

Bringing clarity to the cloud: practical guidance for the procurement of cloud services

"I cannot over-state the importance of being on the front foot for GDPR. If you haven't already started preparing, start now.

Make this a matter of priority. Make this a matter for your Board. This isn't a case of 'each company for itself'.

GDPR compliance will be fundamental to the health of the UK's digital economy, and it would be irresponsible and very risky to ignore it and hope that it goes away. It won't."

Simon Hansford,
Chief Executive Officer,
UKCloud

Foreword



Jeff Thomas, Chairman, UKCloud

The explosive growth of the adoption of cloud services over the past 12 months is requiring businesses and providers to take stock of the market and for the advisers to ensure the legal parameters are fit for purpose.

As Brexit is upon us it is so important that the legal framework for Cloud activity is understood, as we want the UK to be seen as the safest country in the world to do business with.

The entrepreneurial spirit being shown by this sector is exciting to watch, but far reaching regulatory change means that learning how to use cloud and get the best from it takes careful consideration. This paper is designed to share the landscape and to bring clarity in very practical terms to the legal framework that currently exists.

Policymakers too should take note that the sector is in real need of practical guidance and this paper is a helpful 'call to action' to ensure providers and purchasers of cloud services are operating within the framework of the law and not trying to navigate in a whole new landscape.

The law is clear but the sector needs to keep talking and we urge continued communication and policy discussions to ensure the potential exponential growth is maximised. Sector growth should be unharnessed within the current framework, but it is in danger of being overwhelmed by the larger players creating their own approach which might dominate the market.

I am confident that the practical guidance within this paper will provide the sector with the keys to future success and a clear message to providers, to think through the consequences of what they are doing and seek advice if further clarity is needed.

Contents

05	Introduction
06	What is data protection and why does it matter?
07	Why was GDPR implemented?
08	Evaluating cloud providers – taking a step back
10	Making sense of long arm legislation
11	Codes of conduct – the way forward?
13	UK Investigatory Powers Bill
14	Danger for cloud providers from customer blanket information security policies
15	Mitigating steps for suppliers
16	Sector specific cloud regulation
18	Case study: Corsham Institute Digital Diabetes Coach
20	Conclusions: Compliant cloud procurement – key legal pressure points
23	Acknowledgements

Introduction



For customers procuring cloud services, it is essential to understand fully the impact of data protection and privacy on the process.

The areas of greatest concern are focused specifically on how a customer selects a supplier who is compliant with all the necessary legal obligations that affect it, how to identify and mitigate service risk, and how to allocate liability for the service between a customer and supplier according to the price of the service and risk the supplier accepts. How that liability is effectively allocated and how it impacts sub-contractors in the supply chain is also an issue.

Data is borderless by its nature, but local laws impact decisions that businesses can make on the locations they can store and process data. This extra territorial legislation impact on data and privacy complicates decision-making around which cloud provider to use. For example, both European data protection laws (following the implementation of the General Data Protection Regulation (GDPR), which comes into force in May 2018) and US laws with their associated extra territorial effect, can impact the choice of cloud provider due to their location and "nationality".

GDPR is generating significant attention because of increased protection for data subjects and the stronger focus on enforcement. The uncertainty over data transfer persists as a result of privacy activism and recent calls to review data transfer mechanisms which allow both Privacy Shield and European Union (EU) model claims and multiple overlapping decisions over the impact of law enforcement authorities' rights to access data. This is further fuelled by the Snowden revelations, the impact of Brexit and the ongoing transition to the Trump Administration in the US.

Notwithstanding the complexity of decision making, both intelligent procurement and careful analysis of the legal implications can eliminate many of these concerns.

It is necessary (and still possible) for customers of cloud services to navigate the legislative complexity in order to develop a data strategy that will seek to ensure consistent and compliant protection for personal data and other business data.

The introduction of GDPR will only increase this scrutiny and associated compliance requirements. Therefore, a clear data strategy with a strong grounding in GDPR compliance is essential, and given the well-publicised fines regime that will enable national data protection authorities to levy fines of up to 4% of group worldwide turnover or €20,000,000 (whichever is the higher) for breach of the basic principles of processing in GDPR and data transfers.

This paper aims to focus on the infrastructure as a service market, not the wider cloud market, including software as a service. We hope to provide a practical guide to those who are buying cloud services, as we are conscious that good practice promotes not only a safe environment in the UK for businesses to flourish, but delivers on the UK Government's promise to make the UK the "hardest target" for cyber crime. The challenge is to consider the consequences of what you are doing and the wider repercussions, and whether the law will provide a framework to help you, or present obstacles to a commercially reasonable solution.

What is data protection and why does it matter?

Data protection is a measure to protect the rights of data subjects (all of us in our personal capacities). It evolved from privacy rights, that are enshrined in a number of international privacy standards. Privacy is a fundamental human right, as follows:

"The GDPR is a huge step forward to build a strong and bottom up approach regarding data protection in Europe. As a European leading cloud computing provider in Europe, we strongly believe that having the same standards in the UK and EU after Brexit regarding data protection will help both citizen and business to have stronger protection, and a more useful technical framework."

Alban Schmutz SVP Public Affairs at OVH.

Article 8 EU: Charter of Fundamental Rights of the European Union Art 8 – Right to respect for private and family life

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Art 12 UN Universal Declaration of Human Rights and International Covenant of Political and Civil Rights

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Understanding this point is fundamental for those businesses that can deal with personal data, including its storage and how it is processed. It cannot be stated often enough that data protection is not a law to enable businesses to exploit data, but a consumer measure to protect European citizens.



Why was GDPR implemented?

GDPR is designed to improve the balance between private citizens, business and public authorities. This is made clear in the early recitals of the regulation. "Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced". (recital 7 GDPR).

The GDPR is intended to be cloud friendly although the regulation does not specifically mention cloud computing.

The EU's paper "Unleashing the Potential of Cloud Computing" in 2012 made clear from the very start of the process of GDPR's development that data protection was a central part of the Commission's strategy to enable cloud computing.

At a European level, the GDPR is part of the EU's Digital Single Market, an overlapping puzzle of at least 16 Directives and Regulations in three key pillars, which look at:

- access to digital goods and services
- environment – a level playing field for digital networks and innovative services
- economy and society maximising the growth potential of the digital economy.

As such, it is only one small part of the overall business agenda for Europe.

There are references in GDPR to the use of "new technology on a large scale" and "rapid technological developments and globalisation". Unfortunately, despite the stated requirements for level playing fields in these policies, data protectionism and data politics are heavily at play in the privacy arena. The EU is justifiably concerned to ensure that the freedom of EU citizens is preserved and that data transfers can be made according to a data transfer solution that is deemed adequate for the purposes of Chapter V of GDPR.

Once implemented, GDPR requires cloud providers who are processing the data of EU citizens to comply with the Regulation whether the data centre or servers are located in the EU or outside. If located outside the EEA, an appropriate data transfer solution must be implemented by the cloud provider in order to ensure compliance.

GDPR will apply to the UK from 25 May 2018 and, when Brexit occurs, the law will remain in force unless amended by virtue of the Great Repeal Bill. This currently looks unlikely. The UK Government stated in its Report on Brexit, published on 2 February 2017, that it will "seek to maintain the stability of data transfers between EU Member States and the UK".

"Data protection emerged from the consultation and the studies launched by the Commission as a key area of concern that could impede the adoption of cloud computing. In particular, faced with 27 partly diverging national legislative frameworks, it is very hard to provide a cost-effective cloud solution at the level of a digital single market. In addition, given the cloud's global scope, there was a call for clarity on how international data transfers would be regulated. These concerns have been addressed, in completion of another Digital Agenda Action, by the proposal of a strong and uniform legal framework providing legal certainty on data protection by the Commission on 25 January 2012. The proposed regulation addresses the issues raised by the cloud. Centrally, it clarifies the important question of applicable law, by ensuring that a single set of rules would apply directly and uniformly across all 27 Member States."

Extract from "Unleashing the Potential of Cloud Computing", prepared by the European Union

Evaluating cloud providers – taking a step back

When considering a contract with a cloud provider, it is important to take a step back, and look at the information security risks and the data protection implications of the service. Careful analysis at this stage can enable both parties to identify and manage the risks of the service, and ensure that the expectations and requirements of customers and suppliers are maintained, with the appropriate steps undertaken to mitigate risks.

Here are some suggested questions to ask yourself and/or the potential supplier:

Datalocation

Q: Are there any regulations or laws that mean I must locate my data in a particular territory or region?

A: This may be a specific law, or sector specific sector requirement, such as health data requirements or local banking law.

Dataprotection

Q: Are there any privacy impacts of the service? Does the customer have the necessary consents from the data subjects whose data the cloud provider may be processing in order to provide the service or host it? If the cloud provider is designing a solution that is liable to have a high risk to the rights of data subjects (Article 35 GDPR) has it conducted a privacy impact assessment (PIA) to embed privacy by design into the system?

A: PIAs are potentially required for all new services and even business acquisitions. There is as yet no guidance on any requirement for infrastructure providers to conduct PIAs for infrastructure services, either from the Commission or any national regulator.

Privacy

Q: Do I need to consider privacy separately from data protection?

A: Privacy is not necessarily the same as data protection, and general care should be taken not to interfere with the fundamental rights of EU citizens in processing personal data. In practice this will include measures to ensure that data is collected in accordance with the basic principles of GDPR (Article 5) and then processed with the necessary consent of the data subjects (Articles 6 and 7). Much of the current debate over bulk transfers of personal data and the confusion on international data transfers relates to this privacy issue.

Datatransfer

Q: What happens about personal data outside the EU?

A: Where the service involves storing personal data outside the EU, an appropriate data transfer solution must be implemented.

The EU model clauses are the most common means for enabling international data transfer. It is this means of transfer that is also under scrutiny as there are claims that it may not provide adequate protection against law enforcement authority surveillance and interception. Privacy Shield is the US Data transfer mechanism, replacing Safe Harbor from April 2016 following the upholding of the privacy case against Facebook Ireland by a privacy activist, Max Schrems, by the Court of Justice of the European Union.

Privacy Shield is a self-certification regime requiring participating businesses to:

- inform other businesses about data processing so the privacy commitments are enforceable under US law;
- inform individuals about their rights to access data, when public authorities may request access to that data and liability in the case of onward transfer;

- provide a free of charge complaints mechanism, with binding arbitration as a last resort;
- provide full purpose limitation on collection and clear data retention policies.

Privacy Shield is beginning to be adopted, but there are still teething troubles implementing the shield for effective transfer as regards the disclosure and transparency measures that data recipients must give to confirm equivalent protections to Privacy Shield for the data transferred. It is also subject to legal challenge by Digital Rights Ireland. Judgment is currently reserved in the case of data protection commissioner v Facebook Ireland Limited & Maximillian Schrems 2016/4809P. The US Government has applied to be an intervening party.

Case study:

Google Inc and Vidal – Hall and others [2015]

This is a relevant well-known example where human rights have been invoked and where there were complex arguments raised concerning whether browser generated information collected by using cookies and then aggregated and used to serve up advertising preferences in isolation or in combination with other data could constitute personal data. The case confirmed internet users may have a right of redress when their browsing habits were used without their consent. The case enabled the complainants to claim for misuse of private information (a tort or civil wrong). It also established that economic or pecuniary damage did not have to be established for an EU citizen to succeed in obtaining judicial redress, and as data protection law protects privacy not economic rights there may be a right of redress for moral damage.

"Both data privacy and security are only as strong as the weakest link in environments where an organisation's data traverses multiple clouds.

As part of a framework that Cisco developed with IDC to monitor cloud adoption (the Cisco Business Cloud Advisor), we have found that almost 63% of British organisations use some form of cloud, with the majority (65%) of them doing so as part of a hybrid cloud strategy. The GDPR highlights some of the key challenges faced by organisations already grappling with the increasing complexity of this hybrid IT world. And in this type of environment, it's especially critical for end-user organisations to adopt an approach that ensures the ability to extend important elements like management, analytics, networking and security across multiple environments – both cloud and non-cloud alike.

Everything Cisco does is tied to cloud and enabling capabilities that our customers and partners need. Crucially, we cover the complete landscape and are continually innovating and expanding our cloud offerings to meet demands and provide the freedom to choose the best environments and consumption models for our customers."

[Terry Greer-King, Director, Cyber Security, Cisco](#)

Source: IDC InfoBrief, sponsored by Cisco, Cloud Going Mainstream. All Are Trying, Some Are Benefiting; Few Are Maximizing Value. United Kingdom. Findings. September 2016.

Making sense of long arm legislation

The EU data protection standards are de facto data protection standards across much of the world, by requiring its laws to be complied with whenever EU citizen data is processed over borders. Other nations also have "long arm" legislation that potentially allows those so-called "third" countries' laws to apply to their citizens' data. This is particularly the case with regard to laws relating to requests for access to data across national boundaries.

This has been an extremely controversial area of law and careful investigation is required on a case by case basis if this is a necessary part of your data sharing strategy. Specific legal advice will be necessary in these cases, which may involve both UK/EU and US opinions.

Three key laws for EU/ US transfers that you need to know about are:

USA Patriot Act 2001

This is anti-terrorist legislation that was brought into law following 9/11. As such its impact is narrower than often stated. However, it has clearly raised the extra territorial nature of data access in the digital age. The law allows access to business records in national security cases, thus having extra territorial effect.

Under Section 45, the FBI can potentially obtain records held by US companies and records those companies have direct access to, and prevents the businesses subject to these FBI requests from disclosing them. Potentially the company communicating information following an FBI obtained order may not be sued even if privileged information is disclosed. It is possible for there to be a direct conflict with the governing law or express terms of the cloud contract, for example English law, which may mean the disclosure is not compliant with the law of the contact, even if the disclosure is required under US law.

US Stored Communications Act

This is an Act implemented in 1986, which addresses storage and disclosure of electronic communications and transactional records held by ISP's. Extra territorial requests under this Act carried significant concerns for the cloud industry as these requests had the potential to extend legislation to very different technologies than those prevailing thirty years ago, when cloud had not been conceived.

Case study:

US Stored Communications Act in action

The Microsoft Ireland case is well known. This case was resolved in July 2016, and an appeal in January 2017 failed to reverse the decision. It was established that the US Stored Communications Act did not enable access to data held on Microsoft cloud servers in Ireland, as the Act in the Second Circuit of New York was not intended to have extra territorial effect. There were significant technicalities in this case around what form of request was given (warrants vs subpoenas), so while the decision was a welcome clarification for cloud providers, it was not a general solution to the problem of what cloud providers can and cannot do in response to US law enforcement authority requests.

Rule 41 Federal Rules of Criminal Procedure (Department of Justice)

This little publicised change to US civil procedure rules came into effect on 1 December 2016. The rule allows the FBI, on the authority of a single warrant, to remotely access servers anywhere in the world where a crime suspect is using anonymising technology to conceal the location of their computer or for an investigation into hacked or infected computers.

Campaigners assert that this gives US law enforcement the right to hack servers or computers even if their actions are concealed through technological means. Some of the media headlines around the cases are alarming as the potential scope of the law has not been clarified; for example a mass scale botnet attack where thousands of devices are hijacked as part of a hack could potentially become searchable under a single warrant.

The implications for cloud providers are not yet totally clear, albeit that many providers will not knowingly host the sorts of materials that investigators may be most interested in, or even be aware of the nature of the materials their customers process. For many providers, a careful review of acceptable use policies (AUP) or similar policies may be in order here to cover obvious concerns.

This will not prevent the law enforcement authorities from exercising lawful rights, but may give the cloud provider clearer contractual guidelines over what they are obliged to hand over and a right to terminate or suspend the service if the data processed is illegal or in breach of the provider's AUP.

Codes of conduct – the way forward?

GDPR allows certification schemes to be adapted as a way of demonstrating compliance with certain of the obligations on data processors (Article 28 GDPR). As such they are potentially a very powerful means of enabling suppliers to demonstrate through technical and organisational means rather than purely contractual promises of security.

The EU has been active with regard to codes of conduct. Currently a Cloud Data Protection Code of Conduct is in an advanced state of preparation by the Cloud Select Industry Group (C-SIG) and a second code prepared by a number of European cloud providers is also under development by Cloud Infrastructure Service Providers (CISPE) and has been considered by C-SIG.

On the matter of accessing law, these codes are reasonably consistent manner. However, the CISPE code adds significant uncertainty with the addition of wording from the Article 29 Working Party opinion on the C-SIG code that prevents law enforcement authorities from making massive and disproportionate requests. This is impossible for the provider to police in practice, but may also become a feature of the C-SIG code after its final review from the Article 29WP.

"As a group of Cloud Infrastructure Services Providers operating in Europe, CISPE launched a Data Protection Code of Conduct available to any CISPs in EU/EEA. The CISPE Code of Conduct sets rules to help to achieve the GDPR goals / regulation, taking into account the operations of any infrastructure provider."

Alban Schmutz SVP Public Affairs at OVH

Umbrella agreements for data interception

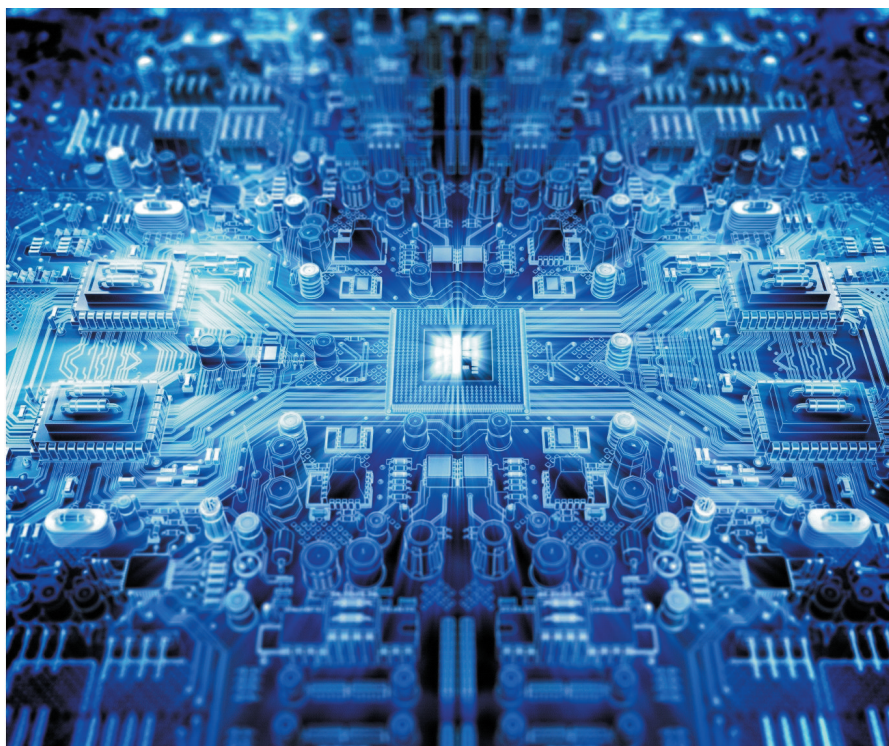
Data interception and cooperation between law enforcement authorities is driven by a comprehensive umbrella agreement, created in September 2015, between the EU and USA and covers:


- All personal data (and expressly references names and addresses, and criminal records) exchanged between the EU and the US for the purpose of "prevention, detection, investigation and prosecution of criminal offences, including terrorism".
- It is lawful and the EU states the "Umbrella Agreement will provide safeguards and guarantees of lawfulness for data transfers, thereby strengthening fundamental rights, facilitating EU-US law enforcement cooperation and restoring trust".

- Enables judicial redress for EU citizens. The express aim of the EU is to embed equality of treatment in the US courts for EU citizens. This has been enabled by the Judicial Redress Act, which also formed a key backdrop to the Privacy Shield negotiations.

Access to data for law enforcement request

Article 23 GDPR has exceptions for national security defence public security; the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; etc "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society."





"The increase in regulation governing data and privacy has significantly changed the deployment of data centres particularly by hyperscale organizations. Enterprise customers will be seeking to ensure compliance with GDPR across Europe and their expectation will be to find the same terms available in the UK. Any shortfall could impact our competitive capabilities."

Philip Low, Broad Group

UK Investigatory Powers Bill

In the UK, the Investigatory Powers Bill has finally received royal assent but there are strong challenges around the measures included in it. The law consolidates and extends the powers of law enforcement authorities. Some cloud providers will potentially be caught within the scope of the law or be required to respond to law enforcement requests, and if they are, they may have to retain metadata about transactions: a potentially huge undertaking with significant cost implications.

Although the Act applies to "telecommunications operators" this term is widely drawn, and encompasses pure network providers and service providers who facilitate the creation, management or storage of communications. This potentially covers social media and, according to the draft code of practice for the Act, internet based services (eg web mail), messaging apps and "cloud based" services. The definition does include application and website providers in so far as they provide telecommunication services.



Danger for cloud providers from customer blanket information security policies

While there is much progress in the making of new laws and codes of conduct covered here, these will still not come into force until 2018 at the earliest. New certification structures could take 2-3 years to become effective so there will be a significant time lag between the coming into force of GDPR and full adoption of certification schemes.

In the meantime, customers as data controllers are responding to the perceived difficulties or inconsistencies in national law by seeking to impose their own standards and policies on cloud providers - standards that potentially exceed the rights by individual national laws in order to strive to achieve global consistency.

This has benefits for the data controller, but while the issues they generally address are reasonably consistent, there is no real consistency of requirements or standards between data controllers. As such each data controller will impose slightly different standards on its cloud providers as data processors, resulting in legal and regulatory risk for processors. This will have particular implications once GDPR becomes law, as controllers and processors are potentially jointly and severally liable for losses incurred by data subjects.

Common themes in customer information security policies

Most policies are very similar and include provisions as follows:

- **Technical and organisational measures to protect data:** These policies apply often both to personal data and non personal data. Provisions on actual measures can be very granular and specific to the controller.
- **Security incident:** These may be defined to include suspected breaches as well as actual breaches of security, and often include hacks irrespective of whether the hack could have been prevented by taking the security measures the policy mandates. There is an obligation usually to identify, prevent, investigate and mitigate security incidents and compulsory reporting is within tightly detailed time limits (usually 48 hours).
- **Audit:** These enable the customer to audit information security measures and to remediate defects or issues discovered, which may not be limited to specific failures to achieve the measures in the policies.
- **Data transfer:** This requires compliance with applicable legal requirements including sector specific legislation and to maintain an adequate data transfer mechanism.
- **Business continuity and disaster recovery:** These plans are generally auditable on the basis set out above.
- **Continuous improvement:** Often the policies require the supplier to continue to develop the service without additional payment to comply with new law and regulation, even if unforeseen. The interpretation of these laws and standards can be subjective, or require compliance with best practices which can potentially exceed any relevant service levels or compliance standards "through the back door".
- **Damage to the value of the business:** Often the policies contain rights for immediate termination for the service if a security incident occurs. These override carefully negotiated termination rights. In effect a single security incident can therefore completely destroy the business.
- **Guarantees of security:** Some of these policies effectively amount to a guarantee of security, with indemnification obligations and immediate termination rights in the event of breach. This may not be desirable even for the customer, as while it produces a transfer of legal risk, there is simply no substitute for identifying the actual security measures and standards to which the cloud provider performs (ie what the provider does and does not do with regard to information security). If a provider accepts a risk it cannot actually protect against, or cannot comply with, this deprives the customer of the ability to mitigate the threat by other means.
- This includes selecting the right supplier in the first place who does offer the right security measures and standards for a price the customer is willing to pay, which is a preferable remedy to claiming damages in the event that there is a security incident.
- This is a classic case of prevention being better than cure, as it will be far preferable to spend available resources on prevention rather than paying fines for breaches that would not have occurred had a reasonable and transparent dialogue taken place at the evaluation stage of selecting the cloud provider.
- **Unlimited liability:** Liability to data protection and information security breaches is often not capped.
- **Inconsistent standards:** Customer policies will all have similar features, but are potentially inconsistent in material aspects which means it is difficult to manage according to fully consistent process and standards, creating risk.

Mitigating steps for suppliers

As well as encouraging consistent negotiation standards for contracts and emphasising that the customer should get what it pays for, there are a number of steps suppliers can take to address these concerns, namely:

- Maintain own policies and procedures. These should be "living" documents not just created for an ISO certification or to satisfy an auditor. Generally, it is reasonably easy to tell in a due diligence process if the policies of a cloud provider are complied with in practice and embedded in the processes and procedures of the business.
- Standards and certifications. Most cloud businesses of scale maintain ISO 27001 certification. This does not in itself guarantee a specific level of security, as it is possible to describe the measures the business does and does not take. In a scenario with a complex supply chain (for instance a third party data centre) the providers in the supply chain should also maintain the appropriate certifications.

Additional standards may also be appropriate:

- Cyber Essentials are a basic requirement for all government contracting. Cyber Essentials Plus covers the same requirement but is more detailed.
- Cloud Security Alliance's (CSA's) STAR Certification is based on ISO 27001 and CSA's cloud controls matrix. This is a standard which is becoming recognised by government.
- Certification schemes. As previously covered, the GDPR will encourage certification schemes to be created. This will enable objective standards of data protection to be certified in a consistent manner and therefore produce consistency for the supplier and a means for it to describe the measures it produces for the customer to evaluate.

- The EU cloud Code of Conduct which sits alongside the GDPR is in draft, but has been subject to detailed criticism by the EU Article 29 Working Party (29WP) for lack of rigour. The June 2016 version of the Code will be resubmitted to the Article 29WP with changes made following their further recommendations, but there will be no further public consultation on the Code. It will then remain to be seen if issues such as the access to data by law enforcement will, in fact, result in the Code being unusable in practice by larger scale providers, other than as a benchmark to state where compliance is achieved and where the provider knowingly diverges from the standards.



Sector specific cloud regulation

There has been a very interesting development in the UK with more sector specific regulation affecting cloud services. The UK government "cloud first" policy has demonstrated a commercial approach to risk, compared with some of the more monolithic government outsourcing contracts. Increasing access to SME's for public sector businesses is consistent with the UK Government's 25% target of IT spend to be fulfilled by SME's.

The UK public sector can assess cloud providers against the minimum standards in the standard G-Cloud contract – framework and associated call off contracts.

Cloud providers on the G-Cloud framework have to comply with certain policies and procedures including government security guidance. These set out the standards that affect hosting and government data.

Government guidance on implementing the cloud security principles accommodates an approach that the commitments of service providers are not contractually binding and constitute "service provider assertion" as one of the three means of addressing the cloud Security Principles (contractual commitment and independent validation being the others). This approach will require review in preparation for GDPR.

In comparison with other sectors, such as financial services which has increased contractual obligations for suppliers following the 2008 crash and increased cyber risk, the G-Cloud framework provides a more flexible framework. This is particularly relevant for the security measures that have to be guaranteed by contract and where liability is potentially capped even for security breaches.

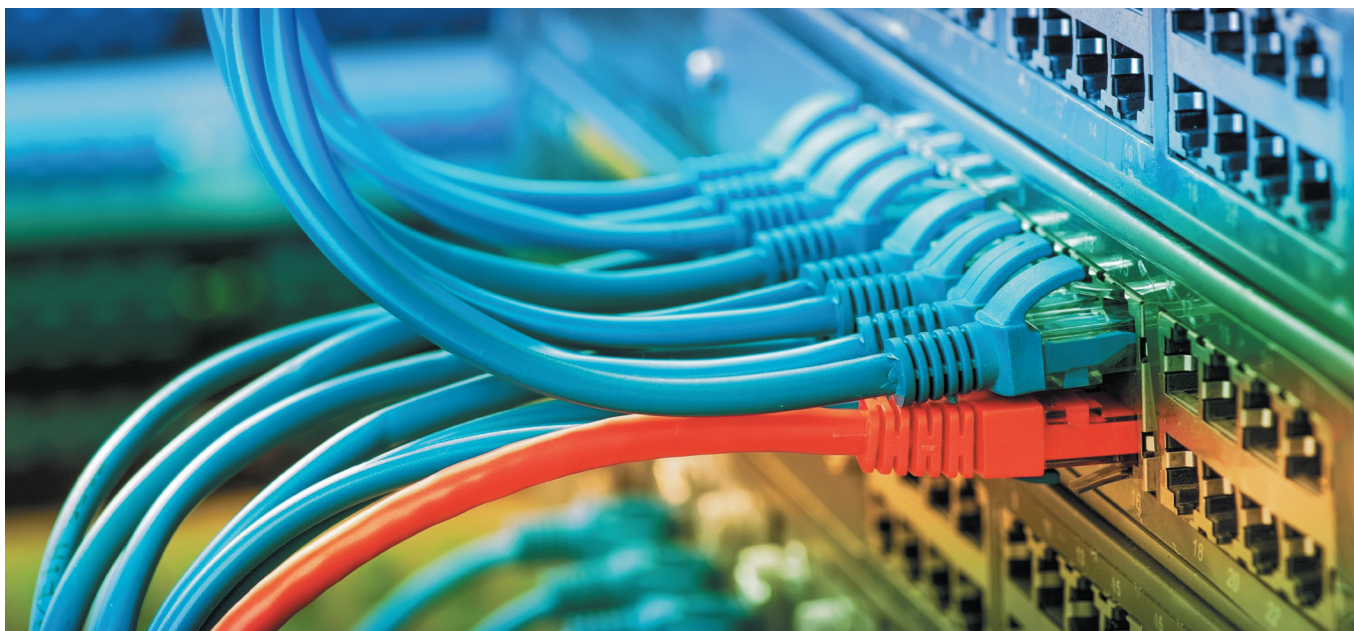
The G-Cloud framework has evolved since its inception but is still significantly less onerous than private sector framework agreements produced by multinationals for cloud or hosted services.

Case study: The public sector context

AWS, one of the hyper scale cloud providers, owned by Amazon, makes a distinction between security at the infrastructure layer it provides (security "of" the cloud), and also the obligations of customers for their data (security "in" the cloud) which is a helpful distinction.

The AWS white paper notes that AWS does not incorporate the measures as contractually binding obligations:

"While AWS delivers these benefits and advantages through our services and features, the individual public sector organisations are ultimately responsible for the management decisions relating to the use of secure cloud services for OFFICIAL Information using the information presented in this whitepaper. We encourage you to use AWS services for your organisations to manage security and the related risks appropriately".



In this table we aim to show the differences between the early and current iterations of the framework:

Comparison of Customer Data / Buyer Data requirements	G-Cloud 2	G-Cloud 9
Not to remove proprietor notices	✓	✓
Purpose limitation – not start of use except where necessary for obligations	Only personal data	✓
Supplier to supply data or request in formal request by customer	On termination with data conversion at customer cost	✓
Supplier to ensure integrity of data	✓	✓
System holding data to comply with customer security requirements	✓	✓
Specific accreditation requirements including guidance and assurance standards	No	✓
Usual review of accreditation status	No	✓
Immediate notification and remedial action in case of breach	Notification by supplier in terms customer of remedial action it proposes to take	✓
Provision of information about Data Protection Act compliance	Audit right	✓
Appropriate technical organisational, operational and technological measures	Personal data only technical and organisational measures	✓

It is interesting to note that the "pure" contractual provisions in a G-Cloud framework and call off are in fact less detailed in later iterations of G-Cloud.

The new frameworks make a stronger distinction between data protection (technical and organisational measures to protect personal data) and customer/buyer data (which is all data processed or managed by the customer). The provisions in recent frameworks are significantly more detailed, so that protections cover all data in a similar manner to personal data.

Case study: Corsham Institute Digital Diabetes Coach

Corsham Institute (Ci) is a not for profit organisation, whose mission is to accelerate an inclusive digital society that is citizen-centric and trusted. We do this by creating a physical and intellectual space to convene, connect, educate and innovate across sectors. One of the work-streams within Ci is Strategic Thought Leadership.

Within Research and Innovation, a key activity focuses on the design, development, testing and deployment of citizen-centric digital products and services. Ci seeks opportunities for large scale social and economic impact with a strong emphasis on both the health and education sectors. Strategic and legislative pressures aside, the very nature of these projects demands increased levels of citizen trust in how an individuals' data is controlled, handled and processed. This additional layer of due diligence is essential in creating products and services that add value to citizens at both the individual and societal levels through enabling education and health systems that optimise their offering for citizen good. It also places greater emphasis on selecting and working with the right cloud partners.

The Ci Innovation & Research flagship project for 2017 is the Digital Diabetes Coach (DDC) which is funded by NHS England and Innovate UK. The DDC programme has brought together global technology business such as UKCloud, innovative SME's and local NHS delivery partners committed to developing a citizen-centric digital product that enables greater self-management of Type 2 diabetes and, simultaneously, through its optimised integration into the NHS care systems, is also designed to provide societal benefit through data analysis, education and faster decision-making.

Based on the mutually supporting principles of Secure-By-Design and Privacy-By-Default, this project has been designed to meet with the objectives outlined earlier and to scale from a localised pilot testbed to a regional and national holistic DDC solution that fits within the UK Health Enterprise.

From the start, trust, ethics and security were placed at the very centre of the project. These drivers made UKCloud a natural platform partner given their architecture and operating model. The key touchpoints in delivering success included the emphasis on data location, data protection, privacy and data portability.

In order to build trust with patients and clinicians and to facilitate the future integration of this pilot into the national digital care system, a Secure-By-Design approach was adopted whose aim was to make systems as free of vulnerabilities and impervious to attack as possible. This is being achieved by continuous testing, authentication safeguards and adherence to rigorous programming and system integration practices.

In tandem, privacy was a key requirement throughout the entire systems engineering and development approach. This up-front investment in data protection and data location will, we believe, help to build the trust required from all users of the system from patients and clinicians to system procurers and regulation bodies.

A trusted platform that complies with current and future regulatory requirements, such as GDPR 18, is essential if that platform is to maintain its place in the market and provide self-sustaining value for money.

For the DDC, we have worked closely with UKCloud to ensure that data collection methods, for specified, explicit and legitimate purpose are further processed in a manner that is incompatible with those purposes, aligns with Article 5 of GDPR, known as the Accountability Principle, and that the necessary processing consents conform with Articles 6 and 7 (identifying and complying with the necessary legal consents including demonstrating that consent was explicitly and unambiguously offered by the individual to the controller). Furthermore, adopting these future-proof methodologies actually lowers the barriers for patients and healthcare providers in engaging with, and delivering, a world class care system for citizens with diabetes.

A further benefit of this approach has been the ability to work with providers, especially UKCloud, in devising and delivering optimal operational standards and working arrangements. Looking forward, Ci is leveraging this success into a series of other citizen-centric opportunities and fully intends to maintain its commitment to deploying fully integrated solutions that deliver self-sustaining benefits at the individual and societal levels grounded in trust, ethics and security.

"Data centre operators and cloud service providers are grappling with the complexities of legislation related to data flows and data protection. At the bottom of the service stack, colocation providers need to identify whether or not they could be classed as data processors under the new legislation. They also need to understand how any changes in their business model may impact this status; so for instance if they choose to provide additional services in response to customer demand, they need to understand the point at which this affects their legal status and, more importantly, how they can identify and anticipate potential liabilities."

Emma Fryer, Associate
Director, techUK

Conclusions: Compliant cloud procurement – key legal pressure points

While every situation and service relationship is different, below are some possible approaches which in summary provide you with issues to consider if you are procuring cloud services:

Using the GDPR to good effect

The GDPR will become law in the UK in May 2018, whether Brexit has been triggered or not, and when it is triggered the UK will have to either adopt a direct equivalent to the GDPR or enable legislation that is adequate for the purposes of equivalence with the GDPR. The UK government, which implements the law, has not announced exactly what it will do, but the Information Commissioner's Office, which enforces the law, is clear that the law will be equivalent to GDPR.

This does enable UK cloud businesses to prepare for the future, at least in part. The GDPR does drive transparency in supply chain, and a clear description of the measures data controllers must ensure flow down to data processors, which is essential particularly with regard to the data processor flow down requirement in Article 28 GDPR.

Certifications and standards

ISO certification is a basic badge of compliance that can be built upon. It remains to be seen whether the code of conduct initiatives will succeed or if individual providers will in fact rely on already existing international standards such as ISO 27001 or ISO 27018. We would expect international standards to prevail, and for there to be a continuing tension with the European law makers and courts over the adequacy of these measures. A more appropriate form of audit or transparency reporting is highly desirable for SME cloud providers and should be encouraged.

Customer engagement

A common consensus between suppliers and customers as to the purpose of the contract is necessary. A well drafted contract should identify clearly what the provider is responsible for delivering and what lies outside the scope of delivery. Contracts should function as an allocation of liability to known risks as far as possible, enabling the provider to understand the risk of using the service against the cost. This is because in cloud, the customer generally gets what it pays for. Understanding the risk is important and also ensuring that not all the risk lands on the provider where the customer is not paying for appropriate levels of service and security.

Contracts

It is essential that cloud contracts are fit for purpose. There is a significant difference of approach between UK and US law contracts in particular, despite the relatively similar Common law legal systems compared with Civil law jurisdictions. Large scale multinational cloud providers with multiple services often impose complex contract structures that can be difficult to navigate, and which are difficult to reconcile with the flow down requirements that data protection laws require. It is possible for these providers to become more flexible in their approach to contract negotiations, or perhaps more likely, to develop sector specific provisions and to meet the general requirements of the law by providing the necessary transparency information to meet data protection laws where the cloud provider is a data processor.

Increased focus on insurance

Cyber insurance for data controllers is a necessary protection for business with significant volumes of personal data. As well as providing payment for liability rising from a breach (the policy should be checked to assist if it caters for data hosted with outsource providers and in the cloud) the policy often includes incident response and crisis management to contact and mitigate the breach.

Customer obligations

Many cloud contracts do not impose significant obligations on the customer. It may be desirable for the contracts in the cloud world to be more explicit about positive obligations with regard to data integrity and data backups that the customer should operate (if these are not part of the service) rather than for these important matters to be covered implicitly by exclusion of the provider's liability for loss of data. This will be particularly important once the joint and several liability regime in Article 82 GDPR comes into force so that the processor can demonstrate without ambiguity that it is not liable at all for the breach: ambiguity will be dangerous in this regard.

Clear allocation of liability

The GDPR includes new provisions potentially making processors and controllers jointly and severally liable for damage to data subjects. Clauses allocating liability will become common in cloud contracts so that the suppliers (and their insurers) bear the proportion of liability according to fault. However prices for services could rise to cover this cost, and the inevitable complexities in litigation, potentially with multiple parties to many claims, and with multiple jurisdictions involved, could significantly increase the complexity and cost of litigation before sufficient legal precedent is established. Regulation 82 paragraph 2 GDPR provides that "a processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller". As such the processor will have to maintain a very clear record of instructions from the controller and the processor can only avoid becoming jointly and severally liable to the data subject (irrespective of any reallocation of that liability in the contract) if it can prove that it is not in any way responsible for the event giving rise to the damage.

Supply chain management

Like its predecessor in the UK, the GDPR requires a data controller to have adequate technical and organisational measures to protect the personal data of data subjects. The precise measures are not stated.

Specific regulations now apply to processors, including cloud providers, as detailed in the table opposite.

The combined effect of these changes is to greatly increase transparency of the measures the data processor takes to protect the personal data and transparency to the supply chain. It is not clear how these measures will in fact be capable of being flowed down the supply chain, in particular to the hyperscale public cloud providers. Unless the approved code of conduct emerges to enable processors to demonstrate supply chain compliance with technical and organisational measures. There is anecdotal evidence in the market of IT service providers, now beginning to split cloud services for software as a service and platform services where the supplier requires the customer to contact directly with the hosting provider for infrastructure services. This marks a return to old fashioned application service provider or hosted services, with all the attendant inconveniences of managing multiple suppliers and potential incompatibilities between layers of the IT stack that cloud was in part intended to eradicate.

Data protection and long arm law has directly driven the location of data centres, whereas public cloud was previously borderless. Most large scale providers now offer guarantees that customer data will remain within specific zones to ensure compliance with data protection laws. Some 70 - 80% of the London colocation market in 2016 in the UK was driven by the requirements of the hyperscale providers for data centre space (CBRE market insight, February 2017).

Summary of key provisions of General Data Protection Regulation affecting cloud providers

Article 25	Data protection by design and by default	Designing services for compliance/certification.
Article 26	Joint controllers	Determine in transparent manner responsibilities for compliance.
Article 28.1	Processor – standard of performance	Sufficient guarantees to implement appropriate technical and organisational means.
Article 28.2	Processor – subcontract	Enlisting sub processors needs “prior specific or general written authorisation”. Controller must receive information of intended changes “thereby giving the opportunity to the controller to object to such changes”.
Article 28.3	Processor – contract flow down	Contract flow-down requirements (a) to (h) set out minimum contract requirements in the contract between (controller and processor) sub processor, adherence to codes of conduct (28.5) can also evidence compliance.
Article 28.4	Processor	NB Notice 28.10 processor has to pass down obligations to sub-processor otherwise it remains fully liable to controller.
Article 30.2	Records of processing activities	Records to be made available to supervisory authority.
Article 35	Data protection impact assessment	Controller obligation but flow down to processor or need for information to feed into the assessment.
Article 79	Right to exercise judicial remedy against controller or processor	Jurisdiction of controller/processor.
Article 82	Right to compensation and liability	Joint and several liability issues. Processor liable where it has not complied with processor obligations in GDPR or has acted outside or contrary to lawful instructions of controller – jointly and severally liable with controller.

"Colocation take-up and demand from the Cloud & IT sector accounted for 70% of the total 155MW transacted across the four major European markets of London, Amsterdam, Frankfurt and Paris in 2016. This equates to around 110MW from this sector alone. We have never seen this kind of dominance from one sector. In context, no single full-year across the four markets had ever even surpassed 80MW of total take-up until 2016. Consequently, influence that these few companies are having on the overall market dynamics and procurement process for colocation space in the major four markets of Europe is significant.

Large cloud service providers have fundamentally changed the procurement process for colocation space. Some operators of data centres are building entire facilities and business models around the requirements of just a few hyperscale companies. Due to the scale of their deployments, these occupiers are able to dictate more favourable commercial terms, which also includes shorter-term contract commitments."

Mitul Patel, Associate Director,
CBRE Ltd, Data Centre
Solutions

Acknowledgements

We are grateful to those who have contributed their time and insights to the creation of this whitepaper. They include:



About Charles Russell Speechlys

Charles Russell Speechlys is a law firm headquartered in London with offices in the UK, Europe and the Middle East.

We have an unusually broad range of skills and experience across the full spectrum of business 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 businesses, 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

If you are interested in more information on our services, please speak to your usual contact or alternatively:

Mark Bailey

Partner

Technology, Media & Telecommunications

T: +44 (0)20 7203 6519

mark.bailey@crsblaw.com

Our offices

London

5 Fleet Place

London

EC4M 7RD UK

T: +44 (0)20 7203 5000

Cheltenham

Compass House

Lypiatt Road

Cheltenham

Gloucestershire

GL50 2QJ UK

T: +44 (0)1242 221122

Guildford

One London Square

Cross Lanes

Guildford

Surrey

GU1 1UN UK

T: +44 (0)1483 252525

Doha

Palm Towers, Block B

15th Floor, Suites 1508-1510

West Bay

Doha

Qatar

T: +974 403 16611

Geneva

9-11 rue du Prince

1204 Geneva

Switzerland

T: +41 (0)22 591 18 88

Luxembourg

2 rue Jean Monnet

L-2180 Luxembourg

T: +352 26 48 68 00

Manama

Bahrain World Trade Center

Floor 24 East Tower

PO Box 31249 Manama

Kingdom of Bahrain

T: +973 17 133200

Paris

26 rue de la Baume

41, Avenue de Friedland

France

T: +33 (0) 1 70 99 09 00

Zurich

Basteiplatz 7

8001 Zurich

Switzerland

T: +41 (0)43 430 0200

charlesrussellspeechlys.com

This is a White Paper which is for general review only and a guide to the topical issues contained in it. The comments in this paper do not constitute legal advice and no liability is accepted by Charles Russell Speechlys LLP, UKCloud Limited or any of the contributors or their partners, directors or employees including liability of negligence.

Charles Russell Speechlys LLP is a limited liability partnership registered in England and Wales, registered number OC311850, and is authorised and regulated by the Solicitors Regulation Authority. Charles Russell Speechlys LLP is also licensed by the Qatar Financial Centre Authority in respect of its branch office in Doha. Any reference to a partner in relation to Charles Russell Speechlys LLP is to a member of Charles Russell Speechlys LLP or an employee with equivalent standing and qualifications. A list of members and of non-members who are described as partners, is available for inspection at the registered office, 5 Fleet Place, London, EC4M 7RD. For information as to how we process personal data please see our privacy policy on our website charlesrussellspeechlys.com.