Supply chain arrangements

The ABC to GDPR compliance

A spotlight on emerging market practice in supplier contracts in the run up to 25 May 2018 and beyond.

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 existing data protection obligations have certainly been "tightened up" a notch, fundamentally, the current underlying data protection principles remain largely unchanged.

The new EU data protection framework does, however, introduce 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 existing legislation only controllers have statutory liability and any processor liability is 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**") can currently levy under the existing 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 are, embarking on 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 (see box titled "GDPR-repapering – how to navigate the minefield").

On the dawn of the GDPR application deadline, this article consolidates early emerging market practice, as we shine the spotlight on:

- The mandatory processing requirements to be incorporated into data processing agreements and some early challenges in doing so;
- Trends in supply chain protection and allocation of risk between controllers and processors;
- Emerging trends in the general approach to negotiating processor clauses;
- Navigating the minefield to successfully implement a GDPR re-papering exercise; and
- The benefits of a GDPR re-papering exercise beyond simply GDPR compliance.

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 ofrequirements 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:

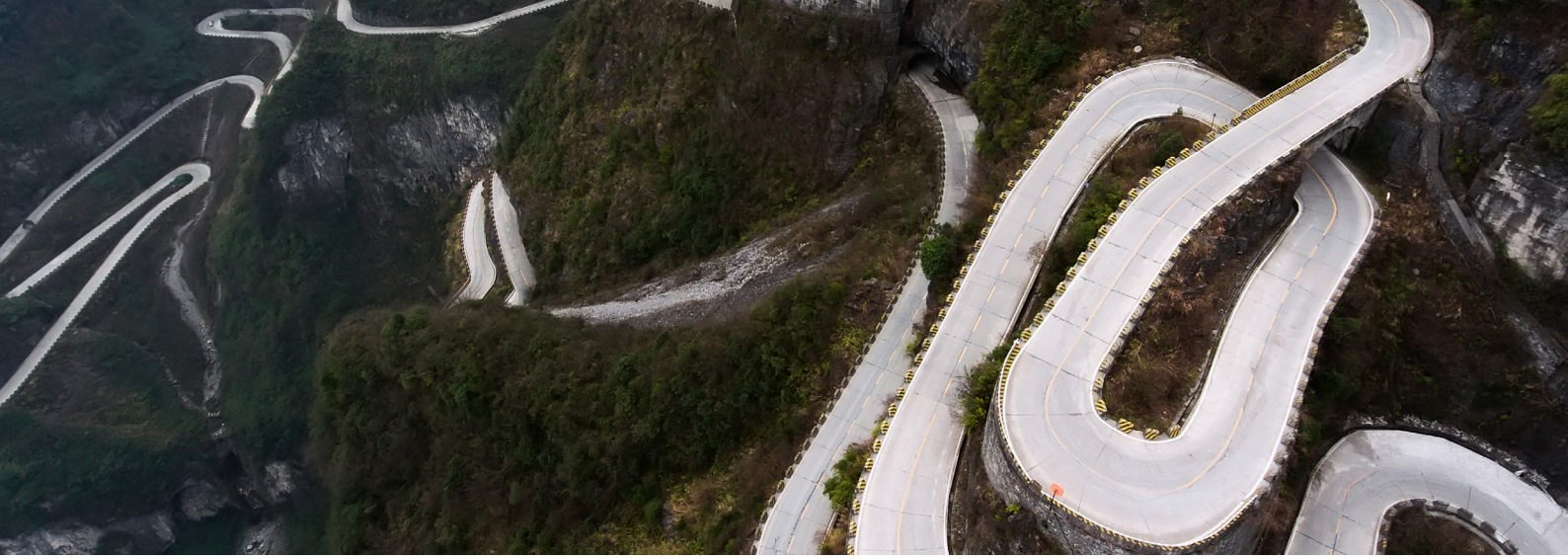
- Only act on the controller's documented instructions;
- Impose confidentiality obligations on all personnel who process personal data;
- Ensure the security of the personal data that it processes;
- Abide by the rules governing appointment of sub-processors;
- Implement measures to assist the controller 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.



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 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, will suffice. In the absence of further guidance, in practice, this may well depend on a risk assessment of the nature and type of processing at hand. Multi-tenanted platform service providers (such as cloud providers), for example, and other processors with complex supply chains will no doubt struggle with these requirements. It is also difficult for controllers and prime processors to be able to impose these requirements on leading service provider sub-processors who contract on their own suite of standard terms, with less flexibility to tweak them.

Audit rights – an extension of the accountability principle:
Amongst the information requirements to demonstrate compliance with Article 28, the GDPR also requires processors to allow for, and contribute to, audits (including inspections) conducted by the controller or a chosen auditor. The ICO guidance states that this requirement will mean that processors should keep records of its processing activities. It is worth considering the inclusion of any such provisions in light of existing information, record keeping or audit provisions in a data processing agreement.

Innegotiating these provisions it is also worth considering how prescriptive the audit process should be; how often is an audit permitted? At who's cost? What is the scope of the audit? Who should the auditor be and how should they be appointed? Can the controller rely on the results of an audit carried out by the processor?

Again multi-tenanted platform service providers, in particular, tend to strongly resist audit rights due to by logistical challenges inherent in the nature of the services they offer; however parties may seek to compromise by using a jointly appointed or supplier-appointed independent third party auditor.

Security measures – what is appropriate?:
The processor is subject to the same security requirements as the controller; it must take all measures required under the security provisions in Article 32 – namely to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing. Whilst the GDPR goes on to set out a non-exhaustive list of measures (including pseudonymising and encrypting personal data) it is not prescriptive as to what measures an organisation actually needs to implement to comply with this obligation, as this will need to be assessed on a case by case basis. Related challenges for negotiation in a supply chain context therefore include: what security requirements this obligation actually imposes in practice (taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of processing, as well as the risk associated with the loss or disclosure of personal data); whether the processor needs to comply with detailed security requirements imposed by the controller; and how parties can actually evidence compliance with these requirements. Also refer to the section below titled "*Additional processor protections?*"

A processor is also required to assist the controller in ensuring compliance with its data breach notification requirements (both to the supervisory authority and the data subject), taking into account the nature of the processing and information available to the processor. The ICO has indicated that it will issue more prescribed guidance in due course on the specific requirements, however, in the meantime, ambiguity remains over how much assistance is required by this obligation, whether "reasonable" assistance will suffice, whether the processor should be entitled to charge for such assistance and whether this places additional regulatory responsibility on the processor for the controller's own compliance.

Gold-plating:
The ICO Guidance re-iterates that the Article 28 provisions are very much a minimum set of terms; controllers and processors may wish to supplement them with additional processing provisions. Whilst controllers continue to have more extensive liability than processors under the GDPR, the former are still reliant on processors to assist them in complying with their legal obligations. As a result, there are likely to be certain areas where controllers require processors to fulfil obligations that go beyond those set out in the Article 28 mandatory provisions, in order to comply with the GDPR.

A prime example is the requirement to notify a supervisory authority of a personal data breach; a controller is required to do so "without undue delay" and, where feasible, no later than 72 hours after having become aware of it (unless it is unlikely to result in a risk to the rights and freedoms of data subjects). Whereas a processor is simply required under the GDPR to notify the controller "without undue delay" after becoming aware of the personal data breach (in addition to complying with the "assistance" obligation referred to above). Controllers may require further protection that the processor will notify them with enough time for the controller to meet its statutory obligation and specify a time period within which to do so (for example within 24 hours of becoming aware of the breach). The Article 29 Working Party guidance on personal data breach notifications confirms that the processor has an "important role to play" in this regard, suggesting that the processor "promptly" notifies the controller.

It is often these "gold-plated" provisions that are the subject of most negotiation in data processing agreements as well as the related provisions addressing the respective risk allocation of the parties referred to opposite.

Impact on supply chain protection and allocation of risk

Early sight of a weak link in the supply chain

The change in risk profile of controllers and processors, gives rise to a need for clear contractual allocation of responsibility and liability for data protection between the parties (and any sub-processors). In our experience it is also important to balance this risk allocation against a co-operative controller/processor relationship, for example if there is a cyber incident, to best resolve any potential issues in the quickest and most effective manner.

The December 2013 data breach on Target Corporation (reportedly affecting approximately 110 million customers) is a prime example of where a third party contractor could be a weak spot in an organisation's data protection and security supply chain. In that case, an HVAC contractor with access to Target Corporation's network was reportedly the gateway used by criminals to compromise Target's systems and ultimately install malware on a large proportion of point of sale devices just before the traditional Black Friday sales. This allowed the criminals to farm huge amounts of personal data from credit and debit cards.

In addition to the requirements mandated by the GDPR and any guidance, it is therefore common practice to undertake due diligence and a related risk assessment of each contractual relationship in the supply chain, followed by imposing data protection or cyber security requirements on suppliers appropriate to that risk. These protections should extend both up and down the entire supply chain (refer to "Sub-processors" above). In lieu of any approved "code of conduct" or "certification" being issued for processors to adhere to in order to demonstrate sufficient guarantees of GDPR compliance (as envisaged under the GDPR), due diligence goes some way to providing further comfort in this regard.

The GDPR also enshrines concepts such as privacy and security by design (requiring controllers to think about privacy and cyber security at the inception of projects and systems) and data protection impact assessments (largely in respect of higher risk data processing and to be undertaken prior to commencing the processing). It is therefore unsurprising that we are starting to see more organisations seek early engagement with potential suppliers, as well as data protection and cyber security requirements being addressed as key criteria in an RFP. This can empower a customer at the early stages of a procurement and give them leverage to consider alternative providers if dissatisfied with a particular supplier.

Risk allocation shift – emerging market practice?:
Article 28 is silent on liability between the controller and processor. This is unsurprising given the bespoke nature of risk allocation between the parties and the need to balance and consider a variety of factors on a case by case basis, including the nature of the service provision and the relative exposure and mitigation measures available to each party. The liability regime falls outside the prescriptive mandatory provisions and therefore, theoretically, outside the scope of any re-papering exercise or re-negotiation of data processing provisions. However, we are now seeing a shift in the focus on, and related negotiation dynamic regarding, liability and indemnity protection. Whilst it will be some time before we are able to determine the approach to market practice, one thing is certain; liability regimes for breach of data protection provisions are being elevated in importance for both parties.

A position of uncapped liability for data protection breaches is definitely not market practice in the GDPR era. On the controller side, controllers are pushing for data protection breaches to be carved out of the overall liability cap; requesting high value "super caps" instead, in line with the higher penalties under the GDPR. On the processor side, processors are strongly resisting high caps for all but the most complex, high value and high risk data processing agreements This approach is reflected by requests from controllers for more extensive contractual insurance obligations and a need for both parties to review the extent of their existing insurance coverage (including cyber liability insurance in the event of a data breach, given potential gaps in some traditional insurance policies).

In certain markets (particularly in the United States) we are also starting to see data loss being included as a specific head of loss under which a customer is able to claim under the data processing agreement. As well as specific heads of loss being called out in the context of indemnities for data protection breaches (e.g. fraud prevention costs, breach notification costs).

Confidentiality: a back route to unlimited liability protection?:
Whilst processors are now resisting uncapped liability for breaches of data protection obligations, the offer of unlimited liability for breach of confidentiality often remains unchanged. Some controllers are therefore considering whether a data protection breach could fall within the scope of a confidentiality breach under the agreement as well and, in turn, within the scope of a more favourable liability cap. Whilst personal data breaches will not always amount to breaches of a confidentiality clause, a number of data breaches could well fall within scope. As a knock-on effect we are therefore starting to see increased scrutiny of confidentiality provisions and liability as well.

How does a contractual liability regime now align with the statutory liability regime?:
In the event of breach involving both a controller and a processor, we anticipate that the regulator would investigate and apportion liability between the parties. Data subjects are now also entitled to claim directly against the processor or the controller for damage suffered from non-compliance. Both controllers and processors can however be exempt from liability if they were "not in any way responsible for the event giving rise to the damage" (potentially a relatively high threshold) – in which case one party is able to claim back from the other party all or part of the damages or compensation paid. The same principle applies in respect of liability between processors and sub-processors. Of course, this statutory apportionment of liability under the legislation gives rise to uncertainty as it remains to be seen how it fits with any contractual apportionment or limitations of liability in the data processing agreements.

General approach to negotiating processor clauses – early emerging trends

Re-papering: Battle of the forms:
Failure to implement Article 28 provisions gives rise to an automatic breach of the GDPR, with the potential tier two fine (of up to €10,000,000 or 2% of annual worldwide turnover, whichever is greater) acting as a clear incentive to undertake the re-papering exercise. As a result it is not uncommon for the controller to initiate the process for varying data protection provisions and, in some cases, prepare the necessary addendum or side letter in an effort to control the scope and positions taken in the document. However, it is equally possible for the supplier to initiate the process itself, for example as part of a review of its own suite of standard terms, particularly where the service being provided is an "off-the-shelf" standard commoditised offering to customers. GDPR-compliant terms are also a way for suppliers to distinguish their offering in the market, particularly those with a highly regulated target client base.

There is some ambiguity around whether it is the controller or the processor's responsibility to put a data processing agreement in place. Article 28 states that "processing by a processor shall be governed by a contract" without referring to which party is responsible for doing so. It may be that this ambiguity in the legislation is deliberate to enable regulators to investigate whichever party is effectively more at fault for not putting the data processing agreement in place. Either way, in the interests of certainty it is arguably in both parties' interests to update agreements in line with the new GDPR requirements.

Re-papering: When suppliers won't accept the mandatory clauses:
Given the relatively high profile nature of the GDPR and the two year implementation period, most suppliers should understand the need for data processor provisions – albeit with differing views on the extent of those provisions. However, in certain sectors, we have started to see suppliers positioning themselves as controllers rather than processors (whilst also asking for a commitment from the customer in relation to lawful disclosures of data). Whilst this position avoids the need for Article 28 provisions, the underlying controller-to-controller arrangement would still require review and likely re-negotiation to ensure GDPR compliance. Given the factual nature of the status of each party, in these circumstances it is worth requesting evidence to substantiate any assertion that a supplier is a controller and, if satisfied, consider drafting to cover both scenarios.

Additional negotiation time:
The additional mandatory requirements under the GDPR (as well as measures that controllers seek to incorporate to enable their own compliance) have the potential to give rise to more detailed data processing provisions and, in turn, more protracted negotiations going forward. The GDPR contemplates standard contractual clauses approved by the European Commission for Article 28 purposes – an action that, if exercised, may certainly whittle down some of the more minor points in dispute, in the same way that the current standard contractual clauses can do for international transfers of personal data outside the European Economic Area. However, we have not yet seen any move by the European Commission to create these standard contractual clauses and, given the potential for "gold-plating" provisions referred to above, there is potentially a limit to how far any such templates will be able to assist in any event.

Looking ahead: watch this space

Arguably the more prescriptive nature of the controller/processor relationship under the GDPR and the closer scrutiny warranted by both parties, is no bad thing for ensuring supply chain protection and further building trust and relationships with data subject. The GDPR makes it very clear that whilst risk can be outsourced to others in the supply chain, overall statutory responsibility cannot be outsourced.

The ICO currently prides itself on its "pragmatic and proportionate" approach to enforcement, with high fines being regarded a method of last resort. To date, the ICO has taken a light touch approach to investigating and enforcement action in respect of data processing arrangements as well. It remains to be seen whether this will continue once the GDPR applies, as well as the approach adopted by overseas regulators who may be more willing to invoke monetary penalties for non-compliance. As we look ahead to 25 May 2018 and beyond, one thing is for sure, with the potential for increased enforcement power and higher maximum fines, plus the enhanced awareness of data subjects' rights and their ability to exercise those rights, controllers are likely to be held to account over their processing activities now more so than ever.

GDPR re-papering – how to navigate the minefield

The re-papering exercise is clearly a vital step in any GDPR compliance programme, but it is also important in the context of managing data protection and cyber supply chain risk. There is no regulator-mandated approach. However, in our experience we suggest using a structured approach to navigate this exercise and set out some recommendations below.

Demonstrating compliance

Not only does this approach help to manage the logistics of a large scale exercise, but the process and related documentation (including the privacy impact risk assessment) also go some way to assist with demonstrating compliance with the Article 28 requirements – both in the run up to the May deadline and beyond. In fact the Information Commissioner, Elizabeth Denham, last year sought to allay fears over a hard 25 May 2018 deadline; confirming that compliance should be an "evolving...ongoing effort", with the ICO taking into account whether an organisation can demonstrate effective accountability arrangements when considering any regulatory action. The Information Commissioner expressly referred to an organisation being able to show it has been "thinking about essential elements" (reviewing third party processor contracts for GDPR compliance was specifically referenced as an essential element) and related responsibilities within the business.

Due diligence

The key is to clearly **understand all of your third party relationships**, in particular to identify: (i) what contracts exist that involve the processing of personal data? (ii) with whom? and (iii) the subject matter of each agreement (including the nature and extent of personal data being processed). The latter is of particular importance to indicate the relative data protection and cyber related risk associated with the processing activities under a particular arrangement. Which, in turn, informs the most appropriate next steps. Given the somewhat daunting task (for larger organisations, in particular) of ensuring huge volumes of third party contracts are GDPR-compliant by the May deadline (and beyond), categorising these contracts according to risk profile allows an organisation to focus time, resource and cost efforts appropriately.

Templates

A market practice is developing of using an **addendum or side letter** to vary existing data protection or cyber related provisions, with further variants of these templates depending on the relative risk profile of the arrangements in scope. For example, a comprehensive longer form addendum that "gold-plates" the minimum GDPR requirements may be appropriate for a smaller number of higher risk agreements (involving the processing of a huge amounts of personal data, which could include sensitive personal data), compared with a shorter form addendum that covers the bare minimum GDPR requirements and may be more appropriate for a high volume of lower risk arrangements (involving incidental processing of limited amounts of personal data).

Process Manual

A process manual provides a much needed **framework around the logistics of a large-scale exercise**, to keep up the momentum of the project, ensure it runs effectively and efficiently within target time scales and that any issues are resolved swiftly. The manual will be of particular relevance where the exercise has been outsourced to a third party provider (such as a law firm). Among other areas, it can be used to identify the risk categories of contracts envisaged, allocate responsibility between the project team (including supplier relationship owners across the many third party contracts), set out template emails to suppliers, process steps and timeframes for negotiation including when to send follow up emails and when an escalation procedure is invoked (for example due to lack of counterparty response or failure to agree a position following a certain number of iterations). Again the process and triggers are likely to differ depending on the risk profile of the arrangement in question.

Playbook

A playbook sets out the parameters within which **the project team are able to negotiate** the addendum or side letter. Given tight time frames, the playbook would usually envisage one or two iterations of amendments with a fall-back position in respect of each iteration for each provision. This allows for a consistent negotiation approach across all suppliers and, alongside the templates, can be a useful starting point for negotiating data protection provisions in an organisation's standard forms going forward as well. Low risk arrangements may be non-negotiable or subject to even more limited iterations.

Beyond 25 May 2018

Many aspects of the process referred to above remain equally relevant to new procurements entered into after the 25 May deadline as an indication of good industry practice. The risk assessment exercise, in particular, will continue to be important to the approach adopted in respect of any such new arrangements.

Benefits beyond just GDPR compliance

The key to GDPR compliance is not just in satisfying a check list of requirements but requires a "whole of business" effort to change an organisation's attitude and operational approach to data, as well as the way in which compliance filters through an organisation. As well as the challenges that the GDPR brings, a well-run GDPR programme (and in turn any negotiation of data processing provisions and re-papering exercise) also brings with it benefits beyond simply achieving compliance.

Contractual "health-check"

When undertaking any review of third party agreements or any repapering exercise in relation to the GDPR, it may also be prudent to consider other key topical issues in parallel, to avoid the need to revisit each contract more than once (which will no doubt be resisted by a supplier) and seek to maintain leverage when negotiating any amendments.

Prime examples of current areas to also focus on and conduct risk assessments, include:

- **Cyber security** issues – to take account of the implementation of the **Network Information Security Directive ("NISD"),** which recently applied to "operators of essential services" and "digital service providers" on 10 May 2018. **The next instalment of our practical GDPR series of briefings will take a closer look at the nexus between data protection and cyber security**;
- **Brexit** related considerations – to seek to **future-proof agreements** going forward to take account of the UK's exit from the European Union, potentially any transition period agreed with the European Commission and to avoid unintended or undesirable consequences (for example unintended termination triggers or uncertain or undesirable definitions), as well as considering any contract migration to take account of any business relocation; and
- In due course, **e-privacy** issues – with the ongoing **overhaul of the e-privacy framework** still to be finalised and still currently the subject of debate at the European level.

HSF market leading re-papering offering

Our cross-disciplinary Data Protection, Privacy and Cyber Security practice is able to offer pragmatic, market-leading, cost-efficient solutions to tackle any re-papering exercises – including working with our low cost Alternative Legal Services teams and aided by cutting edge technology solutions and process improvement techniques. No matter what stage your organisation is currently at in implementing its GDPR strategy and whether you are in need of a GDPR, NISD, Brexit, e-privacy or any other review and re-papering of large volumes of your supply chain agreements, we are perfectly placed to ease the burden.

Key contacts

Miriam Everett
Consultant, Head of Data Protection and Privacy
T + 44 20 7466 2378
miriam.everett@hsf.com

Claire Wiseman
Senior Associate, TMT & Data
T +44 20 7466 2267
claire.wiseman@hsf.com

Nick Pantlin
Partner, TMT & Data
T + 44 20 7466 2570
nick.pantlin@hsf.com

Marcus Turle
Consultant, TMT & Data
T +44 20 7466 2886
marcus.turle@hsf.com

© Herbert Smith Freehills LLP 2018