techtalk.travel

Data Sovereignty in Hospitality, a Closer Look

Michael Heinze
Chief Architect at
Shiji Group

www.linkedin.com

JULY 2021

ARTICLE #7
www.techtalk.travel

With the increased popularity of cloud storage and computing systems, information that used to be stored on-premise now sits in data centers around the world, making it more challenging to comply with data processing regulations. This has made the topic of data sovereignty important for the hospitality industry, which works best when it has good amounts of guest data and preferences. An industry like hospitality, which is all about personalisation, can't operate without good data.

Today, data sovereignty is still a new concept that is more important than ever, especially with increasing amounts of personal data being stored in places the guest does not control nor even fully comprehend.

THE RELATIONSHIP BETWEEN DATA SOVEREIGNTY, RESIDENCY, AND PRIVACY

The concepts of "Sovereignty", "Residency", and "Privacy" are closely related when it comes to data, but they require some clarification. Data residency refers to businesses deciding the geographical location where their data will be stored. They may, for example, choose one particular country due to its favourable privacy regulations or low-tax environment. For example, a company – located in country "C" – may have found it favourable for their business to store their data in country "B" where they can save on certain costs. Thus the data residency is country "B".

Data sovereignty refers to the stored data being subject to a specific country's laws meaning it must respect the regulations of that country, such as privacy and other regulations (including that the data must be accessible to the government in case of legal need). So, in the above example, the data would be accessible and governed by the rules of country "B" even if neither the company nor the customers are located there.

While privacy is related to data sovereignty and data residency, it is again different in that privacy is how one protects personal data from being misused. In the example above, this is quite obvious if the data from a citizen of country "A" is stored in country "B" and country "B" has very lenient data protection laws, it could pose an issue for the citizen of country "A". These three concepts are thus closely related but not the same.

Data sovereignty controls how and, more importantly, where users' data is stored. The notion is that data should always be subject to the nation's legislation where it is collected. For example, if certain user information is collected in a European hotel, the EU regulation (GDPR) should prevail. In hospitality, this is particularly intricate, as users' data could easily be created in the US (to book the reservation) and stored in a hotel in Europe, creating gray areas in the interpretation of the regulation.

While the European regulations of GDPR are often cited as regards to data sovereignty, it is important to differentiate between GDPR and pure data sovereignty. Generally, many data sovereignty initiatives (including data localisation laws, e.g. in Russia) have been introduced to ensure that personal information is given appropriate protection irrespective of its location. This idea has been viewed as closely linked with governments/ control (because some countries require the

data to be maintained within its borders), but it could interfere with the free flow of freedoms or simply the free flow of data (a concept rooted in the EU).

GDPR does not provide data residency requirements per se, but instead, it regulates cross-border transfers in general. For example, GDPR does not prohibit cross-border transfer. Still, it is required to have a basis for the transfer and implement appropriate safeguards aimed at ensuring that personal data are protected no matter where they are stored.

Arguably, the most controversial aspect of data sovereignty is how it also dictates the way governments can or cannot access user information. A typical example is the Patriot Act: the US Government has the legal right to access data that is stored on US soil. This is similar to China which has rights for data stored on its soil, and, in all cases, it is a right that governments exert in the name of national security. This becomes an issue when the data of one country's citizens is stored in another country, and national security cannot be enforced. Thus the need for data sovereignty legislation.

DATA SOVEREIGNTY, A POLITICAL PROBLEM?

While there is a lot of political and public relations equity in the topic of data sovereignty, this is primarily an issue of protecting peoples' and companies' data from being misused. Beyond politics and press, the reason why data sovereignty is important is that citizens and companies live and operate in their country and follow the laws, enjoy the freedoms and the protections that come with living or operating in their country.

These freedoms and protections are known to the citizens and businesses who can operate with prediction since they can access their laws. What they do and how they live is adjusted around their local laws. But if the data about how they live is stored in another country where these freedoms and protections are different, it poses a problem.

So beyond the political aspect, this issue is essential for both people and companies and how they conduct their lives and businesses. This is the real reason why it is so important.

It is crucial to state this issue in order to understand the reasons behind data sovereignty. It is about keeping people and businesses' freedoms and protections in the place where they live and conduct business because those are the rights, rules, and legislations they live by.

There are common misconceptions that certain countries have laws that give them access to all the data of businesses of their country, for example, that the Patriot Act gives access to all the data of a US company, or that the Chinese government has access to all the data of any Chinese company. This isn't accurate and is the very reason data sovereignty is important: governments can legally request access to data that is only in their country. A US company that is registered and operates in Europe and hosts the data in Europe does not come under the Patriot Act, in the same way, a Chinese company that is registered and operates in the US and hosts the data in the US is not subject to Chinese government data laws.

DATA SECURITY AND PRIVACY IN HOTEL TECH

In our data-driven industry, security is often synonymous with the protection of guests' personal data. The principal data breaches of the last few years involved guests' information stored in PMS'. Yet, hotels

need to store personal data to operate and thus maintain high-security levels to protect their guests.

Security of personal data is a particularly central topic for privacy requirements. Not complying with all the privacy regulations (such as European GDPR, Californian CCPA, Brazilian LGPD, or South African POPI) can be a threat, one that should be identified as early as possible in the process of selecting technology solutions. Ensuring that the compliance of the system is verified by an external auditor and certified – for example, with an ISO/IEC 27018 certificate, the code of practice for protection of personally identifiable information (PII).

That being said, it's undeniable that modern systems have an advantage when it comes to data protection, as they were created when GDPR and similar regulations were developed. Older software may have a limited architecture that makes it much harder to be compliant with privacy regulations. This is particularly challenging for large, on-premise systems because, in extreme cases, security measures can't even be applied, like some legacy technologies that do not support encryption.

DATA RESIDENCY AND CLOUD SYSTEMS

For a system to be compliant with the main security and privacy requests, let's debunk some myths about data sovereignty. As we've already discussed, the main idea of data sovereignty is that a customer's data should be subject to the country's laws in which the data is collected and processed. The data residency of personally identifiable information is a bigger challenge for cloud-based solutions compared to non-connected on-premise systems. Luckily, by now, most major cloud computing providers have built-in systems to control where the data is being processed and stored, even though this is not necessarily the case in hotel tech.

For example, the Microsoft 365 website clearly states that «we start with the assumption that our enterprise customers would like to have their business data stored and processed close to home. Wherever possible, we do just that.» So, the location for tenants created with a billing address in France or Germany, for example, will never be the US but the EU.

Amazon Web Services offers the possibility to use different regions of AWS so that the application can be deployed in multiple locations, such as the EU, US, China, and so on. Customers have the possibility to decide in which part of the world their data (or their customers' data) should be stored. In practical

terms, a hotel technology vendor can build a storage system for global chains where the data from European hotels is stored in the EU, data from US hotels is stored in the US, data from Chinese hotels is stored in China.

EXAMPLES OF DATA PRIVACY IN HOSPITALITY

In our industry, if a hotel is working with a provider that is following both security and privacy guidelines, it will be able to have its data stored in a particular region, according to where the property is located. However, hotel chains and groups may need their guests' data to travel between different regions. A fitting example is loyalty programs: loyal guests should be recognised at any hotel of the chain or group, and they should be able to check their loyalty points no matter where they are.

Transferring the data to another region is achievable if the guest has explicitly agreed to share their data beyond the region. Then, based on the local regulations, data can be shared either globally or with another region. In some countries, this means that a copy must be kept locally.

In Europe, the very nature of the service of staying in a hotel allows properties to collect and process personal data of their guests: hotels are authorised to process personal data because the data is needed to provide the service; hence consent is not the only legal basis for data processing. Moreover, unlike many Asian jurisdictions, GDPR does not require permission for cross-border data transfers, but that does not mean that personal data can be moved around without any safeguards. The main goal, on the contrary, is to ensure that personal data will be protected wherever they go. GDPR requires transparency and informing individuals what happens to their personal data, including where they are transferred to and why.

On top of that, hotels can openly ask their guests to share their data if they explain in their privacy notice the personal information that will be copied abroad for global systems, such as the loyalty program mentioned before. Of course, in this case, the guests should explicitly agree and authorise joining the program and hence sending their data to other locations. Aggregated, anonymised data (such as occupancy rate, ADR, etc.) do not fall under the regulation, so a European hotel can share this information with the headquarters in the US and vice versa.

CONCLUSION: DATA SOVEREIGNTY IS A MOVING TARGET

Data sovereignty is a relatively new concept introduced by the rise of cloud computing. We may go as far as saying that the whole idea of sovereignty is the "decolonisation of the cloud." That is why both hotels and tech vendors should approach data sovereignty as a moving target. Most countries are working on new, stricter privacy regulations, and data sovereignty is an integral part of these regulations. On this website (Data Protection Laws of the World), you can compare data protection laws worldwide and make sure you're always compliant. Picking your vendors based on their compliance to data sovereignty laws is crucial to avoid your valuable customers' information getting into the wrong hands.

Michael Heinze

Chief Architect at Shiji Group

Michael has over 25 years of hospitality industry experience and has held a number of leadership positions in both new and established companies in Europe and the United States. With a background in software design & coding, databases, networking, IT consulting, product management, software development process design, business process design & re-engineering, strategic and tactical product management, sales and public and private financing. He participated in or managed five company buy-outs or larger-scale investments and many smaller-scale fundings during his career.