SLAUGHTER AND MAY

Processing under the GDPR: risk and liability shifts

October 2016

With the GDPR now technically in force, and just over 18 months before it applies in Member States, we look at how this new regime will impact on your processing arrangements, from mailing services to large-scale outsourcings, and what steps you need to take now to prepare.

Familiar concepts but a stricter regime

The new General Data Protection Regulation ('**GDPR**') imposes a more prescriptive and, for many jurisdictions including the UK, tougher data protection regime than under the current law, including in the area of processing arrangements. It retains many of the basic concepts and roles from the current law. For example, customers procuring processing services will continue to be data controllers (i.e. the party determining the purpose and means of the processing) while suppliers will still tend to be data processors (who process personal data on behalf of the controller). However, a number of key changes mean that the dynamic of this relationship is likely to change. In particular:

- the GDPR increases the regulatory requirements as a whole, which may increase the cost of processing data. This includes requiring that a detailed list of provisions be included in any processing agreement;

- data processors now face direct legal obligations under the GDPR in areas such as security, record keeping and international transfers – under the current regime the regulatory burden falls solely on data controllers. The GDPR also provides that controllers and processors will be jointly and severally liable where they are both responsible for damage caused by their processing (although where one party pays all of the compensation for the damage, it is entitled to claim back relevant amounts from the other party/parties);

- the sanctions for breaching the GDPR are significantly higher than under the current regime. Current penalties of up to £500,000 will increase to fines of up to 4% of annual worldwide turnover or €20m, whichever is greater (or up to 2% and €10m, depending on the breach) - and apply to both controllers and processors.

These factors combine to increase the risk profile associated with processing personal data not only for customers but also for suppliers, which in turn may impact on how the parties approach their processing relationships.

Now is the time to act

By 25 May 2018 all processing arrangements must be GDPR compliant. Organisations should therefore be taking action now to ensure that any arrangements which will still be in force after this date comply with the new provisions – this includes both new arrangements (when selecting and contracting with new processors) and existing engagements (where sufficient time must be scheduled to renegotiate existing terms). *See box: Next Steps*.

While some processors may resist taking action yet, citing the uncertainty surrounding Brexit, there is arguably sufficient clarity now. *See box: Impact of Brexit.* The law is in agreed form, and controllers that postpone preparations risk being left behind the curve as competitors and suppliers start making changes to contractual positions and processes.

Impact of Brexit

UK organisations should still prepare for the GDPR despite the Brexit vote as, even if it does not remain part of the UK's legal framework post-Brexit:

- it is unlikely that the UK will have left the EU before May 2018 (when the GDPR becomes 'live');
- many organisations will still be caught by the GDPR regardless of whether the UK is in the EU or not as it has a wide territorial reach. It applies to any organisations selling goods and services into the EEA or monitoring behaviour;
- it is likely that any post Brexit data protection regime will be similar to the GDPR (providing adequate or essentially equivalent protection), given that the UK will still want to maintain close trading relationships with EU countries, which are likely to involve the transfer of personal data.

The UK's new Information Commissioner (Elizabeth Denham) also recently recognised these points in her first speech as Commissioner (See speech 29/9/16).

Impact of the GDPR on processing arrangements

The GDPR impacts on all aspects of the processing relationship, from how to choose a processor to what to include in the processing contract and how data is dealt with at the end of that arrangement. It also impacts heavily on the risks associated with processing personal data for both controllers and processors, which in turn affects the contractual risk allocation between those parties.

Choosing a processor

Under the GDPR controllers can only use processors '*providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of GDPR and ensures the protection of the rights of data subjects*.' This is much broader than the current requirements (which focus on controllers obtaining guarantees around security) and means that controllers are likely to carry out a broader due diligence exercise when selecting a processor than they might currently undertake.

The concept of accountability and focus on being able to demonstrate compliance which run throughout the GDPR may also impact on how controllers appoint their processors and the records kept about such appointments. For example, under the GDPR controllers must conduct data protection impact assessments (DPIA) in certain, higher risk, and scenarios. They may therefore want to consider whether it is necessary, or good practice, to carry out a DPIA before entering into a major new processing arrangement (such as a strategic outsourcing

involving new technologies or processing services involving profiling or large amounts of 'special' categories of data).

Negotiating a processor contract

The GDPR, in common with the current regime, requires that whenever processing is carried out on behalf of a controller by a third party, those parties must enter into a written contract. However, it greatly increases the list of provisions that must be included in that contract.

The required provisions are listed in Article 28(3) of the GDPR, and set out in the box below (*GDPR: Contractual Requirements*).

GDPR Contractual Requirements

Article	Requirement
28(3)	Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed and the obligations and rights of the controller. The contract must stipulate, in particular, that the processor will:
28(3)(a)	process only on documented instructions, including regarding international transfers (unless, subject to certain restrictions, legally required to transfer to a third country or international organisation);
28(3)(b)	ensure those processing personal data are under a confidentiality obligation (contractual or statutory);
28(3)(c)	take all measures required under the security provisions (Article 32) which includes pseudonymising and encrypting personal data as appropriate;
28(3)(d)	only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object); flow down the same contractual obligations to sub-processors;
28(3)(e)	assist the controller in responding to requests from individuals (data subjects) exercising their rights;
28(3)(f)	assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities (Articles 32-36);
28(3)(g)	delete or return (at the controller's choice) all personal data at the end of the agreement (unless storage is required by EU/member state law);
28(3)(h)	make available to the controller all information necessary to demonstrate compliance; allow/contribute to audits (including inspections); and, with regard to (h), inform the controller if (in its opinion) an instruction infringes data protection law.

Codifying best practice?

The current requirements (set out in the Data Protection Directive 95/46/EC and implemented in the UK by the Data Protection Act 1998) focus on the processor following the customer's instructions and providing sufficient security guarantees. In practice, controllers will require a more detailed list than this for all but the most basic of processing arrangements. Market practice over the years has gradually seen the addition of clauses on a range of protections, from security breach notification to assistance with subject access requests. To an extent, the GDPR provisions therefore codify current best practice. However, the prescriptive nature of the GDPR means it is unlikely that even the most detailed of pre GDPR clauses will completely satisfy the new requirements.

For example, one area where the GDPR goes beyond current market practice is sub-processing (sub-contracting by the processor to a third party who can be an individual consultant or a corporate supplier). While it is not uncommon for there to be restrictions around sub-contracting in existing contracts, the GDPR:

- prevents the processor from sub-contracting without the controller's prior written consent;
- requires that, where general rather than specific consent has been obtained, the processor informs the controller of any changes (giving them an opportunity to object); and
- states that sub-contracts must contain the 'same' (rather than the more commonly used 'substantially similar') data protection obligations as are set out in the main processor agreement with the controller.

Cloud providers, and other processors with large and dynamic supply chains, may find these provisions challenging. It will therefore be interesting to see how the market develops in this area – will these processors try to impose standard data protection terms on all of their customers and sub-processors (which may make it harder to win contracts from larger, regulated clients) or will these provisions drive a change in their processes? And what if the sub-processor is a big player in the market with its own standard terms?

Going beyond GDPR requirements

While processors now have some direct obligations, controllers still have more extensive liability than processors under the GDPR. They remain liable for all damage caused by processing which infringes the GDPR, where-as processors are only liable under the GDPR when they breach processor specific provisions or act outside the controller's instructions. Controllers are therefore often reliant on processors to enable them to fulfil their legal obligations.

Despite the detailed nature of Article 28(3), there are therefore still some areas where controllers may want to go beyond the GDPR's contractual requirements to assist with their own compliance.

For example, in relation to breach notification, controllers have an obligation to notify their supervisory authority of a data breach without undue delay and, where feasible, within 72 hours. However, processors only have a duty to notify their controllers 'without undue delay'. Controllers may feel that this does not give them

sufficient comfort that the processor will notify them in time to meet their 72 hour target, and may therefore wish to put an actual timeframe (e.g. 'promptly and in any event within 24 hours') into their processor contract.

Impact on negotiations

The long list of contractual provisions required under the GDPR together with those additional measures that controllers may feel are necessary to enable compliance, mean that processing clauses (and the negotiations which accompany them) are likely to become much longer and potentially more contentious.

That said, the European Commission has a right under the GDPR to lay down standard contractual clauses. If standard clauses are produced, and widely adopted, signing processor clauses may instead become more of a tick box exercise (akin to entering into the current model clauses for international transfers). However, even if the clauses become standardised, the parties must still satisfy themselves that sufficient measures and protections are in place before signing, particularly given the potential for high fines if they are not.

Impact on risk profile

The GDPR has already raised the profile of data protection, and is starting to change its risk profile for both controllers and processors. As a consequence we are beginning to see an increased focus in negotiations on the liability and indemnity provisions associated with data protection. Questions around risk allocation are the subject of much debate. For example, should warranties and indemnities be in favour of both customers and suppliers? Should data protection liability sit outside liability caps (or be subject to a super cap)? How do caps work with the entitlement to claim compensation back from other controllers or processors also responsible for the damage in question? And should data losses be included in any liability 'inclusion' clause? However, it is vital that these remain commercial debates around risk allocation, rather than dry legal wranglings, if the parties wish to reach a successful outcome.

The changing risk dynamic may also impact on other areas of the negotiations – for example around insurance requirements, and on the willingness of the parties to 'sign-off' on the appropriateness of certain technical and organisational measures. In particular the fact that both controllers and processors will have direct obligations to implement appropriate technical and organisational measures relating to security (rather than the controller flowing this down contractually to the processor) may make it more difficult for them to agree on what is a cost effective, and yet appropriately secure, solution. In the future it may be that approved codes of conduct or certification mechanisms are used to help parties demonstrate adequate security (and the GDPR does expressly allow for this). However, in practice these may be some way off. For now, what is 'adequate' is therefore harder to gauge.

Comment

While the GDPR brings increased regulation and the potential of high fines (up to 2% of worldwide annual turnover or €10m for failing to include the correct provisions in a processor contract, and up to 4% and €20m for other breaches) it is still unclear how local data protection regulators will choose to enforce it in practice. In the UK the

Information Commissioner's Office has always taken a pragmatic and relatively business friendly approach to regulating personal data, and to-date processing arrangements have not been a particular focus of their attention.

However, undoubtedly the risk of fines will make it harder for data controllers and data processors to take some of the risk based decisions they currently take around entering data processing arrangements. And while it may be difficult to currently predict what regulatory approach will be taken once the GDPR applies, the new law is certainly expected to impact market practice and negotiations in this area.

This article was written by Rob Sumroy and Natalie Donovan. If you would like any further information on processing arrangements, or advice on your GDPR compliance programme, please contact Rob Sumroy, Rebecca Cousin, Richard Jeens or your usual Slaughter and May contact.

Next Steps:

Now is the time for both controllers and processors to take the necessary steps to ensure their contracts, and the processes associated with them, are ready for the May 2018 GDPR deadline:

Existing Contracts	New Contracts	Generally
Renegotiate existing contracts: ✓ Audit your supply chain to understand which contracts require renegotiation. ✓ Review your contracts to see who is responsible for implementing changes in law. ✓ When negotiating the GDPR provisions consider: (i) the date from when new provisions should apply – now or May 2018? This may depend on any associated costs; (ii) whether to roll this into a wider renegotiation.	**Ensure new contracts are GDPR ready:** ✓ Review your procurement and processor selection process: do you need to carry out increased due diligence or a DPIA? ✓ Future proof now: sufficient detail exists now to include GDPR ready provisions in arrangements that will continue post May 2018. ✓ Ensure any mandatory change clauses cover future data protection changes and guidance.	**Consider what else needs to change in your organisation:** ✓ Ensure your back-end processes are ready for May 2018. This includes, for example, procurement, record keeping, governance, training and audit functions. ✓ Review your insurance policies – are the heads of loss and limits appropriate? Do they cover losses caused by data breaches or breach of data protection legislation? Are these covered if the loss is caused by your processor?

Rob Sumroy
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Natalie Donovan
T +44 (0)20 7090 4058
E natalie.donovan@slaughterandmay.com

October 2016