Microsoft Azure and Data Privacy

How to mitigate the data privacy issues of Microsoft Azure public cloud without a wholesale cloud migration
The original battlegrounds of the cloud industry were cost, uptime, flexibility and scalability. These became cloud technology’s central tenets, from which it grew to become the foundation of most businesses.

Microsoft Azure is the epitome of this. Microsoft has built an enterprise-level service based on an enormous network of innovative, high-performance and secure multi-tenant datacentres, and delivers it to thousands of businesses at a competitive cost.

But the business world is different now. Businesses used to see it as a relief that their data was stored elsewhere in the nebulous “cloud”, where the burden and cost of its maintenance and security were no longer their direct responsibility. Now it’s a threat.

Societal values have changed, as have the legislative frameworks that reflect them. And there is one universally applicable issue that has recently bubbled to the surface: data privacy.

Customers, and the regulators that protect them, expect businesses to whom they have entrusted their data to guarantee its safety and the appropriateness of where and how it is processed. Suddenly, nonchalance and devolving the responsibility of a business’ data environment to a cloud provider is no longer good enough, meaning data residency and overall privacy have never been higher on a CIO’s worry list.

Frustratingly for businesses that take data privacy seriously, some of Microsoft Azure’s key operational practices do not make it easy to abide by data residency requirements, whether regulatory or internal policies.

This presents a problem – the tools, capabilities and scale of public Azure are market-leading, making migrating to an alternative, lesser platform unappealing to say the least. But equally, some continue to be nervous relying on public Azure while faced with data privacy obligations.

How therefore does an Azure-dependent, privacy-conscious business find a suitable balance?
Microsoft allows customers to select a geographical region, or “Geo”, where their data is primarily held. These include the EU, Canada, UK and Australia amongst others. On the face of it, this gives customers robust assurances of data residency.

However, Microsoft also makes it clear that a customer’s data, potentially including personal data, may be held in or backed up to the US by default, regardless of the “Geo” the customer has selected.

Microsoft warns customers of the specific instances where data will be stored or replicated in the US. These include:

- Where the customer is using Microsoft Cognitive Services, in which case data may be transferred and stored globally.
- Where the customer is using Microsoft’s beta and pre-release services.
- Most far-reaching of all, in the back up of web- and worker-role software deployment within any of its Cloud Services.

In practice, this means that any Cloud Services customer, regardless of how deliberately and carefully they may have chosen where their data will reside, will likely see their data stored in the US.
The immediate claim by many alarmists is that because customer data is replicated in the US as a matter of course, Microsoft Azure violates the GDPR.

Of course, this is not true.

Just as many other cloud vendors do, Microsoft Azure provides EU Model Clauses in its contracts. These clauses guarantee that the privacy-respectful practices required by the EU for data to move beyond the EU’s borders are followed by Microsoft, even when the data is held in a country whose privacy laws do not require such safeguards. Microsoft was in fact the first cloud provider to receive a letter of endorsement on their clauses from the EU’s Article 29 Working Party – the EU’s data protection authorities.

It is a strong pledge, and also useful when incorporated into contracts as these clauses make it legal for companies, and Microsoft itself, to transfer or hold EU personal data anywhere within the Microsoft network, including in the US. All without fear of undermining clients’ GDPR adherence.

But this is not the end of the story.

Microsoft’s routine movement of customers’ data to the US may not be in violation of the GDPR, but for some companies, especially those who were unaware of the practice at the time of signing up, it remains highly concerning for a variety of other data privacy and residency reasons.
Problem #1:  
US Government access

If your company’s data is stored in the US, or within non-US datacentre facilities owned by US-headquartered businesses, then the US Government has a number of legislative tools that allow them to issue a warrant demanding access to your data, should it be deemed supportive of national security or criminal proceedings.

These mechanisms include most famously the Patriot’s Act, but also the recently-passed CLOUD Act, the Electronic Communications Privacy Act, National Security Letters (NSLs), and the Foreign Intelligence Surveillance Act (FISA).

Clearly, this applies to data held in any Microsoft Azure datacentre, no matter where it may be.

There are many entirely legitimate businesses who would simply prefer to avoid the possibility of their data being accessed by the US Government. The reasons for the reticence are varied. It may come from the nature of their services and the confidentiality they guarantee to their customers. Often, it stems from the sensitivity of the data they hold, such as customer records, geo-location data, health data or intellectual property. In other cases, it is simply because of firm ethical principles that resent the possibility of government access.

Problem #2:  
Other legal requirements

GDPR is not the only legal or regulatory framework that may dictate how and where a company’s data needs to be stored.

Although very few countries have data localisation laws that explicitly require their citizens’ data to remain solely in that country – Russia being the most frequently cited one – there are other territories whose local laws and regulations create such a requirement in practice.

On the following page, we investigate some national and industry-specific laws that have done exactly this.
Canada

The main national privacy laws in Canada are PIPEDA, which governs how the private sector collects, uses or discloses personal information, and the similar Privacy Act for the public sector. Neither of these have data residency stipulations, only requirements that adequate controls are put in place when data is stored abroad.

However, under Canadian national law (Direction for Electronic Data Residency) and also Nova Scotia and British Colombia provincial law, it is generally illegal for public bodies to store personal information abroad.

Also, many of the regulated industries in the country are explicitly required to show the highest levels of respect to the security and privacy of their clients' personal data. For example, the Canadian accountancy, legal, investment, insurance and health industries are all expected to be able to finitely control the environment in which their data and all its copies are held.

This is of course difficult with public cloud infrastructures that routinely replicate or store data across indefinite locations within or outside the specified region.

Jersey and Guernsey

Many companies seek to take advantage of these countries' beneficial tax regimes. This requires the companies to be not only incorporated within the region but also managed and controlled there too.

But despite the phrasing of the legislation (Income Tax (Jersey) Law 1961), the reality is that this is more than an issue of the residency and activity of the board members. The courts showed in Barclays Bank’s dispute with the HMRC in 2006 that they will also take into account where the company conducts its core activities, and that this includes where data is stored and processed.

In other words, companies wishing to take advantage of the Channel Island tax regime could find themselves undermined if their data is routinely stored and processed abroad.
Luxembourg

Similar to in Canada above, financial services companies in Luxembourg need to be able to evidence the robustness of their customer data environment to their regulator, the Commission de Surveillance du Secteur Financier (CSSF).

This includes not only the security measures in place and the confidence in the physical facility, but also the ability to guarantee full knowledge of the data’s location, and that of all replications.

The difference is that Luxembourg’s beneficial tax regime – and the potential for its abuse – means that the CSSF is prone to audit financial services companies more frequently than other industries’ regulators. And with the growing number of embarrassing data leaks from countries with similar tax regimes, such as the notorious Paradise Papers and Panama Papers, there is increasing concern over the lack of transparency or specificity of typical public cloud data residency practices, including those of Azure.

Switzerland

Switzerland has potentially created a data localization law in all but name. Its Federal Data Protection Act was updated in 2018 to enact the GDPR. It mirrors much of it, including prescribing that Swiss data subjects’ data can only be transferred to countries with “adequate” data protection laws. So far, no difference to the GDPR.

However, the new law has extended the definition of what constitutes a data subject (or “natural person”) in Switzerland to include not just individuals, but also legal entities i.e. companies. Because no other country’s privacy legislation currently defines a data subject in this way, there is speculation that nowhere can technically be deemed to have “adequate” data protection laws – the US included. This is yet to be tested in courts, but it seems to create a situation where data on Swiss citizens and businesses must remain within Swiss borders.
Problem #3: Transparency

Many businesses have internal policies that require exacting clarity over where their most sensitive data is held and the environment in which it is stored.

M&A data, company IP (especially bespoke algorithms), R&D data and customers’ financial or health records are all examples of data deemed by many companies to be too sensitive and valuable to let out of their immediate control.

Rather than the usual blind trust that typifies those that use the cloud, these businesses place such value on their data that their policies require precise examinations of an external datacentre’s physical security; knowledge of exactly where their sensitive data is held and that requisite security processes are being carried out; and exactly the same for any backup sites too.

While this same motivation drives many companies to retain some of their data on-premise, this level of transparency and familiarity is of course entirely possible with cloud infrastructures – although not where data is routinely copied to unknown sites abroad.

Problem #4: Security

For many, Microsoft’s habitual movement and replication of data constitutes a perceived security risk. Firstly, on a purely technical level, the more your data moves, the larger your potential attack surface. While the data is in transit, it is inherently more vulnerable.

Secondly, Microsoft is anecdotally the second most cyber-attacked organisation on the planet, only after the Pentagon. There may be very few reports of major Microsoft datacentre breaches or outages, but for the particularly security-conscious, Microsoft is just too popular a target.

Finally, and perhaps most simply, the more locations that your data is moved to and replicated in, the greater the risk of a breach. This factor is made all the more concerning when it is unclear exactly how many locations this may entail or where they are.
Firstly, do not panic! You are not alone. And nor will you have to sacrifice access to the innovative tools, scale and availability of public Azure.

The good news is there is no need to migrate your entire IT infrastructure.

There is a far simpler approach.

Rather than moving your entire estate to a wholly new platform (a highly complex, costly and time-consuming endeavour), or bringing it all on-premises (therefore ceasing to benefit from the benefits of the cloud), you can instead delineate between what is suitable for your current public cloud and what is better held elsewhere. In essence, create a hybrid environment.

Hundreds of businesses who want to mitigate against the legislative, privacy and security issues mentioned above do exactly this.

They use the Azure public cloud for compute resources, its advanced analytics tools, the development and testing of new projects and applications, and of course the storage of large volumes of less sensitive data. Meanwhile, sensitive data, critical applications and intellectual property are earmarked for a more suitable environment – one whose location is pre-specified, reassuringly permanent and in an appropriate jurisdiction; and whose security facilities are known and approved.

But what exactly is a “more suitable environment”? 
Put your sensitive data in Azure Stack

Hybrid cloud typically brings great advantages of privacy, cost and efficiency, but it can also lead to issues of inconsistency between the two environments. This additional management burden usually creates additional costs, often in the form of recruiting new skillsets.

But if you are using Microsoft Azure public cloud, then there is an alternative.

Microsoft Azure Stack is an extension of Azure and delivers the agile and innovative public Azure services from within defined, identifiable, jurisdiction-specific datacentres, e.g. in Canada, the UK, Channel Islands or mainland Europe.

Because Azure Stack is a natural extension of Azure, the use of the two together creates the only consistent hybrid cloud on the market, while tackling all the security, residency and transparency objections mentioned above.

This consistency is essential for efficiency and reliability in a hybrid environment. The uniformity of tools, self-service portal and APIs across Azure and Azure Stack allow for faster app development and deployment, and more innovative projects to be pursued.

In all, a hybrid environment comprised of Azure and Azure Stack enables the creation and deployment of modern, powerful applications, without compromising data residency.
A four-step guide to safeguarding data privacy within the cloud

While creating a hybrid environment is cheaper, faster and more effective in the long term than migrating to an entirely new platform or on-premise resource, it still requires careful planning and execution.

1. **Identify** the spectrum of risk across your data

   This is arguably the toughest step. Delineating your estate requires complete knowledge and understanding of what data is most suitable for a jurisdiction-specific environment, and what your business deems safe to leave in public Azure.

   This requires an assessment of your data in not just a technical sense, but also in terms of its risk in relation to privacy legislation, internal policies and external threats - alongside your appetite for risk in each area.

   This risk analysis may seem like an alien role for an IT team, but this is the new business environment. Regulators expect to see this data safeguarding mindset across every department’s processes, and will take a more punitive approach to those that lack it.

2. **Design** a suitable infrastructure that respects and reflects privacy requirements

   Only once the data’s risks, characteristics and requirements are understood can a hybrid environment be planned.

   This is far more than a technical architecture step. And requires a wider, more strategic focus than simply the technology involved. Insufficient or imprecise application of data privacy considerations while designing your infrastructure will undermine the value that your hybrid environment can deliver.

   Businesses that have deployed hybrid architecture successfully however have used Privacy Architects to ensure the balance is struck between the cloud platform’s performance, the business’ overall requirements and objectives, and of course regulatory adherence. Over-emphasising one would lead to the others being dangerously underserved – and the project failing.
3. **Migrate** your risk-sensitive data, critical workloads and essential applications

One of the greatest benefits of creating an Azure hybrid environment with Stack is how easy this part of the process is. The absolute consistency across the public and Stack environments means that there is no need to re-architect any applications or even limit what data and workloads can be moved out of public Azure into Stack.

Almost anything designed originally to be deployed on public Azure will run in Azure Stack (provided the Resource Provider has been ported to Stack), without change, in a DevOps model. This is reflected in the fact that the Azure Resource Manager (ARM) QuickStart templates have equivalent version QuickStart ARM templates designed for Stack.

4. **Manage** and oversee your hybrid environment

This is one of the most crucial aspects of a successful migration, though it is often overlooked. A hybrid environment inherently requires greater management than a single-location one, but by no means does it need to be twice the burden.

Once again, the consistency between public Azure and Stack means that this is simplified. Security, load balancing, audits and change management processes are identical across both environments, removing many of the common issues encountered with day-to-day management of multi-cloud environments.
Hybrid Azure and Stack from Calligo

Calligo has an unequalled combination of in-depth experience in Microsoft Azure technology, public and hybrid cloud platforms and data privacy and residency. Together, this makes us uniquely placed to support your Hybrid Azure deployment.

Why should you partner with Calligo?

Cloud Expertise

- Over 100 man years of experience in public and hybrid cloud.
- Over 10 man years of experience in integrating with and managing Azure and Azure Stack.
- One of the first independent cloud service providers in the world to offer Microsoft Azure Stack in partnership with Lenovo.
- One of the largest networks of fully-owned and multi-tenanted Azure Stack deployments on the globe, including:
  - Canada
  - Two in Luxembourg (making us the largest provider in the country)
  - The only Azure Stack deployments in Jersey and Guernsey
- Full cloud consultancy services, from design to deployment.
- High-performance managed services team.

Data Privacy Expertise

- Calligo’s public and hybrid cloud offerings were first in the world to be designed with trust and data privacy at their core.
- First cloud service provider to offer data residency guarantees.
- Dedicated data privacy professional services team, including Privacy Architects.
- Currently supporting companies around the globe with their data privacy obligations, including some of the biggest brands in the world.

For more information visit: www.calligo.cloud
Calligo is a data optimization and privacy specialist.

We believe that data privacy is the starting point to any interaction with data. Our unique collection of innovative cloud-based services covers the entire data journey, from capture and storage to analysis, monetization and archival - with data privacy embedded at every step.

These services include public & hybrid cloud, data analytics, artificial intelligence and archival & erasure services, all supported by ‘privacy-first’ data management consultancy and specific assistance with national, international and industry-specific data protection obligations.

**Cloud Infrastructure**
Our public & hybrid cloud platforms come with market-leading performance guarantees and were first to be designed with data privacy & sovereignty at their core.

[Learn more >](#)

**Data Privacy Services**
Our services instil international, national and industry-specific data privacy requirements into the core of your IT infrastructure and wider processes.

[Learn more >](#)

**Data Insights**
A portfolio of analytics and artificial intelligence services that help you extract the fullest possible value from your data, underpinned by a ‘privacy by design’ ethos.

[Learn more >](#)
To learn more about how Calligo can provide Hybrid Azure and Azure Stack, don’t miss out on the following:

**So you’re deploying Hybrid Azure?**
7 hazards to watch for
Making a hybrid public Azure and Stack environment work for you

Download here >

**Azure Stack - The Best of Both Clouds**
How a hybrid cloud environment using Azure Stack delivered by Calligo can solve the residency, security and access requirements of your most sensitive data.

Download here >