GDPR series: practicalities of managing the controller — processor relationship

Jenai Nissim, Legal Director, TLT LLP, explains exactly how to negotiate the new requirements for data processor-controller contracts

Current data protection legislation has been in place for over 15 years. In that time, technology has moved on significantly, with data processing occurring within milliseconds, sometimes without individuals even being aware of it taking place. The advent of big data has enabled use of personal data for profiling and analytics in ways that were previously unimaginable.

Today, most data processing takes place using a number of organisations situated in multiple locations, meaning that it is hard to maintain control over who has access to the personal data and exactly what they are doing with them.

Changes introduced by the General Data Protection Regulation ('GDPR') place data processors under direct regulatory responsibility for the first time, recognising their importance in the data supply chain. So, what do these changes mean for the data controller-data processor relationship? And how should controllers and processors manage this relationship now?

Engaging data processors under current law

Using the UK's implementing law as an example, current data protection law can require that data controllers enter into written contracts with data processors when engaging them for data processing. In the UK, such contracts need to state that the data processor will act on the instructions of the data controller and will comply with the same obligations placed on a data controller under the Seventh Data Protection Principle of the Data Protection Act 1998 (the requirement to keep data secure).

Whilst data controllers operating in a regulated environment will insist on more robust and detailed contractual provisions, perhaps detailing the processing activities and audit requirements, many contracts contain 'light touch' data processing conditions. This may prove problematic for many organisations that currently engage data processors, as the requirements introduced by the GDPR are far more prescriptive.

Additionally, data controllers must demonstrate that the provisions are being complied with.

Any data processing contracts which run beyond 25th May 2018 will need to be drafted (or amended) to incorporate the expanded GDPR requirements.

Engaging data processors under the GDPR — a whole different ballgame?

The GDPR introduces two key changes which relate to the engagement of data processors:

- mandatory contractual clauses which must be included in all contracts; and
- using only data processors that are able to demonstrate compliance with the GDPR.

The mandatory clauses

There are a number of mandatory clauses to be included in a contract between a data processor and a data controller, which are set out under Article 28 of the GDPR. Below we take a look at these mandatory clauses, how compliance could be demonstrated and the practicalities of doing so.

Data processors must only process the data on documented instructions from data controllers, unless required otherwise by law:

This is not a new requirement under the GDPR. However, the mandatory clauses which must be included in a contract under the GDPR are much more prescriptive, and both data controllers and data processors must be able to demonstrate how these comply with these provisions.

All contracts should set out clearly the expectations of the data controller in terms of the processing to be undertaken and the data processor should not process the data outside of these instructions. If a data processor does so then it risks assuming liability as a

(Continued on page 4)

(Continued from page 3)

'data controller', and therefore may become subject to a raft of additional compliance requirements under the GDPR.

Complying with this provision may seem simple, given that at the outset of any data processing relationship the parties should be clear what personal data are being processed and this can be included in the contract.

However, many organisations fail to consider how to address changes to the processing activities as the relationship progresses. It is therefore key to ensure that an appropriate change control mechanism is in place in the contract and within the organisation to ensure that if, for example, a new service is undertaken and this results in data being processed differently than is set out in the contract, that appropriate changes are made to the contract, and any new privacy risks associated with the processing are considered and addressed.

Data processors must ensure that personnel used for data processing are committed to an obligation of confidentiality:

The obligation of confidentiality can be established through contractual provisions with personnel, and should be re-enforced through data protection training. Additionally, in some circumstances personnel may be subject to professional ethics and confidentiality rules (for example health care professionals or lawyers).

When engaging a data processor, it is prudent for data controllers to perform due diligence prior to entering into the contract and during the relationship, to ensure that the data processor places an obligation of confidentiality on individuals (including sub-contractors) having access to the personal data and that these individuals are provided with the necessary training to help them understand their obligations under the contract and the GDPR.

"In order to comply with these provisions, organisations should consider implementing a robust process with third party suppliers which not only requires notice of any changes to sub-processors, but also includes checks by the data controller, for example, a monthly review of who is processing personal data."

Data processors must implement appropriate measures to ensure a level of security appropriate to the risk associated with the types of data being processed:

There is no definition of what 'appropriate' technical and organisational measures are, but consideration should be given to the 'state of the art, the costs of implementation and the nature, scope, context and purposes of processing'. However, asking a data processor to provide a privacy impact or other risk assessment on the processing activities to be undertaken should enable a data controller and a data processor to demonstrate that they have:

- identified and considered any privacy risks with the processing;
- assessed the severity of these risks and how they could be mitigated;
- documented decisions taken about whether or not to accept or mitigate any privacy risks; and
- implemented any appropriate technical and organisational measures to safeguard the personal data and manage the risks.

Data processors must comply with certain obligations relating to using sub-processors:

Under the GDPR, a data processor must obtain the data controller's written consent prior to engaging a sub-processor. Further, the data processor must notify the data controller of any changes to the use of the sub-processor, for example appointing a new or replacement sub-contractor.

In order to comply with these provisions, organisations should consider implementing a robust process with third party suppliers which not only requires notice of any changes to sub-processors, but also includes checks by the data controller, for example, a monthly review of who is processing personal data. This helps to ensure that the provisions are being complied with and no unauthorised sub-contractors are being used inadvertently.

Data processors must assist data controllers with complying with the GDPR:

Data controllers must appoint data processors who are able to assist the data controller as it complies with its obligations under the GDPR. In particular, the data processor must assist the data controller with:

- implementing appropriate technical and organisational measures to safeguard the personal data being processed for example anonymising the personal data and ensuring that systems which process personal data are reliable and can be brought back on-line for example in the event of a system failure;
- responding to data subject requests as individuals exercise their rights under the GDPR;
- notifying personal data breaches to the relevant regulatory authority for example the ICO and in certain

circumstances the individuals impacted; and

- assisting the data controller with any data protection Privacy Impact Assessments ('DPIAs') to assess the privacy risks of any data processing activities and the steps which should be taken to mitigate or eradicate such risks.

Data controllers and data processors may find that the cost of the data processing services increases as a result of these compliance requirements.

It is important for both the data controller and the data processor to set out clearly what the expectations are of both parties in terms of the services to be delivered. For example, does the data controller expect the data processor to carry out a full DPIA prior to the data processing services commencing? What role will each party play in the event of a personal data breach? Who will bear the costs of each activity?

It is best to agree these provisions at the commencement of the relationship and include these in the contract in order to avoid unnecessary negotiations over price at a later when the data controller is already heavily reliant on the data processor.

At the behest of the data controller, the data processor must either delete or return all personal data at the end of the term of the processing services.

In order to comply with the GDPR, a data controller needs to know the location of the personal data at all times and the processing activities being undertaken in relation to those personal data. This requirement remains in place once the data processing services have been completed. The contract should clearly specify what should happen to the personal data once the contract ends, and appropriate provisions should be included in order to ensure that this happens. For example, the data processor should provide an attestation to the data controller that the personal data have been destroyed.

Whilst an attestation is a perfectly acceptable way to demonstrate compliance, this should not be relied on entirely and the data controller must undertake its own compliance checks to ensure that, for example, the personal data have been destroyed by a reputable organisation — as opposed to have been thrown in a skip, for example.

Data processors must provide all information necessary to demonstrate compliance with their obligations under the GDPR including allowing and contributing to inspections conducted by the data controller or another auditor mandated by the data controller:

In order to demonstrate compliance, the data processor will need to allow the data controller, the Information Commissioner's Office ('ICO') (or their auditors) to carry out audits and inspections to verify compliance. Provisions should therefore be added to the contract setting out this right.

Where a data processor acts for a number of data controller clients, the data processor may attempt to push back on the existence of such audit rights, for example by limiting these in terms of the timing or scope of any such audit. Whilst in theory this seems acceptable, it is important to note that the regulator's right to assess compliance with the provisions of the GDPR should remain unfettered.

Monitoring data processors

Given the responsibility for demonstrating how data controllers comply with the GDPR, and the fact that this requirement extends to the use by data controllers of data processors to process personal data, data controllers should consider setting up a compliance programme specifically to monitor the use of data processors. Such a compliance programme should include as a minimum:

- prior to engaging a data processor, assessing how the data processor can comply with the relevant provisions of the GDPR, for example being able to demonstrate that it can implement appropriate technical and organisational measures to safeguard the personal data;
- reviewing the data processors own data protection compliance programme, the activities undertaken under the programme and approach to data protection generally to ensure that this is consistent with the expectations of the ICO and the GDPR; and
- periodic assessments of the data processors' ability to still meet any initial assertions provided when the initial compliance assessment of the data processor was undertaken.

The assessments and monitoring undertaken should be proportionate to the risks posed by the outsourcing. There is no one size fits all approach and how your organisation approaches a compliance monitoring programme will be based on your own internal privacy risks, those posed by the data processor and the processing undertaken.

Negotiating contract terms and liability under the contract

With fines for non-compliance with the GDPR increasing to the greater of €20,000,000 or 4% of annual worldwide turnover, caps on liability under contracts are likely to be a focus for both the data controller and the data processor. Data processors will not want to commit to a high cap on liability which, in reality, if it is relied upon may leave the data processor being unable to financially continue to run its business. Plus, data controllers will not want to commit to a cap on liability which is too low and does not cover fines and the additional costs of dealing with data breaches such as management time, damage to its reputation and remediation costs.

Furthermore, under the GDPR the data processor now has liability for data protection breaches and could also be subject to an ICO decision directly, whether this is a warning, enforcement action or administrative fine.

(Continued on page 6)

(Continued from page 5)

When negotiating data processing agreements, there is never a right answer as to how much a cap on liability should be for a breach of data protection legislation. However, when setting any caps on liability for breach of the GDPR, consideration must be given to:

- the nature of the personal data processed;
- the manner in which the personal data are processed; and
- the purposes for which the personal data are processed.

For example, processing names and email addresses for marketing purposes using an established database or system poses fewer privacy concerns than processing biometric personal data via a new mobile app. It therefore follows that the cap on liability for breach of data protection provisions in both these cases will differ given the differences in the risks.

Conclusion

There are clearly a number of compliance issues arising from the use of data processors to process personal data and these are not likely to go away anytime soon. Whilst guidance is expected from the UK regulator on contracts and liability, in the interim data controllers should consider the processes they use for choosing and engaging with data processors to ensure that they are able to demonstrate that they are meeting the requirements laid down by the GDPR.

Jenai Nissim is leading a Workshop on 'Creating a GDPR Compliance Programme' at the 16th Annual Data Protection Compliance Conference in London on 13th October 2017.

For further information, and to make a booking, visit www.pdpconferences.com

Jenai Nissim
TLT LLP
jenai.nissim@tltsolicitors.com