Legal responsibilities of processors — a guide

Olivia Whitcroft, Solicitor and Principal of OBEP, gives advice on how processors can meet their obligations under the GDPR

Data protection rules for processors changed dramatically in May 2018, when the General Data Protection Regulation ('GDPR') kicked in. Processors had new direct obligations to comply with the law (or, in countries where there were already limited direct obligations, significantly more of them). They needed to put in place new internal compliance and risk procedures in areas such as information security, security breaches and record-keeping, and some were required to appoint a Data Protection Officer. Processors also needed to re-assess their procedures and terms for engaging with customers.

Discussion on GDPR compliance often comes from the perspective of controllers (perhaps with an 'and also' for processors). The focus of this article is the responsibilities of processors, from the perspective of the processor.

(Note: This article is written during the Brexit transition period, during which the UK is still being treated as part of the EU, and is still subject to the GDPR. Comment on the impact of Brexit appears towards the end.)

Who is subject to GDPR processor rules?

The quick answer to this question is that all technology or service providers who handle personal data on behalf of other organisations may need to be prepared to apply GDPR processor obligations, whether or not they are based within the EU.

Under Article 3(1), the GDPR rules apply to processors established within the EU. This means that, even to the extent the EU processor has a customer base outside the EU, it needs to comply with the processor rules (though its customer may not necessarily need to comply with the controller rules). This is the position taken by the European Data Protection Board ('EDPB') in its Guidelines on the territorial scope of the GDPR (Guidelines 3/2018, copy at www.pdpjournals.com/docs/888051).

Non-EU processors may also need to apply the rules, either because they have customers within the EU, and the customer contracts impose GDPR obligations on the processor (including those under Article 28), or they are involved with targeting or monitoring EU individuals on behalf of a non-EU controller (under Article 3(2) GDPR). This is the position taken by the EDPB within its Guidelines.

This effectively means that, as well as EU-based processors, any other provider worldwide may need to bring itself in line with GDPR processor rules, or at least have the option of doing so, if there is a chance its customer organisations (i.e. controllers) may be based in the EU or may target EU individuals.

Acting on the instructions of the controller

Under Articles 29 and 32(4) of the GDPR, the processor, and anyone acting under its authority (such as staff members), must use personal data only on the instructions of the controller. A processor will want to ensure that it is clear on the scope of such instructions at the beginning of the relationship, and what will be the procedures and costs for additions or changes. These can be recorded within the contract (as discussed below), or related service documentation.

There is an exception to the requirement to follow instructions: where required by law to use the data in another way (in which case the processor must generally inform the controller of this). However, note that this is EU (or EU Member State) law — the exception does not cover laws of other countries. Processors subject to the rules but based outside the EU will need to assess whether the laws of their jurisdiction may require additional use or disclosure of relevant personal data, and, if so, how this will be managed, as it is likely to be incompatible with the GDPR (and with customer contracts).

The end of Article 28(3) GDPR (relating to contracts between pro-

(Continued on page 4)

(Continued from page 3)

cessors and controllers) contains an oddly-placed requirement for processors to notify the controller if, in their opinion, an instruction infringes data protection laws.

Contracts between processors and controllers

Article 28(3) of the GDPR sets out matters which must be covered within contracts between a processor and a controller. The processor (as well as the controller) should ensure that appropriate terms are included. Here are three key tips for these contracts:

- don't forget to describe the relevant processing activities and put the obligations into context;
- don't forget to include obligations on the controller as well as the processor; and
- consider the practical impact of the obligations, and tailor the provisions accordingly.

Many data processing agreements are essentially a 'copy and paste' of processor obligations under Articles 28(3)(a) to (h). Broadly, these cover the following matters:

- acting on the instructions of the controller;
- imposing confidentiality obligations on staff;
- information security;
- appointment of sub-processors;
- assisting the controller with data subject rights, information security, security breaches and data protection impact assessments ('DPIA');
- return and deletion of data; and
- demonstrating compliance.

However, the concern with this approach is that they are generic obligations with no context or framework in which to apply them in practice. It also overlooks the first paragraph of Article 28(3), which requires the contract to 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'.

"Many data processing agreements are essentially a 'copy and paste' of processor obligations under Articles 28 (3)(a) to (h). However, the concern with this approach is that they are generic obligations with no context or framework in which to apply them in practice."

Some matters for processors to consider when preparing standard terms, or reviewing contracts provided by controllers, include the following:

For what specific activities and data do you act as a processor, and is this clear in the contract? If the contract is too all-encompassing, it may inadvertently impose processor obligations in relation to activities for which you act as a controller (such as use of customer account details). Or it may include unexpected types of data which you are not prepared to process (such as sensitive data requiring greater security controls).

Is the scope of the controller's instructions clear? As well as covering the general scope of services, consider related matters such as interaction with data subjects, data sharing and data transfers made on behalf of the controller. Or, if instructions are provided regularly, ensure it is clear how you will receive them. If the controller may change its instructions, consider what impact this could have on cost or the manner in which you provide services.

Is the contract clear on the controller's responsibilities? This may cover areas such as lawful basis, data minimisation, data retention and international data transfers. As the processor, you will not want a contract which imposes obligations only on you.

What is the practical split of responsibilities in relation to data security? To take a simple example, the processor may agree to encrypt its systems, and the controller may agree to keep passwords confidential.

What will 'assistance' to the controller look like in practice? Consider what specific actions may be required of the processor in assisting with data subject rights and security breaches, and for what activities a DPIA may be relevant. Also clarify timescales and resources for assistance, and who will bear the costs. Where appropriate, the contract could be supported by procedural documents and arrangements.

How will data be returned or effectively deleted at the end of the relationship? Systems may need to be set up in such a way such that this does not become an onerous exercise.

What may the controller's audits look like in practice? Consider the time, resources and costs involved, and whether to limit the regularity and scope of such audits.

Is the controller looking to include obligations beyond the main matters within Article 28? For example, the controller may require assistance in relation to other aspects of compliance, or may impose additional obligations impacting how and where the processor provides its services. Processors should assess whether such obligations are feasible for them, and how they impact resources and costs.

What liability and indemnity provisions are there? These may tie in with liability provisions of the main services agreement, or the parties may negotiate separate limitations, caps and indemnities for data protection matters. Processors should also assess their insurance cover for data-related breaches.

What is the governing law and jurisdiction of the contract? This might impact the interpretation or enforcement of the provisions.

Data security and personal data breaches

Under Article 32 of the GDPR, processors must implement 'technical and organisational measures to ensure a level of security appropriate to the risk'. Processors therefore have direct legal obligations for information security, in addition to their contractual obligations to controllers. Processors will want to ensure consistency between obligations imposed by controllers and their standard measures (or work out how to resolve any differences).

Article 32 goes on to specify that measures may include: pseudonymisation and encryption; the ability to ensure ongoing confidentiality, integrity, availability and resilience of systems and services; the ability to restore availability and access in the event of an incident; and a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

Codes of conduct and certifications approved under the GDPR at EU or Member State level (once these exist) may be used as an element to demonstrate compliance.

Under Article 33(2) GDPR, the processor must notify the controller 'without undue delay' after becoming aware of a personal data breach. Controllers often look to include a more specific notification period within processor contracts, such as 24 or 48 hours. Processors will usually want to make it clear that the period starts after they become aware of a breach (rather than necessarily the time of the breach itself). Guidance on the meaning of 'aware' is provided in the EU Article 29 Working Party Guidelines on personal data breach notification (WP250 v.1, copy at: www.pdpjournals.com/docs/888052) as endorsed by the EDPB, though processors should be alert to any alternative definitions of 'awareness' specified in the contract.

As part of information security measures, processors should also consider how they will detect breaches promptly. 'Without undue delay' is not defined, but means as soon as possible. The GDPR does not require processors to assess the circumstances or severity of a breach prior to notifying the controller, though the controller may separately require assistance with this.

Sub-processors

Articles 28(2) and 28(4) of the GDPR impose obligations on processors in relation to sub-processing. Additional requirements or procedures may be specified within data processing contracts. The key elements are as follows:

- Authorisation — the processor must have 'general' or 'specific' authorisation from the controller prior to appointing a sub-processor;
- Contract — the processor must have a contract with the sub-processor which mirrors the obligations in the contract between the processor and controller; and
- Liability — the processor remains liable to the controller for the actions of the sub-processor.

There is variation in the way sub-processor authorisations are set up. The GDPR wording on this point is a little unclear, though the process is often driven by standard terms of the controller or processor, and subsequent negotiation between the parties.

It is common for processors to prepare a pre-approved list of specific sub-processors within a schedule or attachment to the contract, and for the contract to have a process for updating this list. The list could alternatively refer to potential sub-processors, or criteria for appointing sub-processors.

There is then the question of whether changes to sub-processors need approval (often favoured by controllers), or whether the controller is given a right to object. Or, if the pre-approval is sufficiently wide, neither may be required. For processors who service many customers, it is likely to be impractical to seek the prior approval of every customer each time changes are made. Processors may therefore want to prepare a sufficiently wide list of pre-approved sub-processors (including any sub-sub-processors), an easy way to notify customers of changes, and, where required, an efficient procedure for objections to be raised. Consideration should also be given to what happens if valid objections are received (or approval is not given), such as alternative sub-processors or termination of the services.

There are also challenges for processors in mirroring obligations of customer contracts within sub-processor contracts, particularly where the respective contracts are based on standard terms of customers and/or sub-processors. Liability terms may also not match up; for example, a sub-processor may impose a liability cap which is much lower than the processor's potential liability to the customer. Unless the processor has full control over all terms within the supply chain, contracts down the chain are unlikely to be perfectly aligned. Processors may wish to focus negotiations on key issues and risks, such as ensuring security and security breach procedures are consistent, and that the processor is able to action effectively the instructions of the controller.

Where a sub-processor is located outside the EU, international data transfer requirements must also be met.

International data transfers

Processors are subject to rules under Chapter V of the GDPR relating to transfers of personal data to jurisdictions outside the EU. This means that if, for example, the processor has an office or data centre in another country (which accesses or processes the relevant personal data), or appoints a sub-processor in another country, it will need to ensure that:

- such country's laws have been deemed to provide 'adequate' protection (under Article 45); or
- another appropriate safeguard is in place (under Article 46); or
- a derogation applies (under Article 49).

Compliance for processors can be challenging, as approved transfer mechanisms are currently limited.

(Continued on page 6)

(Continued from page 5)

The main ones are the following.

Processor Binding Corporate Rules: These can be used to permit transfers of personal data within a processor's group of companies. Whilst they can be a good tailored solution once in place, the procedures for preparation and approval can be detailed and lengthy. They are therefore most commonly used by large multinationals, and are unlikely to be used for short-term or small-scale intra-group transfers.

EU-US Privacy Shield: These can be used for transfers to US companies who have self-certified for the Privacy Shield framework to the US Department of Commerce.

Model contract clauses approved by the EU Commission: These often appear to be the quickest and most obvious solution for international data transfers (other than to US companies who have self-certified for the Privacy Shield). However, a problem for processors is that there are no approved processor to sub-processor clauses. Even where the controller is involved in the contractual arrangements (so the controller to processor clauses can be used), they are a less than ideal set of terms to follow in practice, and they do not even meet GDPR requirements under Article 28 (3) (or Article 28(4) for sub-processing).

Options sometimes boil down to avoiding the transfer all together, or being creative in finding a solution within available transfer mechanisms. There is a risk that inappropriate, impractical or non-sensical terms end up being used just to tick a compliance box.

Additional obligations

Processors must also do the following.

Maintain records of processing activities (Article 30(2) GDPR): These records include names and contact details for all relevant controllers, categories of processing, details of international data transfers and, where possible, details of security measures.

Appoint a Data Protection Officer ('DPO') (Article 37): A DPO must be appointed by public authorities; or where the processor's core activities require either regular and systematic monitoring of individuals on a large scale, or large-scale processing of special categories of data (or data relating to criminal offences).

Appoint a representative within the EU (Article 27): An EU representative must be appointed if the processor is not established within the EU, but is subject to the GDPR by virtue of assisting to target individuals within the EU (as discussed earlier). The EDPB has indicated that the representative should be a separate person or body to the DPO (if appointed). The representative must maintain its own records of processing activities.

Co-operate with the national Supervisory Authority (Article 31).

Where a processor is responsible for a data protection breach, data subjects may take action against it for compensation under Article 82 (1) GDPR: Article 82 also discusses the apportionment of liability between controllers and processors.

Brexit

Brexit complicates matters for processors in the UK, and for those who have customers within the UK. The UK becomes a third country for international data transfer purposes. This means that, unless and until the UK is deemed an 'adequate' country by the EU Commission, processing contracts with UK processors (or sub-processors) may require less-than-desirable standard contractual clauses. The UK will also have its own international data transfer rules which will require new mechanisms for sending data outside the UK (such as a new UK-US Privacy Shield scheme for transfers to the US).

UK processors may also need to appoint an EU representative if they are involved in activities targeting the EU (and potentially vice-versa for EU processors operating within the UK). Hopefully UK data protection law will remain similar to the GDPR, but processors operating within the UK and the EU will also need to get their head around two different sets of laws. The differences may also need to be reflected in contracts with customers. We can of course hope that current discussions between the UK and the EU will assist in addressing these matters before the end of the transition period!

What next?

Two years on from the rules starting to apply, processor procedures are becoming more established, though there are variations in the approach taken (for example, in relation to processing contracts). There remains debate over the interpretation of the rules (such as for territorial scope) and challenges over some of the trickier aspects of compliance (such as international data transfers).

Processors can continue to improve their compliance frameworks as they gain experience of the issues, and their relationships with customers and sub-processors. It is also worth keeping an eye out for new guidance, and additions or changes to legal rules or options. Some changes could complicate matters (such as Brexit), but others may assist, such as new codes of conduct or international data transfer mechanisms.

Olivia Whitcroft
OBEP
olivia.whitcroft@obep.uk