the processor can have no liability for failing to comply with them. Allowing the supervisory authority to proceed against a processor may be appropriate as a secondary remedy where the controller has been required to deal with an access request but has failed to do so properly, but the processor should not be the primary recipient of such a notice.

Processor as joint controller

The provisions on joint controllership set out in Articles 24 and 26(4) do not sit well together. Article 24 contains the following wording: 'where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers…'. This implies that 'joint controllers' are controllers where two (or more) controllers jointly decide the purposes, conditions and means of the data processing. Further, joint controllers must determine their respective responsibilities for compliance with the Regulation by means of an arrangement between them.

This should be contrasted with the position of a processor which exceeds its authority or strays into controllership. Article 26(4) provides that 'if a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.' Here, the processor is not a 'joint controller' with the original controller, because the two have not decided the purposes, conditions and means of the data processing together. Nevertheless, Article 26(4) provides that the processor-turned-controller would be subject to the Article 24 requirement to allocate controllership responsibilities with the original controller.

Taken together, Articles 24 and 26(4) appear to mean that a processor which carries out relatively minor processing outside the scope of its instructions becomes subject to the obligations of a joint controller under Article 24. The outcome has unintended consequences as, presumably, the processor-turned-controller may approach the original controller and demand that the original controller agree with it the exercise of their 'respective responsibilities'. It may give unscrupulous processors a basis to put pressure on controllers by acting outside their remit. In most cases, this would be a breach of contract and it is not at all clear how a regulator would be able to enforce something that amounted to a contractual breach by the processor.

Conclusion

The Regulation is ambitious, seeking to implement wide-ranging reform across many aspects of data protection law. Some themes are relatively self-contained, but others, such as the role of the data processor, are nuanced and complex. It is only with careful reading and analysis of the proposed Regulation that the significance of the changes proposed for data processors becomes apparent.

The responsibilities and liabilities of processors will change fundamentally if the current proposal is enacted. Many processors will not have focused on these issues yet. It is to be hoped that they do so soon.

Thanks to my colleague Rosemary Jay for her contribution to this article.

Bridget Treacy
Partner
Hunton & Williams
btreacy@hunton.com