Compliance Complete
THOMSON REUTERS
ACCELUS™

January 17, 2013

# Increased liability for service providers under proposed data protection law

*By Bridget Treacy*

Changes to data protection law proposed by the European Commission, and currently under review by the European Parliament's LIBE Committee, will impose significant additional obligations on data processors, and allow fines of up to 2 percent of worldwide turnover.

Despite the fact that these changes will have a fundamental effect on the risk assessment of every outsourcing and services agreement, they have received relatively little attention. Businesses must, however, begin to take note because what is proposed will fundamentally change the relationship between service providers and their customers.

## Current position

Current UK data protection law does not impose direct obligations on data processors. Instead, data controllers must enter into written contracts with processors that require the processor to: (i) process data for the limited purposes permitted by the controller; and (ii) ensure appropriate technical and organisational security measures. A processor's liability is governed by its contract with the controller.

## The Draft Regulation

The Draft General Data Protection Regulation currently under consideration will fundamentally alter data protection compliance risk for processors, and the apportionment of risk between controllers and processors. Chapter IV of the Draft Regulation sets out obligations that are imposed directly on processors, who must:

- only process data on the controller's instructions (Art 27) and document in writing both the controller's instructions and the processor's obligations (Art 26(3));
- maintain documentation on the processing activities and make it available to regulators (Art 28);
- cooperate with supervisory authorities (Art 29);
- implement appropriate technical and organisational measures and procedures to safeguard data (Art 30);

- inform the controller immediately of a data breach (Art 31(2));
- carry out data processing impact assessments where the processing is deemed risky, such as data profiling activities,
- processing sensitive data, data on children, location data and biometric data (Art 33);
- obtain prior authorisation for cross-border transfers and consult where a data processing impact assessment is required (Art 34), and comply with cross-border transfer restrictions (Art 40);
- appoint a data protection officer (DPO) (Art 35); and
- obtain the controller's prior permission to appoint a sub-processor (Art 27).

**Contractual requirements**

In addition to imposing direct obligations on a processor, the proposed Regulation specifies the contractual elements that must be included in a contract between the processor and controller. In summary, these are:

- act only on the instructions of the controller, in particular where the transfer of the 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 Art 30;
- enlist another processor only with the prior permission of the controller;
- with the controller, create the necessary technical and organisational measures to enable the controller to comply with individuals' rights of transparency, information, access, rectification, the right to be forgotten, erasure, portability, the right to object and profiling;
- assist the controller in complying with Arts 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 process data otherwise; and
- make available to the controller and supervisory authority all information necessary to control compliance with the obligations laid down in Art 26.

These requirements extend far beyond what is required by existing UK data protection law. The Draft Regulation does not contain any savings provisions to preserve existing contracts. Given

this, and in the absence of any amendment, once the Draft Regulation comes into force, most existing contracts will be incompatible with the new requirements and will require renegotiation. Given the large number of contracts currently in existence throughout the EU, this potentially creates a huge logistical issue for organisations.

**Enforcement against a processor**

Under the Draft Regulation, processors will be liable to enforcement action from supervisory authorities for breach of their obligations. For example, under Art 79(6), supervisory authorities may impose administrative sanctions of up to 2 percent of annual worldwide turnover for breach of Art 26. A fine may be imposed on those who carry out the processing, which would appear to include the processor.

Similarly, under Art 79(5), supervisory authorities may impose a fine of up to 1 percent of annual worldwide turnover on an organisation which intentionally or negligently fails sufficiently to maintain the documentation required by Art 28. The exposure of processors to enforcement action from supervisory authorities is a significant departure from the position under the Directive.

**Administrative burden**

One of the main changes in the Draft Regulation is the expansion of responsibilities not just for controllers but, for the first time under European data protection law, for processors. Processors must take notice of these obligations because they are reinforced by significant enforcement powers. The provisions in the Draft Regulation relating to processors are detailed, and are likely to create significant additional administrative burden for processors (as well as controllers). In particular, the mandatory inclusion of specific contractual provisions will require negotiation between the parties as to the allocation of their responsibilities under the Draft Regulation, which may ultimately affect pricing. These issues have not been widely discussed so far, but they do present significant practical challenges for organisations.