CharlesRussell Speechlys

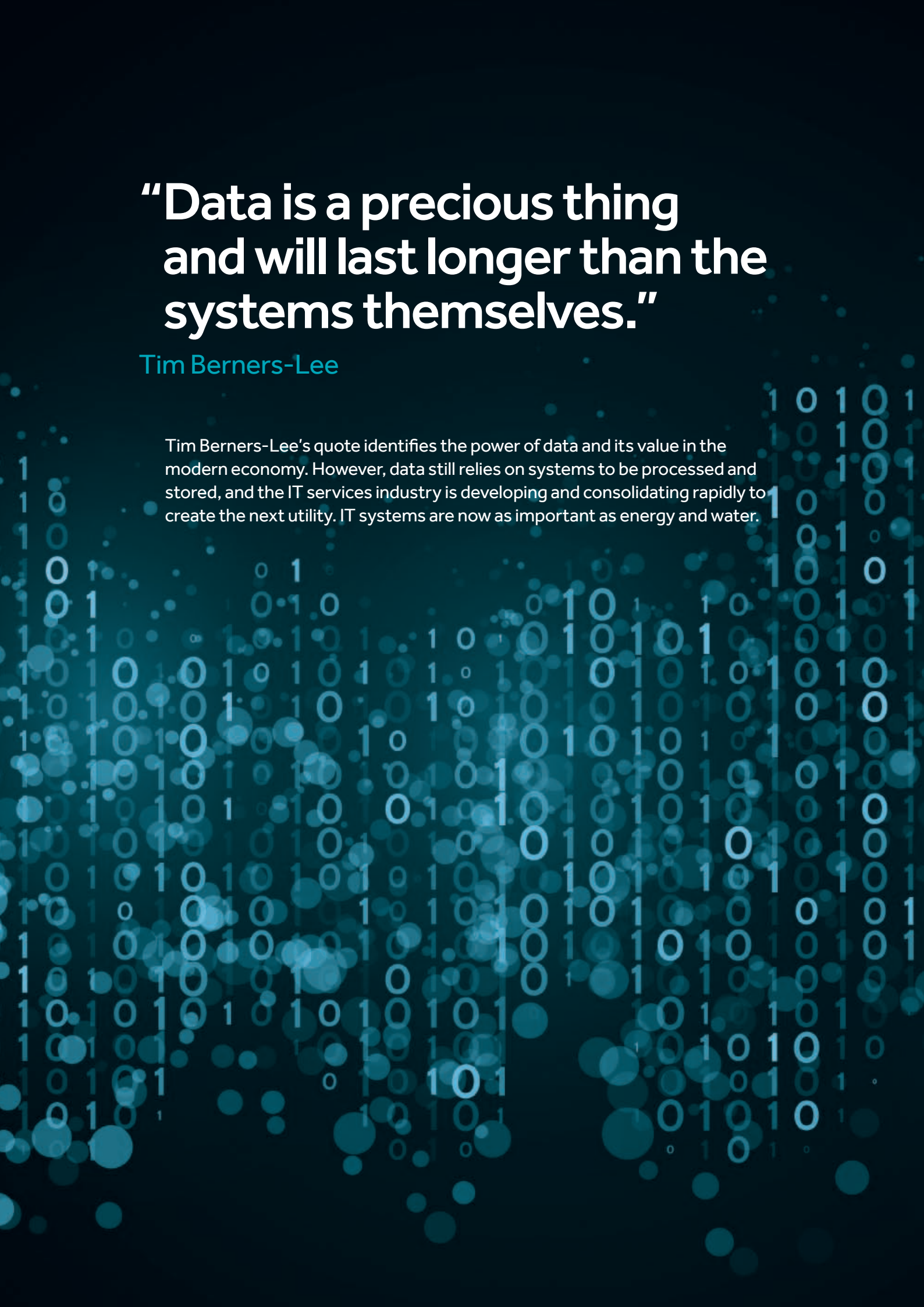
GDPR for IT Services

Keeping compliance at the heart of the controller/ processor relationship

“Data is a precious thing and will last longer than the systems themselves.”

Tim Berners-Lee

Tim Berners-Lee’s quote identifies the power of data and its value in the modern economy. However, data still relies on systems to be processed and stored, and the IT services industry is developing and consolidating rapidly to create the next utility. IT systems are now as important as energy and water.



Introduction

The General Data Protection Regulation (GDPR) (Regulation (EU)2016/679) of the European Parliament and of the Council comes into force on 25th May 2018 repealing Directive 95/46/EC. GDPR is intended to be a data protection regulation for the modern economy, fully embracing the advent of the cloud and distributed computing. That said, GDPR does not mention IT systems specifically, but the technical and organisational measures which are required to protect personal data are to a very significant extent IT related. They cover:

- systems to hold and process data;
- monitoring and reporting on compliance of those measures, including training and monitoring of policies and procedures; and
- detecting data breaches and security incidents.

These obligations will be repeated in the UK's post-Brexit law. Recently published in draft, the Data Protection Bill, which will become the Data Protection Act 2017, incorporates the articles of GDPR into UK laws, and supplements the GDPR with UK derogations in order to be read with GDPR.

Businesses who do not outsource their IT or management of personal data are responsible for compliance as controllers of the data. Many businesses now outsource all or part of their IT services (the Uptime Institute's 2016 Data Center Industry survey estimated 70% of IT is held in enterprise owned data centres, but believes this is an underestimate: the trend to outsourcing is accelerating).

Those businesses who do outsource their data to cloud or IT service providers are reliant on data processors, and often a complex chain of sub-processors engaged by the processors for specific functions, including cloud based software services and infrastructure, networking and communications and data analysis functions. IT services providers can perform either discreet services or fully outsourced services covering the entirety of a business's IT functions.

IT services obligations will intensify

As such, GDPR compliance obligations will fall on the IT services business sector very heavily. IT services providers will also have to protect their own data which they process as data controller "and practice what they preach", as well as having to create a safe environment for controllers' data as data processor.

Under current law, the roles of the data controller and data processor are well understood and these have led to standardised contractual clauses and information security policies produced by data controllers which in many cases effect a flow down of the responsibility for compliance with personal data to the data processor.

The risks under the existing legislation are not insignificant to IT services providers but the processor is not directly liable to the data subject under existing law, and except in the financial services sector, fines and penalties are limited to £500,000 in the UK. In contracts between controller and processor, liability for breach of confidentiality and potentially breach of data protection is often unlimited or subject to separate higher "super caps" to the general limit of liability for service failure.

Fines and penalties escalate under GDPR

GDPR enables, and requires, IT services businesses as data processors to assist controllers to comply with the new law. The risk to IT services providers is significantly increased under GDPR because processors are now directly liable for failures to comply with the Regulation, and processors are also potentially jointly and severally liable with the controller where both the controller and the processor are involved in the same processing, for damage caused by that processing. Also, the fines and penalties are very significantly increased, for certain offences up to 4% of global worldwide group turnover or €20,000,000 whichever is the greater.

Contents

A framework for IT services businesses

The paper looks at measures processors can take to assist controllers to comply with GDPR and to adequately manage the associated risk.

The paper does not aim to be comprehensive but sets out a framework to identify and manage legal risk for detailed program implementation according to the precise nature of the IT services performed. We hope this paper provides tailored commentary for the IT services industry which performs such an integral contribution to the UK economy.

The provisions of GDPR are supplemented by Part 2 Chapter 4 of the Data Protection Bill for the UK.

Controller responsibilities

These are determined by Article 24.1, as follows:

"Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

The definition therefore places the primary responsibility for processing in accordance with the Regulation on the controller, who has to implement appropriate policies in order to comply with its obligations.

Joint controllers

Joint controllers must determine their respective responsibilities "in a transparent manner" under Article 26.1. The essence of this arrangement must be made available to the data subject who can exercise rights in respect of and against each of the controllers.

Processor obligations

Processor obligations have been greatly extended by Article 28. Article 28.1 provides:

"where processing is to be carried out on behalf of a controller, the controller shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of [GDPR] and ensure the protection of the rights of the data subjects."

As before, processing must be governed by a written contract between controller and processor. However, Article 28.3 provides a significantly more detailed set of requirements (a – h), which must be reflected in the contract. The Information Commissioner's draft guidance published in September 2017 provides useful summaries of these measures.

The ICO paper states that contracts between controllers and processors:

- ensure that they both understand their obligations, responsibilities and liabilities
- help them to comply with the GDPR
- help controllers to demonstrate their compliance with the GDPR and
- may increase data subjects' confidence in the handling of their personal data.

Compliance can be evidenced by simply repeating these clauses in the contract, but a wider reading of the Regulation is necessary to ensure that true data protection compliance is achieved.

Under the radar – close cooperation required

One of the provisions that has not attracted very significant commentary is Article 28.3(f) – this requires the processor to *"assist the controller in ensuring compliance with the obligations pursuant to Article 32 – 36 taking into account the nature of the processing and the information available to the processor."*

Article 29 requires the processor and any other person acting under its authority with access to personal data not to process those data except on instructions from the controller unless required to do so by a Union Member State law. There is a general obligation of co-operation in Article 31 which must not be overlooked, which provides that the processor and controller must co-operate on request with a supervisory authority in the performance of its tasks.

There is perhaps an ambiguity in the Regulation regarding the cooperation the processor must provide. While Article 28.3(f) requires the processor to assist the controller in ensuring compliance with Articles 32 to 36, Article 32.1 states that the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. These provisions will need to be carefully considered in light of the particular IT services offered.

In many cases, particularly in relation to infrastructure services only, the measures proposed in Article 32 including pseudonymisation, encryption and data restoration will not be appropriate for the processor to operate at all. Service descriptions should be clearly drafted and records kept to assess the appropriate level of security required for the design of each service. This protects against accidental or unlawful destruction, loss, alteration unauthorised disclosure of or access to personal data processed.

The requirement for IT services providers to assist the controller is potentially difficult. The paper will look at this in more detail in the section below.

Taking steps to identify and manage risk

Pre-contract

Pre-contract, controllers are under a general obligation under Article 25 of GDPR to implement data protection by design and by default. Both of these measures apply technically only to controllers, but processors must ensure that services they design for controllers will assist the controller to comply with the general concepts of data protection by design and data protection by default.

Data Protection by design and by default

Data protection by design requires a controller, *"taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for rights of freedoms of natural persons posed by the processing shall, both at the time of determination of the processing and at the time of processing, implement appropriate technical and organisational measures, such as pseudonymisation which are designed to implement the data protection principles in an effective manner in order to meet the requirements of the GDPR and protect the rights of data subjects".* (Article 25.1)

Data protection by default requires appropriate technical and organizational measures to be implemented ensuring that by default only personal data which are necessary for each specific purpose of the processing are processed. This covers the amount of data collected, the extent of processing and the period of storage and accessibility. (Article 25.2)

Data Protection Impact Assessments are required in more limited circumstances, where the processing is likely to result in a high risk to the rights and freedoms of natural persons.

How to comply

In order to achieve compliance with data protection by design and by default an impact assessment will need to be created with respect to the relevant service, or an approved certification mechanism pursuant to Article 42 used as a means to demonstrate compliance.

"Recital 78 is helpful in determining what services the principles apply to this – the recital states that when developing, designing and selecting or using applications, services and products that are "based on the processing of personal data or process personal data" to fulfil their tasks the producer of the product, service or application should be encouraged to take into account the right to data protection when developing and designing those products, services and applications by reference to the state of the art". While there is no requirement in private tenders to incorporate data protection by design and by default the public sector tenders must take these principles into consideration.

Processors can decide if designing products or services which use new technologies whether to perform their own impact assessments or provide information to controllers for their own compliance. Particular analysis on the nature, scope, context and purposes of the processing, where it is likely to result in a high risk to the rights and freedom of natural persons is needed. This is not defined in the Regulation but there is a detailed supporting guidance from the Article 29 Working Party to determine what constitutes a high risk in this regard.

Alternative approaches include using external certification tools such as ISO certificate processes or the cloud security alliance consensus assessments initiatives as part of the process for internal compliance.

Record keeping features highly

Processors should keep records of formal and informal impact assessments for specific single tenant services and also for each multi-tenant service where a more general impact assessment can be conducted. There is no set format for the precise form of these assessments, but the Information Commissioner's website contains useful guidance on privacy impact assessments. Impact assessment records could be requested by well-informed controllers in supplier due diligence. There may be possible insurance benefits of maintaining privacy impact assessments in order to demonstrate compliance with regulation as part of general record keeping obligations.

Record keeping obligations also need to be examined in detail in the Regulation. The table below shows a number of the record keeping obligations which are implied in the Regulation beyond the requirements in Article 30 which applies only with a business (an enterprise or organisation – not specifically clear in this regard whether this includes all group companies with fewer than 250 persons).

Service design: Clarity on roles and responsibilities

Perhaps the clearest impact of GDPR will be on service design and service performance.

Service providers should be clear at all stages of the service design and contract process what the processor is doing (and not doing) and what the controller is responsible for. There is no specific guidance on how the processor must assist the controller to comply with the Regulation required (by Article 28.3(f)) but for many IT services drawing a clear line between what the supplier is responsible for and what it is not responsible for is an obvious first step.

Larger cloud providers are already seeking to take this approach. Amazon, for example, has drawn a distinction between what it is responsible for – security "of the cloud" – and what the controller is responsible for, which it calls security "in the cloud". The Amazon website includes useful infographics which state that Amazon Web Services is responsible for location of infrastructure and then compute, storage, database and networking elements of the infrastructure.

"In the cloud" requires controller data to be assessed, processed and controlled by the controller which includes the selection of platform applications, identity and access management configuration of security, including operating system network and firewall, client side and server side data encryption at rest and also encryption in transit. This approach has benefits in that it helps the controller to determine exactly what the boundaries of the service are. Microsoft has also created infographics setting out the limits of its service liability including allocation of responsibility to the client for data classification, end point protection, and matching responsibility for controls at infrastructure and application level according to the nature of services provided.

Creating a responsibility matrix

These measures could be useful if incorporated by smaller scale businesses as a means of managing risk. We would recommend the preparation of a responsibility matrix. This can either be a generic shorter form matrix determining security features offered for core key services and stating who is responsible for what, or more detailed responsibility matrices which would support either ISO or similar certifications, or at its most detailed, a process similar to a responsibility matrix for PCI/DSS which allocates on a highly granular level responsibility for specific items in order to protect cardholder data.

Assumptions with regard to security will need to be reviewed and documented in service designs, pitch documents and responses to tender and then properly incorporated in the contract, so they are not excluded by a "whole agreement" clause or similar. In order to do this the contract structure needs to be reviewed including a review of the sales cycle process, so that sales staff and solution architects are appropriately trained in the principles of data protection by design and by default and of the obligations of controller and processor. This means that appropriate records can be built up for the service design and negotiations with controllers to ensure that controllers have acknowledged and understood their responsibilities and also the limits of service design.

Don't ignore due diligence on the data you process and your controllers

In addition, it will be possible to look at the factors in Article 83. This sets out a helpful list of the factors that will be taken into account by the regulator in determining the amount of a fine. Issues that can be taken into account in due diligence would include:

- proper assessment of the number of data subjects affected, so that the processor is at all times aware of approximate responsibility which it has
- evidence of a proper allocation of responsibility between controller and processor (Article 83.2(d))
- processes and procedures in place to co-operate in the event of a breach and
- understanding of the risk that a particular processor or controller takes because of past infringements which could potentially increase the nature of the fine.

Due diligence of this nature would enable suppliers to properly understand their controller and therefore to take appropriate measures in order to avoid dealing carelessly with controllers who have already had records of previous fines.

Record keeping obligations

Express:

Recital 82 – general obligation to maintain records to demonstrate compliance

Article 30 – records of processing activities

- controller (Article 30.1)
- processor (Article 30.2)

Note also Section 60 of the Data Protection Bill that required controllers or processors as applicable to maintain logging records in automated processing systems, these logs must make it possible to establish (a) the justification for, and date and time of, the consultation and (b) so far as possible, the identity of the person who consulted the data (section 60(2)).

Implied:

- Article 5 to support decisions made with regard to data protection principles
- Articles 6 - 8 gathering of consents for lawful processing and consent
- Article 24 assessment of appropriate technical and organisational means and monitoring of policies
- Article 25 data protection by design and by default – privacy impact assessment (Article 35)
- [Article 26 arrangements between joint controllers]
- Article 28 processor to demonstrate compliance of sufficient guarantees offered to data processors
- Article 28.3 (h) information to demonstrate compliance and contribute to audits
- Article 28.3 [records from sub processors]
- Article 29 records of instructions from controller
- Article 32 records of agreement between controller and processor on technical and organisational measures
- Article 33 records sufficient to provide full reporting on data breaks (taking into account Article 35)

Contract negotiations

Don't kick the can down the road

It is in the interest of both controller and processor not to "kick the can down the road" in contract negotiations and to attempt to undo all the good work of the processor in designing the service appropriately. Traditionally, larger enterprises have used information security schedules and data protection provisions in contracts to force risk down onto the processor. This approach does not work ideally in GDPR given the shared responsibility of controller and processor and the risk of exacerbating fines if controller and processor have not demonstrated proper co-operation to comply with data protection.

Collaboration is key

As such, measures simply passing down the technology or operational risk to an IT services provider should be strongly resisted, so that parties are collaborating in order to ensure protection of the data subject's data. It is in the interest of both controller and processor therefore to produce balanced contractual provisions properly recording the common understanding of the necessity to comply with GDPR and then allocating known or arising risks accordingly. The controller must also be prepared to pay adequately for the service so that the appropriate technical and organisational measures according to the sensitivity of the data are taken.

Paying a fair price for data protection

There is also a duty on the parties not to use blanket protections where these are not appropriate, where the data is less sensitive. In our experience, many controllers attempt to apply the same information security procedures for routine business contact information as they use to protect sensitive personal data. This has the impact of greatly increasing risk for the processor, who has to implement controls that may not be necessary or taking the risk that it does not implement these measures because they are not proportionate, and greatly increasing the cost of providing services.

On the other hand, controllers will also have to recognise that paying a fair price for the appropriate service is most likely the way to resolve the data protection obligations rather than requiring processors to fail to operate at a profit. Data will be significantly more exposed to risk if the service provider becomes insolvent or is not taking necessary steps because it is underfunded to provide the services.

Clarity in contracts

Loose language in the contract should be challenged. Many outsourcings and enterprise scale IT services contracts often include a service description that the supplier must comply with, but also requiring the service provider to take all "ancillary" or "incidental" (or similar wording) processes and steps in order to operate the service effectively. Whilst this is justifiable on the basis that the service provider must provide a full service, language of this nature induces ambiguity, and may lead to the parties inappropriately allocating risk or failing to understand where risk may arise. Often disputes or litigation will occur because a controller argues that the service is required to be extended beyond the bare bones of the service description because of the ancillary service provision. The supplier may often reject this. This can lead to the parties failing to address the important information security issues. Clear service descriptions are necessary, according to a responsibility grid or other preferred method dependent upon the obligations of the controller and where the boundaries of the service performance lie.

This will avoid the data protection clause simply being a flow down of security obligations by the controller to the supplier. At the very least, the controller must keep the processor informed of its own data protection obligations with regard to changes in policies and procedures which could affect retention periods for data. This is also relevant to what is stored where and when it is required to be destroyed or deleted.

Controller specific actions

The controller has to take specific actions - for example encryption of data in transit or at rest, or maintaining appropriate policies and procedures with regard to data. It also needs to obtain the necessary consents from data subjects to outsource the processing to a processor, and the contract should record this.

Records of service performance should also be documented and available as necessary according to the Regulation (but avoiding any accidental disclosure of what would have otherwise been privileged legal materials).

At the very least this means that the controller should arguably be agreeing to comply with a general "compliance with law clause" undertaking to comply with its obligations under GDPR. Often this is resisted as it is implicit that parties to a contract should comply with their general obligations at law. However, if there is a clause obliging the controller to comply with the law, for data protection purposes this will give the processor an opportunity to challenge the controller if it is not complying with its obligations, also providing a possible route to a contractual breach or termination for failure to contractually comply. The alternative is just allowing a defence to a claim from the controller against the processor under the Regulation to the degree that the controller has not complied.

Innovation cost

The controller should also be clear as to whether the responsibility for implementing innovations to comply with 'state of the art' or any changes in the profile of data processed would increase or decrease the obligations with regard to the technical and organisational measures taken.

We have written in detail on this requirement in our previous white paper – see our White Paper "Bringing Clarity to the Cloud".

Allocation of risk

Risk tends to flow down to the bottom of a supply chain.

In IT services, however, particularly where the bottom of the supply chain may be a hyperscale public cloud provider such as Amazon, Microsoft or Google, service providers quite rightly will not accept a full flow down of data protection and information security obligations.

Hyperscale providers are very proficient in identifying risk and stating what they are responsible for with regard to their services and what they are not responsible for.

Frameworks, risk and liability

GDPR has proved a useful framework for these organisations to clarify their obligations with regard to statutory compliance, and to be innovative in the means of presenting information so that the supply chain can adequately manage risk. In some circumstances this has meant that using public cloud may not be the right risk decision as the controller may not be able (on the basis of the standard liability positions offered) to obtain adequate contractual damages for the risk it suffers if there is a data breach.

Some smaller managed IT providers are more willing to take on risk with regard to data on a more extensive basis in order to win and maintain business and to obtain appropriate flow down of contractual terms from the controller. Allocation of risk can be achieved by clear limits of liability. Whatever the liability position reached, the controller must consider its business continuity and insurance arrangements in the light of the eventual contractual liability position. In many cases it is not the limitation of liability cap for general service default which is most negotiated. Often this is limited to a percentage of annual service costs of between 100% and 150% of the annual price paid.

Many contractors are willing to accept unlimited liability for breach of confidentiality, but overlaps with data protection clauses must be scrutinised carefully to establish whether or not this includes unlimited liability for data protection related liabilities. Increasingly, caps are being agreed for data protection liability alone. It will be interesting to see how the tariff for these caps will evolve and whether they will increase significantly.

From pre-GDPR limits in recent negotiations, a distinction between a strict unlimited liability for breach of confidentiality and a capped "super cap" liability for data protection seems to be emerging. The indemnity will potentially cover costs of responding to the regulator and paying for the costs of remediation. It is not yet clear whether strict indemnities for fines will also become part of the package and the extent to which insurance coverage can respond.

Joint and several liability

Joint and several liability of controller and processor has attracted significant attention from the IT services community during the preparation of GDPR.

However, the adjustment of joint and several liability does not appear to be a particularly common feature of contractual provisions at present.

Joint and several liability is covered by Article 82: this provides that processors are liable only where they have not complied with the obligations of the Regulation specifically directed to processors or where the processor has acted outside or contrary to the lawful instructions of the controller (i.e. the contract and the instructions under it).

Processors are exempt from liability if they prove they are not in any way responsible for the event giving rise to the damage, but where the parties are jointly involved in the same processing then joint and several liability is possible. If the controller and processor can establish by appropriate service design records and service operation records that they are not both involved in the same processing, then the allocation of responsibility should be clear.

Indemnities against unsuccessful claims

A claim against controller and processor could be subject to abuse by data subjects, so processers could ask for indemnities against the cost of unsuccessful claims. In the relatively rare cases where the same controller and processor are both actually involved in the "same processing", the Regulation provides a means of allocating liability according to fault for compensation paid to an allocated person, but does not allocate costs for unsuccessful claims, or provide a meaningful remedy when the jointly sued controller cannot pay.

It remains to be seen if an insurance provider could arrange to cover this liability. The first defence is however the design service backed up by appropriate records to demonstrate where the processor is responsible and where it is not responsible for the damage. It is only if these defences fail that joint and several liability will be necessary.

Cyber insurance

The cyber insurance market is maturing very rapidly. Contracts should be clear on who will insure for cyber risk. Ideally, processors should not accept a general guarantee of security for its services.

The processor's responsibility under GDPR is to comply with the Regulation and to take the appropriate technical and organisational measures to protect the data. This does not necessarily amount to a guarantee of security.

Tailoring to fit the contract

Potentially this still means a security incident could occur even when the controller and processor have fully complied with their obligations, because the data breach has occurred notwithstanding that the correct defences have been taken. For example, a sophisticated cyber hack or form of denial of service attack could disrupt systems which have been properly protected according to the current state of the act and the processor's contractual obligations. In these cases, or where fault has occurred, cyber insurance obligations must be appropriately tailored to the contract. If a controller insures for cyber risk and the processor is also insured there must be a process to avoid overlapping insurance. This could result in claims being denied or confusion between insurers at the very worst time – when the breach has occurred.

The market is still evolving the terms of the cover but most cyber policies involve the provision of a crisis response team including PR, forensics, guidance on how to manage and report the breach and appropriate legal and professional support. In addition, some policies are offering cover for fines incurred. Although, in the UK market at least, insurers are not fully sure whether fines are insurable because of the element of wrongdoing which a fine can imply.

Where insurance may or may not respond

Taking this into account, data protection clauses in contracts should recognise the circumstances in which cyber insurance may or may not respond. There are at least four possibilities:

1. No insurance cover is in place, in which case a controller and processor must establish who is to report a security incident and the extent to which the processor must cooperate to mitigate. This is generally well covered in the Regulation.
2. If both parties have insurance, it should be established whose policy is responsible for what loss.
3. Where the supplier has the insurance, the supplier's insurance may require the contract to state who is responsible with regard to the management of the security breach and who controls the reporting.
4. Where the controller has insurance, the controller will have considerably more discretion over the measures it takes in relation to a security incident, how it controls this and what information it submits to the ICO. Therefore, appropriate consultation obligations and providing an ability for the processor to assist to minimise its own GDPR exposure will be necessary.

Post-contract obligations

The Regulation is absolutely clear that data protection compliance is a continuing obligation. It requires that the technical and organisational measures to ensure, and to be able to demonstrate processing is performed in accordance with the Regulation must be "reviewed and updated where necessary".

Regular reviews

Costs for these reviews should be properly allocated in the contract. GDPR does not say who pays although ultimately given that the data belongs to the controller, the controller is ultimately responsible for determining how much it will pay. The controller is able to select service providers who provide services at a scale and who are therefore able to offer improved information security. This is due to the scale and specialist nature of the security measures the service providers can establish, and who are able to respond to changes in 'state of the art' better than a controller can do on its own account alone.

Large, specialist processors are therefore potentially very well equipped to assist controllers to comply with GDPR obligations, offering updates on technical and organisational measures, and scanning the horizon for likely risks and providing appropriately priced protections.

Who pays for what

The Regulation does not, however, deal with what happens if the controller will not pay for adequate security measures, and if there is significant concern in this regard, processors will have to be able to justify their decisions, and clearly allocate responsibility back to the controller.

There is a potential conflict with the processor's obligation where the controller must use only processors providing sufficient guarantees to implement appropriate technical and organisational measures. These need to be in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject.

Ultimately if a processor has a material concern that the controller is not willing to pay for the measures it should implement, the processor must keep very detailed records of this and of the steps it has taken to mitigate this risk as

far as possible, and to warn the controller of its obligations. This would appear to be consistent with the processor's responsibilities elsewhere in the regulation where the processor does not have to take full responsibility for the processing, as the obligation to assist the controller takes into account the nature of the processing and the information available to the processor. This means that if the controller is not providing adequate information, the processor should take steps to ensure it is not liable for the controller's failure.

Contract patches

Given the complexity of the new data landscape, controllers will be issuing patches to processors for their contracts to improve data protection provisions.

In many cases, the controller will be trying to impose its own new requirements and a process should be in place to ensure that the processor "gets there first" with its own patches, and also has a process for managing those controllers who impose or seek to impose their own standards first.

Contract patches for the supply chain

GDPR also places controls over the appointment of sub-processors. In order to appoint a sub-processor, a data processor has to receive prior specific or general written authorisation from the controller.

In multi-tenant services, obtaining the consent on a specific basis from multiple controllers will prove extremely difficult and there is significant risk of conflict in negotiations in this regard, particularly with controllers in regulated sectors who have additional obligations to know who they are dealing with in the supply chain. In this case, some process of notification and ability to make representations if a particular sub-processor is likely to be engaged will have to be agreed on a bespoke basis according to the risk that the controller and processor are willing to take.

The processors will also have to implement contract patches to its supply chain including setting out the technical organisational measures sub-processors need to take, the information and records that the sub-processor needs to obtain to manage compliance and how these records will be available both to the controller and the processor, and obligations for notifying of changes to service provision. In time, these clauses will take on their own form.

Certification schemes

In a number of articles of the Regulation, compliance can be achieved by appropriate codes of conduct and certifications.

In the IT services world, there have been a number of initiatives in order to demonstrate compliance using certification schemes. These will prove a useful alternative to detailed due diligence processes, for example, with regard to data protection by design and by default, Article 25 provides that an approved certification mechanism pursuant to Article 42 may be used to demonstrate compliance instead of record keeping alone.

Certification schemes that have appeared so far for IT managed services include the CSIG Code of Conduct. This code produced a draft guide which is subject to strict review is currently being rethought. Alibaba is one of the participants in this scheme.

CISPE has also developed a code of conduct which has been subscribed to by a number of smaller IT services providers. It is also supported by Amazon which has taken the dual approach of issuing new GDPR compliant processor clauses, and complying with certain obligations using certification mechanisms. These mechanisms do allow the providers to set out detailed guidance on the processes that they observe and to achieve a voluntary "kite mark" or similar guarantee of compliance.

The Cloud Industry Forum has also recently announced a Code of Practice – it describes the code "in many ways [as] a checklist for best practice in the provision of cloud services". It is possible both to self-certify, or for an independent assessor to confirm compliance (a certified + mark). The code offers helpful steps towards GDPR compliance, but wisely leaves organisations to take the full decision on steps to GDPR compliance.

Conclusion: key steps to success

It will be for each IT services business to determine the depth of compliance it needs to consider for GDPR, both in its capacity as controller, and in its capacity as processor.

Ideally, a transparent partnership between controller and processor will be the optimum way for GDPR to be complied with in practice, but the depth of compliance requires a strict reading of GDPR.

As this paper highlights, the requirements can be complex, so training staff in their appropriate functions and on detailed requirements of the regulation will assist in demonstrating compliance. The technological measures necessary may well be the IT Service providers' meat and drink, with greater appreciation of records, and of insurance coverage informing the market quite rapidly.

It is not yet clear how many claims will arise under GDPR, and whether the UK Information Commissioner will seek to make an example of an IT services provider. The industry will no doubt take further measures to ensure that its role is adequately understood. The major providers are already taking significant steps to publicise the benefits of GDPR and of services that they are prepared to offer to assist in compliance.

In summary, an informed GDPR compliance process, including approaches to analyse risk, will include three processes to:

- **Enquire:** what personal data is held and where is it, how is it processed?
- **Protect:** to provide information security control, policies, procedures and training to protect the data whilst it is being processed, manage data life cycle, and to ensure data is held according to the principles of GDPR.
- **Report/audit:** to provide adequate records for the business to demonstrate compliance, reports to auditors and controllers and regulators and to report and manage data breach instance as well as other measures to protect data including appropriate contractual provisions, limitation of liability and insurance requirements.

Charles Russell Speechlys works with clients in the UK and throughout the world. Our lawyers are based in 11 locations across the UK, Asia, Europe and the Middle East, and through each of these locations, clients are able to access the full range of the firm's skills and expertise.

We have an unusually broad range of skills and experience across the full spectrum of businesses and personal needs. This gives us a wider perspective, clear insight and a strongly commercial long-term view. We use this approach to secure the growth of our clients as they move confidently into the future. It has made us a leader in the world of dynamic growth and family business, and among the world's leading creators and owners of private wealth and their families. Major corporates and institutions find our more considered and personal approach a refreshing alternative to conventional business law firms.

Contact

Mark Bailey
Partner
Technology, Media & Telecommunications
+44 (0)20 7427 6519
mark.bailey@crsblaw.com

charlesrussellspeechlys.com

London | Cheltenham | Guildford | Doha | Dubai | Geneva | Hong Kong | Luxembourg | Manama | Paris | Zurich