GDPR series: Outsourcing contracts — all changed, changed utterly?

John O'Brien, Associate with Reed Smith LLP, discusses how to comply with the GDPR's rules on outsourcing contracts

The General Data Protection Regulation 2016/679 ('GDPR') will have a significant impact on outsourcing contracts. Although many of the principles of the current Data Protection Directive (95/46/EC) make their way into the GDPR, the compliance burden facing companies will increase substantially under the new law.

Many data protection practitioners will have already experienced the increased complexity of privacy and data protection negotiations between parties to an outsourcing arrangement. This article examines some of the headline GDPR issues that outsourcing companies, service providers and practitioners should be aware of.

Contractual requirements

Most outsourcing relationships will be considered an engagement between a controller (outsourcing company) and processor (service provider). As such, the first port of call for both parties when negotiating an outsourcing contract will be Article 28 of the GDPR. Article 28 comprehensively sets out items that must be included in any contract between a controller and processor. There are some issues that arise time and time again during outsourcing negotiations that organisations should be aware of:

Service provider demonstrating compliance with its GDPR obligations: Under Article 28(3)(h), a processor must 'make available to the controller all information necessary to demonstrate compliance' with its obligations under Article 28 generally. Article 28(3)(h) states that processors should 'allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller'.

Many processors, particularly large, technology service providers, are understandably wary of providing third parties with access to their systems and sites. Such service providers will typically attempt to fulfil their Article 28(3)(h) obligation by stating that they are:

- signed up to internationally accredited programmes that demonstrate their compliance with data protection best practices, such as ISO 27001; and/or
- audited by third parties regarding data protection issues and willing to share the results of such audits. Some service providers specifically state that they will only be subject to written audits.

Depending on the relative bargaining power of the parties and the volume or nature of in-scope personal data, each controller will need to decide whether or not these approaches offer sufficient reassurance.

Service provider obligation to notify an infringing instruction: A hanging paragraph after Article 28(3)(h) of the GDPR has been a source of fascination for data protection lawyers. The offending paragraph states that "with regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions." The issue is that controllers and processors tend to interpret a processor obligation very differently.

Controllers have tended to view the obligation as a broad requirement on processors to keep controllers honest. Processors counter that the scope of the obligation is in fact much narrower, only applying to instructions relating to their compliance obligations under Article 28(3)(h), relying on the 'with regard to point (h) of the first subparagraph' language at the start of the paragraph. Processors also argue that it is not their job to interpret the requirements of the GDPR and to offer controllers quasi-legal advice.

Sub-processors: Article 28(2) of the GDPR forbids processors from engaging sub-processors without 'prior specific or general written authorisation' from the controller. Processors must 'inform the controller of any intended changes concerning the addition or replacement of other [sub-]processors'.

Many large technology service providers are unwilling to proactively inform controllers about the changing shape of their sub-processor ecosystem. They tend to refer controllers to a publicly

(Continued on page 4)

(Continued from page 3)

available list of their sub-processors. They undertake to keep this list updated when existing sub-processors are removed and/or new sub-processors are engaged.

Controllers presented with this approach often, legitimately, question whether such passive provision of information is sufficient to discharge the requirements of Article 28 (2).

Flowing down obligations to sub-processors: Article 28(4) of the GDPR requires processors to flow down 'the same data protection obligations' to any sub-processors they engage to process in-scope personal data. Practical difficulties arise from the requirement for obligations placed on sub-processors to be the same as those in the contract between the controller and processor.

Processors, particularly those located outside of the EU, usually push back on this obligation. They claim that it is difficult, if not impossible, to harmonise and homogenise different contracts executed with different parties, for different purposes. They chafe at any restriction on their ability to freely contract.

Controllers may be presented with alternative promises that processors believe to be more realistic and pragmatic. These may include undertakings from processors that sub-processors are subject to data protection obligations that are substantially similar to those imposed on the processor.

Controllers must balance the letter of the law embodied in GDPR Article 28(4) and the commercial realities facing processors that find it difficult, if not impossible, to insert the same data protection obligations into other contracts.

> ***"Parties with greater knowledge and expertise in this area extract concessions from unwitting counterparties. Such concessions may have significant financial, operational and reputational ramifications for companies down the line."***

Personal data breach notifications: Article 28(3)(f) requires processors to assist controllers in ensuring compliance with controllers' obligations in relation to personal data breaches. Article 33(2) specifically requires processors to notify controllers 'without undue delay after becoming aware' of personal data breaches.

In the outsourcing world, specificity is next to godliness. Controllers are therefore unlikely to be thrilled by the prospect of processors notifying them of personal data breaches 'without undue delay'.

Controllers are required to notify supervisory authorities of personal data breaches no later than 72 hours after becoming aware of them. This is explicitly required by Article 33(1) of the GDPR. This has led controllers to insert into the contract a specific time period within which processors must notify them of personal data breaches they have suffered. Notification by a processor to a controller within 24 to 48 hours of becoming aware of a breach is usually sought. Some controllers go even further and seek to obligate processors to notify them of any suspected personal data breaches. Processors may push back on both these requirements because firstly, they are not specifically mandated by the GDPR and secondly, they place too onerous an obligation on them.

Much of the nervousness felt by controllers on this topic has its beginnings in the Article 29 Working Party's draft personal data breach notification guidelines adopted on 3rd October 2017. These stated that a controller should be considered aware of a processor personal data breach once the processor is aware of it.

Helpfully, the Working Party has changed its position to one that is more realistic and pragmatic. In its finalised guidelines amended and revised on 6th February 2018 (copy at www.pdpjournals.com/docs/887876), the Working Party states (at page 13) that a controller will be considered to be aware of a processor personal data breach 'once the processor has informed it of the breach'. This clarification may lead to a relaxation of controller demands for processors to inform them of any suspected personal data breaches and personal data breaches within 24 to 48 hours.

The outcome of negotiations on these discrete issues usually depends on the relative bargaining strength of each party. When negotiating with large, sophisticated service providers (for example, cloud services providers), they have standard terms and conditions that automatically assume an aggressive pro-processor stance. It is challenging, if not impossible, to convince such service providers to negotiate at all on these issues.

Liability and costs allocation

One of the largest privacy stumbling blocks for outsourcing negotiations is agreeing a liability structure that works for both parties. GDPR liability can arise in the form of sanctions issued by supervisory authorities, or as a result of claims taken by individuals under Article 82. Article 82 allows individuals to claim compensation for material or non-martial damage they have suffered as a result of unlawful processing.

Where a personal data breach occurs due to unlawful processing by a service provider and where the controller is also culpable in some way, the controller is jointly and severally liable for any damage arising.

Many service providers try to cap their liability at the total fees paid by

the outsourcing company under the contract during the preceding 12 months. Such a cap is likely to be entirely insufficient to controllers that, in the event of a personal data breach, may, for example, face financial exposure for:

- administrative fines issued by supervisory authorities;
- the cost of participating in investigations initiated by supervisory authorities;
- issuing notifications to affected individuals;
- compensation and legal fees incurred as a result of claims brought by affected individuals under GDPR Article 82; and/or
- mitigating the impact on their reputations.

In relation to personal data breaches originating with a service provider, controllers will typically attempt to have a separate or augmented liability cap with liability for personal data breaches specifically carved out of the general liability cap. Alternatively or in addition, they may secure a financial indemnity from processors in relation to any costs incurred, including in relation to third party claims.

The result of these two diametrically opposed positions is often a period of spirited negotiations between the parties. Reaching a conclusion that is mutually acceptable will depend, again, on the relative bargaining power of each party. However, other factors that will inform the final settlement include the degree of in-scope personal data and the likely effects of a personal data breach on affected individuals.

Separate to the issue of liability is the issue of allocation of costs generally. The GDPR is silent on which party should bear the costs of compliance. Allocation of costs is, therefore, a commercial point which must be reviewed on a deal-by-deal basis.

Where costs arise as a result of a service provider's breach of contract or negligence, the service provider may be fixed with any costs arising in relation to:

- complying with relevant data protection laws and directions issued by supervisory authorities;
- corrective action necessary to remedy a personal data breach;
- notifying affected individuals, even where this is not required by law; and
- the provision of credit monitoring services for one year where a personal data breach compromises financial information.

On the other hand, it is increasingly the norm for controllers to bear the costs of any audits of processors that they seek to carry out under Article 28 (3)(h).

Cybersecurity insurance has a big role to play when determining liability and cost allocations. Companies should ascertain whether their insurance policies protect against data protection regulatory breaches as well as personal data breaches. Outsourcing companies and service providers should be comfortable that service providers have sufficient insurance cover to match their proposed contractual liability.

Conclusion

The GDPR has significantly complicated the negotiation of privacy clauses in outsourcing agreements. It contains prescriptive requirements that must be included in every outsourcing contract. However, the GDPR is sometimes unhelpfully vague as to what precisely will suffice for controllers and processors to discharge these requirements. This leads to arbitrage between parties during negotiations. It can, in certain circumstances, mean that parties with greater knowledge and expertise in this area extract concessions from unwitting counterparties. Such concessions may have significant financial, operational and reputational ramifications for companies down the line. Any company involved in technology outsourcing needs to ensure it has a strong grip on its GDPR obligations.

For those tasked with navigating outsourcing transactions in the new world of GDPR, some may find W. B. Yeats' words particularly apt: "all changed, changed utterly: a terrible beauty is born."

John O'Brien
Reed Smith LLP
jobrien@reedsmith.com