# The Cloud on the Ground

## GDPR and the implications of storing EU citizens data

Where is your data being stored? The question of where data was physically stored used to be straightforward. But in the last 5 years, things have become more complicated.

# Introduction

Where is your data being stored? The question of where data was physically stored used to be straightforward. But in the last 5 years, things have become more complicated.

As we will outline in this paper, for the majority of companies in the UK, where their data was being stored didn't matter too much. If it wasn't on a computer in their office, it was likely in a data centre in the UK, the US or Europe.

None of those options was, or is, a problem, but as the Article 50 deadline looms (30th March 2019) that situation may change. Most companies in the UK take the view that because GDPR is coming into effect before we leave the EU, we will be 100% compliant post-Brexit.

But compliance with GDPR does not automatically entitle a country to store, process and transfer EU citizen data. We'll look at that more closely later, but first to understand where we are now, we need to look at where we've come from. If you're familiar with the history of data storage in the past 30 years you can skip straight to page 5.

# Contents

# A brief history of computer storage

In the 80's, data was primarily stored on large centralised mainframe computers that would connect to relatively simple, dumb terminals. All of the data storage and computer power would live in hardware dedicated to a specific task. By the 90's SMEs had begun buying their own servers – they were primarily held within their own offices but were also offered "as a Service" in the form of dedicated servers and web hosting.

In the noughties companies started to virtualise dedicated servers and whilst it made everything a lot more complicated, the efficiency gains from pushing hardware further towards its limit more than made up for it.

And now, in the twenty ten's it's not only the servers that are being virtualised but routers, switches, firewalls – you name it, the hardware is being run as software. This "software defined as anything" model not only offers huge efficiency savings but also gives companies much more flexibility to redesign their IT infrastructure on the fly.

Throughout all these changes, there have been Data Centres (DCs) in the background – starting with the mainframes in Enterprise DCs in the 80's, to inner-city (metro) DCs in the 90s to regional DCs like 4D in the noughties. Most recently, 'edge data centres' are in vogue, offering low latency and localised content delivery services.


# What are Data Centres and why should you care?

In the 1980's the only companies that bothered to build and own data centres were the large multinationals – usually in finance, medical or petroleum sectors. By the 90's and noughties, this started to change and a new market for 'colocation' data centres emerged.

The advent of the internet gave rise to companies with multiple offices (and later, staff working from home) needing to connect back to centralised servers. Companies would keep their servers in their headquarters in a server room or in the corner of the CEO's office.

However, outages from things such as power cuts or broken internet connections had a major impact on the productivity of everyone connecting back to those servers. With the added risks such as theft, fire and flood, the demand was there for specialised facilities, designed from the bottom up to house and look after servers.

They had backup power in the form of generators and Uninterruptable Power Supply (UPS) systems, special fire detection and fire suppression systems, advanced security and, of course, very fast and resilient fibre connections to the internet.

*The data floor at 4D's Gatwick data centre*

It wasn't just IT companies that were putting their servers into data centres. Hospitals, VoIP providers, social media firms, web hosting companies and, of course, public cloud providers all put their servers into data centres.

# Where your data lives and GDPR (General Data Protection Regulations)

In May 2018, when GDPR comes into force, the maximum level of fines for data breaches are going to go up considerably. For the most serious offences, the Information Commissioner (ICO) can impose a fine of up to €20 million, or 4% annual global turnover – whichever is higher.

For some companies this could amount to a serious fine – Tesco's Bank was the victim of a major data breach back in 2016. The data from over 40,000 customers was compromised and money was stolen from 20,000 of them. At the time, Tesco's bank had a turnover of £955m but Tescos as a whole filed a turnover of £48.3bn. In other words, if Tesco had been subject to the rules of GDPR following the hack on its bank, it would have potentially faced a fine of £1.9 billion.

As well as enhanced penalties, under GDPR there is now joint and several liability between the data controller and the data processor. In the Tesco bank case, the data controller and processor were the same company but for some businesses who use hyperscale cloud providers, the data processor may be Microsoft or Amazon.

Unfortunately, the rules regarding how fines will be distributed in cases where the data processor and controller are different companies won't be properly established until some test cases are brought to court. Until then, for companies that want to have complete control over their data, colocation data centres (which are generally not considered data processors) will be the safest bet.

## Data without borders (yet)

Whilst fines are getting all of the attention in the lead up to the enforcement of GDPR, there is a bigger potential issue looming as Britain heads towards its exit from the EU - Data Sovereignty.

Data Sovereignty is the question of where data is physically being stored. This hasn't really been too much of a problem until now as our two main trading groups are the US and Europe.

As long as Britain is part of the EU and the single market (which it still technically is right now), the UK is allowed to store, transmit and process data on EU residents. The same is true in reverse – EU cloud providers, data centres and multinational businesses can store British citizen data within Europe.

Whilst it's a bit more complicated, the same is largely true regarding data between the US and the EU. This agreement is called the EU-US Privacy Shield. It's a bit more complicated because in October 2015, the European Court of Justice declared a very similar framework agreement (called the 'International Safe Harbor Privacy Principles') invalid. This was very inconvenient for everyone, so the EU did what it does best, and repackaged the old framework, changed it's name to the EU-US Privacy Shield and kept its fingers crossed.

# Freeflow of data and Brexit

When you throw Brexit into the mix, there's good and bad news. The good news is that the UK Government and the Information Commissioner have both pubicly said that they will continue to abide by GDPR standards following the end of Article 50 in March 2019.

This is a noble sentiment but there are two things that could get in the way. The first is politics and who will succeed Theresa May if she quits after Article 50. The bookies top three favourites at the moment are Jacob-Rees Mogg, Boris Johnson and Jeremy Corbyn (the latter of which can only occur if her exit triggers a general election).

The common thread between these three are they are all anti-Europe and whoever is PM in 2020, they may not like the fact that once we've left the EU, the UK will no longer have any say in EU regulations, including GDPR.

When the EU comes round to amending GDPR, the UK will have to adopt all the changes to remain compliant. The UK played a key part in tempering the first draft of GDPR – the French and the Germans have much higher data protection standards and come GDPR V2.0, they will probably want to implement stricter rules.

# A matter of ‘adequacy’

The second issue that could cause data sovereignty issues for UK businesses surrounds ‘adequacy’.

If a non-EU country wants to have unfettered free flow of data with Europe, the European Commission needs to rule whether the data protection and privacy rules of that country meet the minimum standards of the EU.

On the 9th Jan 2017, the European Commission published a notice to stakeholders confirming that post Brexit, the UK will become a “third country” which may impact personal data transfers from the EU to the UK.

It also means the UK’s “adequacy” for EU Data Protection law purposes is not an automatic right and is a matter for decision by the European Commission. Even if an adequacy decision is not granted, there are other mechanisms for British firms to continue to keep data flowing, but these aren’t going to be as a simple process as if adequacy is granted.

There are a lot of reasons to think that this wouldn’t be a problem (the UK will be GDPR compliant at the point of Brexit, the ICO is well funded and run etc) but there have been sticking points.

# The ‘Snoopers Charter’ problem

For example, there is one piece of British legislation called the Investigatory Powers Act (otherwise known as the Snooper’s Charter), which is in direct conflict with GDPR.  For example, under the Snoopers Charter, a data retention notice can be served on an ISP or cloud provider that orders them to retain communications data from its users.

GDPR, on the other hand, states in Article 7 that consent must be freely given. Organisations are not allowed to use personal data for a purpose secondary to that for which this consent was given without notifying the data subject, who may choose to then withdraw this consent.

In other words, a company served with a data retention notice under the Snoopers Charter will be breaking UK law if it refuses and breaking EU law if it complies.

The European Court of Justice (ECJ) ruled that the UK’s new surveillance legislation were too wide and did not comply with EU law, so in response, the UK government now plans to make a number of changes, such as introducing a new independent body to authorise communications data requests.

The use of communications data will also be restricted to investigations into serious crimes that would carry a sentence of at least six months or more. The bar is raised even higher for web surfing data where the investigating crime must carry a sentence of at least one year.

Whether these changes are enough to pass the standards outlined by the ECJ are still to be tested in court, but either way, the ‘adequacy’ standard for the UK to be compliant with EU data protection legislation is not guaranteed.

In a worst-case scenario, if the UK ended up having a hard or no deal Brexit, it could result in major restrictions on the freeflow of data between the UK and Europe.

Businesses will need to get to grips with where their data is physically stored, what laws their data is subject to and who owns the data centres in which their data resides. The situation is serious and could lead to a data exodus, to the detriment of the UK economy in a few short years.

# What to do about it

From a GDPR data breach perspective, companies should consider the following:

- All businesses should go through the ICO's "12 steps to take now" guide and run through their "data protection self-assessment toolkit"
- Get advice from a qualified Data Protection or Information Security consultant to review how and where their data is stored
- When storing data, (especially personal data) on-site, make sure physical security is adequate and that hard disks are encrypted – there is free device encryption on most platforms, such as Bitlocker on Microsoft devices
- Make sure robust firewall and anti-virus are employed, maintained and updated Implement an audit trail of who accesses a server and when
- Conduct an audit of 'Bring Your Own Devices' (BYOD) and where necessary restrict access to sensitive data
- Consider a 'lift and shift' into a colocation data centre – they are usually more secure than offices, provide redundant systems (including power and connectivity) and can maintain the changing compliance standards from a physical perspective

For companies that hold any personal data in the cloud (British or European) they should:

- Conduct an audit of where the data is held and in which countries
- Where possible, request the data is repatriated back to the UK – this will not only safeguard against a 'No Deal' Brexit scenario but also improve latency
- If that's not possible, then draw up plans to be able to quickly migrate the data to a UK cloud or data centre provider should the UK find itself outside GDPR
- Equally, if they are holding EU residents data, they may need to draw up plans for European cloud and DC providers

***4D Data Centres is a UK based colocation, cloud and connectivity provider. With its data centres and cloud platform residing exclusively in the UK, it is an excellent choice for any company concerned about data sovereignty.***