COMPUTER LAW & SECURITY REVIEW 34 (2018) 881–885

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Supply chain arrangements: The ABC to GDPR compliance—A spotlight on emerging market practice in supplier contracts in light of the GDPR

*Nick Pantlin**, *Claire Wiseman*, *Miriam Everett*

Herbert Smith Freehills LLP, London, UK

ARTICLE INFO

Article history:

Keywords:
GDPR
Supply Chain
Processor
Controller
Liability
Data Protection

ABSTRACT

With ever increasingly complex and disaggregated sourcing supply chains and in the wake of the GDPR application deadline, this article shines a spotlight on early emerging market practice in supplier contracts.

1. You are only as strong as your weakest link

With increased outsourcing to the cloud or other third party external service providers and an increasingly complex supply chain for businesses, modern strategies for leveraging data can bring significant business efficiencies, competitive edge and growth opportunities, but also a range of risks that need to be understood and mitigated.

This has been mapped by a rise in the increased relevance of data protection and associated regulation. In the words of the Information Commissioner, the EU General Data Protection Regulation (the "**GDPR**") represents an "evolution" rather than a "revolution" in data protection regulation. Whilst data protection obligations have certainly been "tightened up" a notch, fundamentally, the underlying data protection principles remain largely unchanged.

The GDPR has, however, introduced some key changes that are giving rise to closer scrutiny of the supply chain protections in place between controllers and processors and, in turn, we are seeing a shift in the approach adopted by both parties in negotiating and implementing data processing arrangements. Key drivers include:

- processors also having certain **direct statutory obligations and liabilities for the first time** in certain areas under data protection legislation (under the previous legislation only controllers had statutory liability and any processor liability was purely contractual);
- controllers being required to impose **specified mandatory data processing provisions** on processors under Article 28 of the GDPR (previous requirements were less prescriptive); and
- of course, the **increased sanction regime** under the GDPR, with monetary penalties of up to a maximum of 4% of annual worldwide turnover or € 20 million (whichever is the greater) for certain breaches. The £500,000 the Information Commissioner's Office (the "**ICO**") could levy

* Corresponding author: Nick Pantlin, Herbert Smith Freehills LLP, Exchange House, Primrose Street, London EC2A 2EG, United Kingdom.
E-mail address: Nick.Pantlin@hsf.com (N. Pantlin).

https://doi.org/10.1016/j.clsr.2018.06.009

under the previous regime pales into insignificance when compared against the potential for this new eye watering exposure.

Combined, these factors mean that the "best practice" concepts afforded statutory recognition under the GDPR, now give rise to a very different risk assessment for both processors and controllers. It is against the backdrop of this new risk profile and the more prescriptive nature of the mandatory data processing provisions, in particular, that organisations have been reviewing and amending their existing supplier contracts (known as "re-papering") as well as re-considering their approach to new procurements, to ensure GDPR compliance going forward from 25 May 2018 and beyond.

2. A recap: the mandatory processing requirements

Engaging a processor to process personal data on behalf of an organisation is common place in both the private and public sectors. In an effort to assist with supply chain protection, increase data subjects' confidence in the handling of their personal data and ensure that such processing meets all requirements of the GDPR (not just those relating to keeping personal data secure as is currently the case), the GDPR sets out a granular set of requirements to govern the controller / processor arrangement.

A controller is required to appoint a processor that provides "sufficient guarantees" to implement appropriate technical and organisational measures so as to comply with the GDPR. There must be a written agreement between the controller and the processor and this data processing agreement must incorporate certain specific terms as set out in Article 28 of the GDPR (refer to box titled "Article 28 mandatory requirements"). In the last few years best practice has evolved to include a range of supply chain protections in data processing agreements from data breach notifications to controller rights to information or request compliance inspections. These provisions are elevated to mandatory legal requirements under the GDPR. The ICO has issued draft guidance on the interpretation of Article 28 and its practical application, setting out a checklist of the GDPR mandatory clauses (the "**ICO Guidance**").

Article 28 mandatory processing requirements: There must be a written agreement between the controller and processor incorporating certain specific terms as set out in Article 28 of the GDPR, placing requirements on the processor to:

- only act on the controller's documented instructions;
- impose confidentiality obligations on all personnel who process personal data;
- ensure the security of the personal data that it processes;
- abide by the rules governing appointment of sub-processors;
- implement measures to assist the controller in complying with the rights of data subjects;
- assist the controller in obtaining approval from supervisory authorities where required;
- at the controller's election, either return or destroy personal data at the end of the relationship (except as required by EU or Member State law); and
- provide the controller with all information necessary to demonstrate compliance with the GDPR, including allowing for or contributing to audits or inspections.

Granular processing description: The legislation dictates that the data processing agreement must set out the:

- subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subjects; and
- the obligations and rights of the controller.

The ICO Guidance clarifies the importance of being very clear at the outset about the extent of processing that a controller is outsourcing; very general or 'catch all' contract terms are expressly prohibited. The clarity elicited from a more detailed description is intended to protect against the possibility of changes being made to the processing scope over time, without taking account of any additional risks posed to data subjects. The level of detail required is not, however, stipulated and further clarity would be welcomed particularly when describing lower risk incidental processing; this may well be addressed in the updated ICO Guidance when it is issued.

3. Some of the key areas in which parties are facing challenges are set out below

Sub-processors – strengthening the supply chain: A combination of requirements under the GDPR seek to ensure that controllers retain control over personal data, even if the prime processor wishes to sub-contract some or all of the processing to another entity. In addition, the original processor cannot absolve itself of liability by using a sub-processor.

Processors are prevented from sub-contracting without the controller's prior written authorisation, which can be general or specific. On the whole, controllers are often unwilling to give *general consents* unless there are clear boundaries or conditions attached to that consent. However, if consent is given, the processor must inform the controller of any changes in sub-processor and give them an opportunity to object. Whether it is realistic to seek *specific consents* for each change in sub-processor will no doubt depend on the complexity of the supply chain and the practicalities of doing so.

The related sub-contract must include "the same data protection obligations" as set out in the head agreement between the controller and the processor. The ICO Guidance refers to "imposing the contract terms that are required by Article 28(3) of the GDPR on the sub-processor" as well as imposing the "same legal obligations the processor itself owes to the controller". The extent to which sub-processor terms need to be truly identical to the controller / processor arrangement (including, for example, any gold-plated terms agreed between the parties) remains unclear, and it is currently not known if an obligation to impose "substantially similar terms that are no less onerous", or to simply flow down Article 28 obligations,