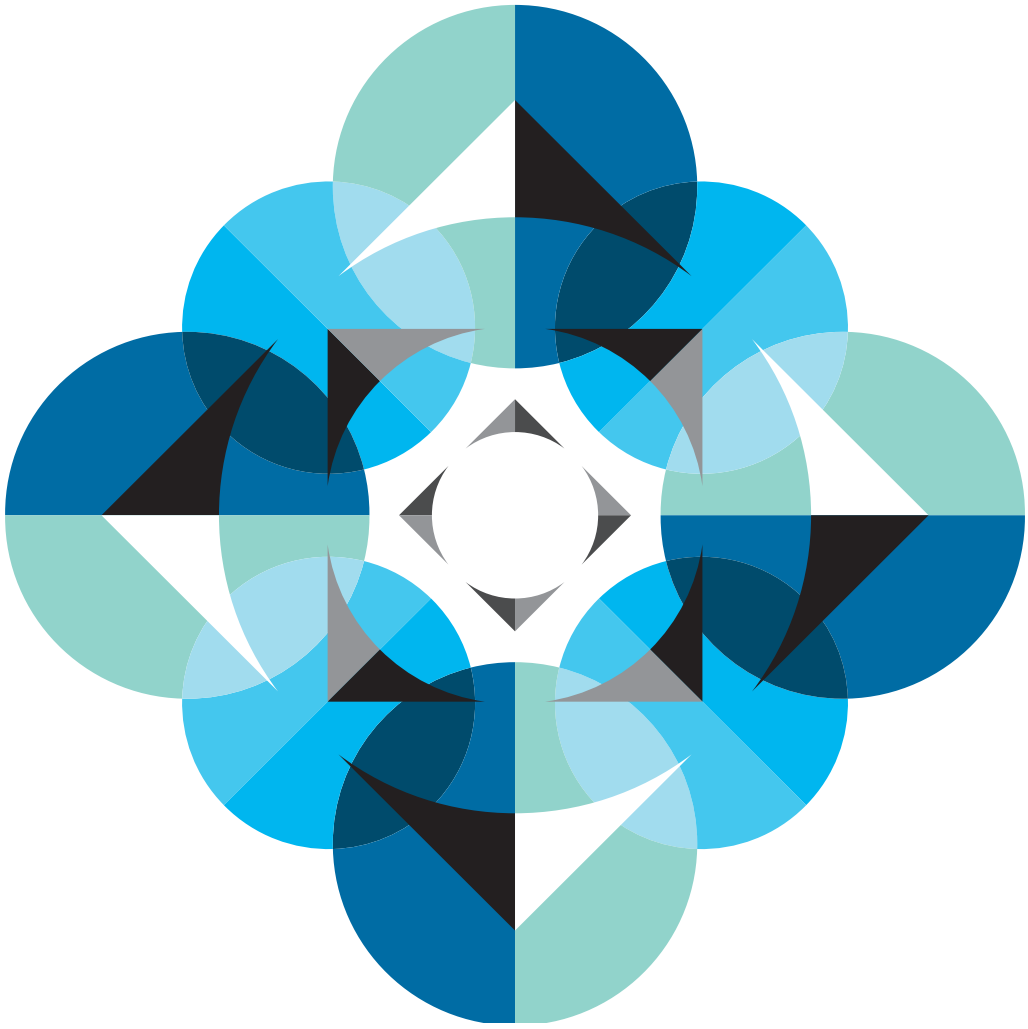
LEWIS SILKIN

Tech solution providers
Getting Data Protection Ready



The General Data Protection Regulation ("GDPR"), takes effect from 25 May 2018, and brings about important privacy changes that will impact most businesses, particularly providers of technology, telecoms and data related platforms, solutions and services. The GDPR is lengthy, complex and prescriptive - this gives rise to new challenges for tech providers that need careful thought, largely to minimise risk and additional cost.

In this note, we seek to give those involved in the provision of tech and data related platforms, solutions and services (such as data storage, SaaS providers, managed service providers, ISPs, telcos and social networking platforms) a flavour of the key changes arising from GDPR. For simplicity, we refer to this broad body of providers as 'tech providers'.

We focus on the tech provider's obligations as a 'data processor'. Of course, in several instances, a tech provider may also be a data controller acting on its own or a joint data controller or data controller in common with a third party, but that is not the focus here.

It is likely that customers will look to share the burden of their GDPR obligations with their tech providers. We therefore look at the key GDPR challenges facing these processors in two parts:

a) direct GDPR obligations

b) indirect GDPR obligations likely to arise in the context of vendor/customer contracts

Although GDPR is a European Regulation, its far reaching territorial scope means that tech businesses located outside of the EEA will also be caught if they are processing personal data of EU citizens

Direct obligations on processors

Increased cost and exposure

Under GDPR, processors will now, for the first time, become directly accountable to the ICO or other regulators for compliance with certain obligations. These include obligations on processors to:

a) have in place adequate security measures;

b) delete or return personal data on request and/or contract end;

c) keep comprehensive records of data processing activities;

d) co-operate with, and provide access rights to systems, premises and records, to regulators and data controllers alike; and

e) ensure that their obligations are flowed down onto sub-processors (sub-contractors and some suppliers) and, in practice, take on responsibility for sub-processors.

Any consumer (or other person) who suffers damage as a result of breach of GDPR has a right of compensation from the controller or processor for breach of their respective obligations. However, a processor can also be liable where it has acted outside or contrary to the lawful instructions of the controller.

GDPR makes data processors directly liable for fines for breach of their obligations up to the greater of 2% of worldwide turnover and €10 million. In some cases, those numbers increase to 4% and €20 million respectively, for example where a processor makes unauthorised data transfers outside of the EEA or where it acts outside the lawful authority of the controller.

We'd be surprised if the ICO flexes the full might of its new muscles in 2018, but the fining ability nonetheless presents a significant new exposure. Tech providers should be taking steps to see how their exposure can be minimised.

One key step is to build or adapt solutions that minimise the amount of personal data being processed and/or to encrypt data and to put corresponding responsibilities on customers. Encryption may not in many cases be feasible and may have an adverse effect on the performance of software or SaaS solutions. If tech providers consider this route, they need to think about building solutions that ensure equal performance for encrypted data and where they put the onus on customer to encrypt data, make it easy for the customer to do so. Encryption is also likely to be a key way of aiding compliance with a processor's obligations to keep data secure (see further below).

Other risk reduction techniques might include seeking to reallocate contractual risk to customers (on the basis that the processor is now directly accountable to the regulator) (e.g. cross indemnities or widening exclusions of liability) and, of course, adequately backing-off risk with suppliers and sub-contractors. The existence and adequacy of product liability, professional indemnity, business continuity and data breach insurance coverage should also be considered.

Sub-processors

In addition to having responsibility for sub-processors, a processor is also required under GDPR to obtain the data controller's prior specific, or general, written consent if it wishes to delegate any processing activities. Consent can be withdrawn where general consent has been obtained and the tech provider needs to add or change a sub-processor, meaning compliance is not straightforward. Many providers may not know up front who all of their sub-processors will be for the contract life, such as with a provider of hosted cloud solutions, where several layers of providers might be involved - compliance in some cases may require some 'out of the box' thinking not only in respect of GDPR requirements but also in respect of customer contract compliance and related negotiations.

Tech providers, especially those offering cloud solutions, should consider including rights of termination where consent to sub-processing is withdrawn to: a) act as a deterrent; and b) avoid any

potential breach of contract claim for not being able to perform the services or deliver the solution as agreed.

Heightened focus on security

Data security is now more than ever a concern for consumers, customers and governments, so it is no surprise that one of the main obligations on data processors is to ensure adequate security.

Under GDPR, processors must implement appropriate technical and organisational measures to ensure personal data is kept secure (taking into account factors such as state of the art and cost). Tech providers will be familiar with this obligation as, in most cases, it will already be flowed down to them contractually. What is more challenging is the fact that GDPR is more prescriptive than the DPA and states that these measures may include:

a) encrypting (and pseudonymising) personal data;

b) having the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;

c) having the ability to restore availability of, and access to, personal data in a timely manner in the event of a physical or technical incident; and

d) a process for regularly testing, assessing and evaluating the effectiveness of all these measures, to ensure data security.

This is onerous stuff, which needs to be factored into pricing models. The requirements may force a fundamental rethink/restructuring of the viability of certain offerings, including tiered offerings. Tech providers need to assess whether their solutions achieve ISO 27001/27002 or equivalent standards or consider obtaining such certifications. One workaround may be to implement the highest possible levels of security for all offerings, whilst passing on costs to customers. Where tiered offerings are used, should those providing less security be restricted to low risk scenarios or data that is not sensitive? What is certain is that different contractual provisions will be needed to help manage the increased risk for tech providers, especially where costs cannot be passed on.

GDPR opens the door to the possibility of industry bodies devising industry-recognised security standards - so it may be in the self-interest of tech providers to be proactive and to collaborate with other tech providers/ industry bodies to amend/develop standards that are GDPR fit-for-purpose but at the same time not overly burdensome or costly to implement. These can then be used as a proactive tool to present to customers, including as part of sales pitches

Appointment of a DPO

Tech providers whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale will now have to appoint a data protection officer ("**DPO**").

The DPO must be a person with expert knowledge of data protection law and practices, whose job is to monitor internal compliance with the GDPR. As the DPO must not have a conflict of interest in conducting his/her role as a DPO, a CEO, FD, IT Director or Marketing Director can't hold the role. Note that a DPO cannot be penalised or dismissed for performing their duties.

According to Article 29 Working Party guidance, "core activities" won't include support functions such as HR and payroll, but could include data collected as an inextricable part of the pursuit of business goals. For example, if a tech provider offers an online HR solution to corporate customers, the processing of employee data is likely to be a core activity.

The guidance states that "regular and systematic monitoring" will include internet tracking and profiling for the purpose of behavioural advertising, providing telecoms services, credit and risk assessment, location tracking, loyalty schemes and the operation of smart appliances. What is meant by "large scale" hasn't been defined, but factors to consider include the number of individuals monitored, the geographic extent and permanency of the personal data collected and the volume or range of data processed. Further, as previous drafts of GDPR did include a definition of "large scale", tech providers should look to those for assistance.

Record keeping and audit requirements

Controllers will no longer be required to notify the relevant data protection authority that they are a data controller.

However, controllers and processors are each required to maintain detailed records regarding their respective data processing activities and to be able to evidence compliance with the GDPR. The new requirements are likely to be more onerous in most cases and tech providers need to ascertain how they will comply, which may require advance discussions with customers, especially where customer requirements change or are made with little notice. For example, cloud providers' systems may need to be engineered to increase logging/recording, which is good for transparency but may increase cost.

Data processors may wish to consider whether to put in place self-certification audit processes to meet the new audit requirements imposed on both controllers and processors under GDPR.

Indirect obligations on processors arising through vendor management

Privacy by design

A key over-riding principle of GDPR is the concept of 'privacy by design'.

This means that businesses need to put in place processes and procedures to ensure **privacy by design** and **by default**. Tech providers must have data privacy at the forefront of their minds when building solutions that process data. For example, think about ways in which the volume of personal data can be minimised, including through anonymisation and pseudonymisation techniques or simply being more focused about the data that is really needed.

LEWIS SILKIN

Also, consider how the responsibility for this filtering process can be passed on to the customer.

Customers will be required to conduct **privacy impact assessments** ("PIAs") to assess the impact of proposed data processing activities each time they plan or propose a new technology, solution or offering that is likely to result in a high risk to the rights and freedoms of natural persons. However, much of this burden is likely to be felt by tech providers. The impact (especially in terms of cost and time) should be factored by tech providers into their offerings. Although PIAs are already considered good practice, it is seems likely that the formalised PIA requirement will add to the sales lead-time. Proactive tech providers are already choosing to pre-empt RFP and similar questions on the extent to which privacy by design and default has been factored into their solution by seeing if they can offer ready-made answers in advance.

New data subject rights

GDPR codifies a number of existing data subject rights and introduces some new rights, all of which tech providers need to be alive to.

These rights are important and include a right to object, right to be forgotten, right of rectification and right of access. Although some of these rights exist now, data controllers will be required to ensure that all data subjects are aware of their rights which, in turn, mean that the likelihood of them being exercised is greater, and will impact the cost of compliance for tech providers.

End consumers and other data subjects also benefit from a new data portability right which gives them the right, in certain circumstances, to request that the data controller provides them, in machine readable format, with all personal data provided to the data controller by the data subject. The Article 29 WP guidance suggests that this requirement can extend to information generated by the data controller about the data subject. Many data controllers will contractually be backing-off this obligation onto tech providers. Tech providers should consider with their customers the extent to which data may be required and not only ensure that their systems and processes can accommodate the request but that they are not out of pocket as a result, especially given the new duty on data processors to co-operate.

Compliance here could present a real headache for cloud providers due to the multi-layered nature of cloud services (especially where the likes of AWS and Microsoft Azure won't negotiate terms). One solution, cost permitting, may be to develop a self-help portal allowing customers the facility to exercise their rights with reduced manual involvement from the tech provider.

Data breach notification

GDPR introduces mandatory data breach notifications to the regulator within 72 hours and in more serious cases requires data subjects to be notified.

Although the primary obligation to notify the regulator (and data subject) rests with the data controller, data processors will be required to notify the data controller of data breaches without undue delay. Staff training should, in particular, be implemented to ensure this can be achieved.

All providers, especially those operating acrossthe EU, should have joined-up and well-rehearsed data security and breach procedures in place which can enable breach notifications to be made quickly, including having appropriate external support in place, such as PR and DR resources.

Forced appointment of a DPO

As mentioned, tech providers may be required to appoint a DPO. However, tech providers should be alive to customer pressure on them to appoint a DPO. Appointing a DPO 'for the sake of it' means that the organisation will then have to comply with the burdensome GDPR DPO requirements, so careful thought is required as to whether (for the sake of vendor management only) a DPO really does need to be appointed.

Closing thoughts and next steps

While well intentioned, the GDPR is too prescriptive for 21st century tech providers, especially for cloud solution providers. Until data protection laws become more technology-neutral, tech providers must work out how best to provide GDPR compliant offerings. Taking the time now to adjust offerings, systems, processes and (importantly) contracts, will help tech providers not only to manage their own risk and cost base, but also to improve the attractiveness of their offerings and minimise lag in the sales process. All this should, of course, help to improve (or at least reduce the impact on) the bottom line.

For more information contact:

Bryony Long
Senior Associate

+44 (0) 20 7074 8435
bryony.long@lewissilkin.com

James Gill
Partner

+44 (0) 20 7074 8217
james.gill@lewissilkin.com

@LewisSilkin
linkedin.com/company/lewis-silkin