Impossible Cloud

GDPR compliance and affordable scalability in the cloud

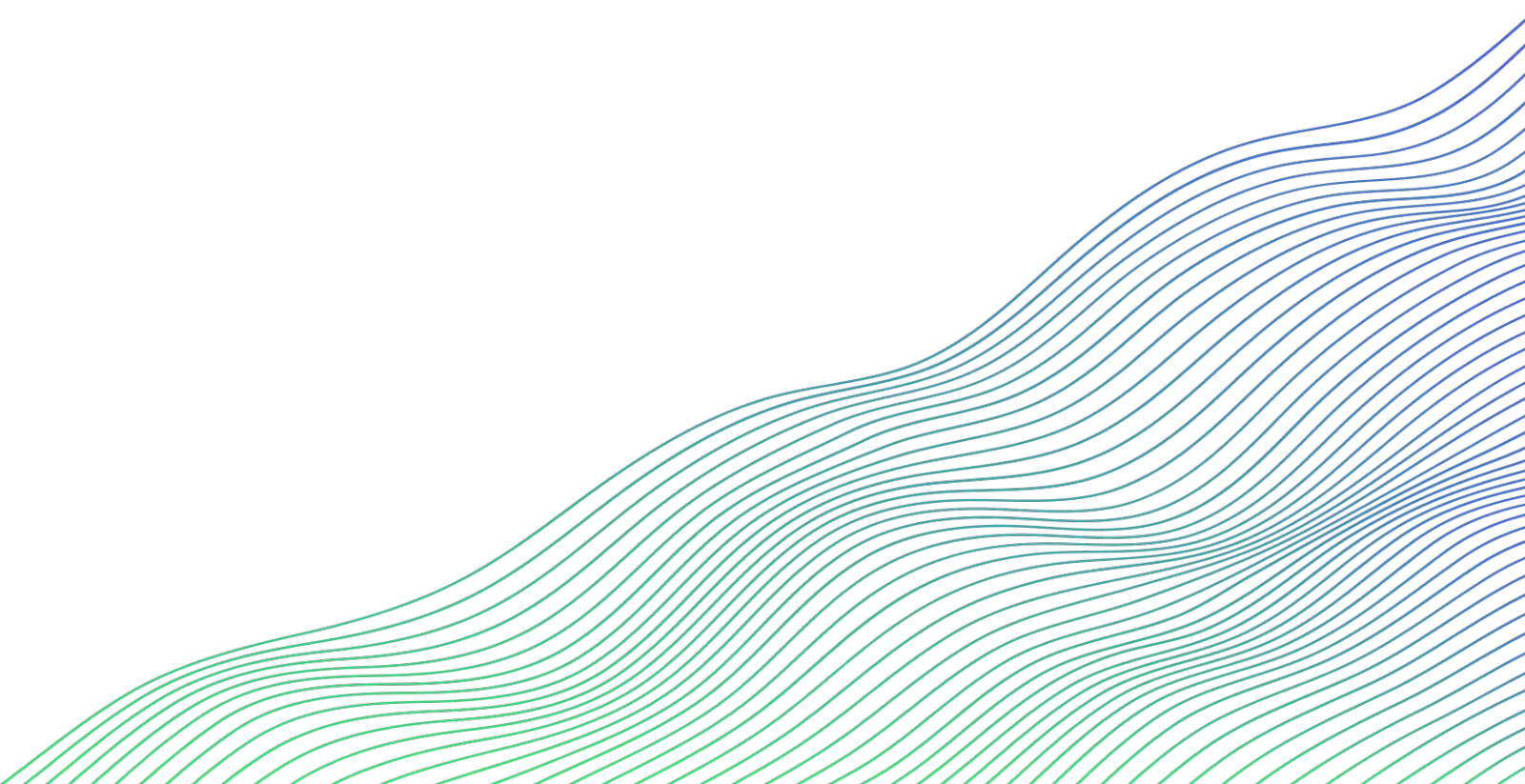
Choosing the right cloud solution for your business

Mar 2024 - Whitepaper

Impossiblecloud.com

Impossible Cloud

Table of Contents



00 Executive Summary

The processing of personal data in the EU is regulated by the European Union's General Data Protection Regulation (GDPR), which has imposed uniform standards in Europe since May 2018.

The GDPR applies to all companies, authorities and associations that collect, process or transmit personal data from European customers, employees or members to third parties - i.e., by the majority of European companies.

If the provisions of the regulation are ignored when storing data in the cloud, there's a risk of very high fines - both for the data owner and for the person who manages the data. That's why every cloud user should make sure that their cloud operator is GDPR-compliant

A server location in Europe or a third country that is considered safe is particularly important. This is the only way to ensure secure data processing.

Cloud operators are predominantly US companies, which is why the US and the EU have been trying to regulate data transfers securely for many years. However, so far all attempts (including the Safe Harbor Agreement, EU-US Privacy Shield Agreement, etc.) have failed.

+

Since July 2023, the **Trans-Atlantic Data Privacy Framework** (TADPF) has represented a new initiative to reach an agreement but according to the CLOUD Act, US-based technology companies must grant the US authorities access to the data.

This means that US companies with subsidiaries and server locations in Europe do **not** offer absolute security and increase the risk of a high penalty for non-compliance.

That's why it's **easier and safer** for European companies, associations and authorities to rely on a European cloud operator, ideally within the European Union.

01 What do you need to know about GDPR?

The European Union General Data Protection Regulation (GDPR) was created to regulate the processing of personal data in the EU and create uniform standards.

"This regulation protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of their personal data.

(DSGVO, Article 1 Paragraph 2)

- The name suggests it pertains to protecting data but it's more correct to say that the GDPR protects the rights and freedoms of **individuals** to whom the data relates.
- Natural, or identifiable, persons are affected by the GDPR. In contrast, companies and legal entities are the addressees of the regulation and required to comply.
- The GDPR came into force in May 2016. After a two-year transition period, the regulation has been **valid since May 2018**.
- Those companies or legal entities who process the data of natural persons must guarantee the legal principles of GDPR outlined in Article 5. These include, above all, the lawfulness of data processing **in good faith, transparency and accountability**.

02 Who does GDPR apply to?

The GDPR is valid **throughout the European Union** for all member states. It thus harmonizes data protection in Europe and creates a uniform and directly applicable legal framework in which the free movement of personal data is guaranteed.

The regulation applies to anyone who collects, processes or transfers personal data from customers, employees or members to third parties. This includes companies of all sizes, corporations, authorities, practices, and associations.

The GDPR therefore applies to every company, every association, and all offices in the EU, including operators of websites or online shops.

Anyone who ignores the provisions of the regulation risks **extremely high fines** of up to 20 million euros or, in the case of one company, up to 4% of annual turnover (whichever is higher). Additionally – and possibly even more serious – the supervisory authorities can insist that **unlawful data processing be stopped** in the event of violations. Depending on the type of business, this can mean the end of a company.

03 Why is GDPR relevant for storing data in the cloud?

The GDPR protects personal data and is intended to prevent unauthorized access. The regulation also ensures that companies and individuals know at all times where the data is, how it is used, and who can use and access it.

To ensure this, a cloud service operator **must work in compliance** with the GDPR.

This also means that every company, every authority, every practice and association must pay close attention to ensuring that the regulation is complied with - not only for themselves, but also for the provider who stores their data.

Important criteria when deciding on a cloud operator include:

- **Server location:** The data protection regulations of the country in which the server is located always apply. This means that data can **only** be stored and processed in a compliant manner within the EU. If the cloud provider is from a third country (such as the US), the level of data protection must be raised to the EU level, which is usually challenging.

- **End-to-end encryption:** In general, the risk of an incident during data processing should be avoided - for this purpose, encryption is explicitly listed as a measure in Article 32 Paragraph 1 of the GDPR, since encrypted content is generally not readable by third parties without a key.

- **Recognition of basic principles:** The cloud operator must recognize and comply with the basic principles of GDPR. As a general guiding principle, only those personal data that are really necessary are processed. The rights of those affected, in particular the right to information under Article 15 of the GDPR, are also granted and those affected can, upon request, find out what data was processed, where it came from and where it was transferred.

- **Certificates**: There isn't yet a specific certificate for a cloud operator's GDPR compliance. Therefore, cloud operators should ensure that their data centers are certified according to ISO 27001 and AICPA SOC 2. This is how cloud providers can prove that legal standards are being met.

04 Are US cloud providers a viable solution?

US providers have a high market dominance and market their storage offerings as part of widely used services and software solutions. There are numerous examples from the business-to-business sector including AWS or Microsoft Azure, but also from the consumer sector such as Apple with iCloud, Google with Google Drive, Microsoft with OneDrive and Dropbox.

As described, the locations of the servers are very important. According to the GDPR, data may **only** be exported to third countries if they offer an "appropriate level of protection".

That's why the US and the EU have been trying to regulate data transfers securely for many years with limited success.

Since 2000, various initiatives have attempted to ensure transatlantic data protection, such as the **Safe Harbor Agreement** (2000-2015) or the **EU-US Priv**acy Shield Agreement (overturned in 2020 by the Schrems II ruling).

All of these initiatives have failed, which is why many US providers offer their services via a European subsidiary with server locations within the EU for GDPR compliance reasons.

Recently (July 2023) there has been a new attempt to transmit data to the US in a legally secure manner. Following in the footsteps of the Privacy Shield and the Safe Harbor Agreement is the **Trans-Atlantic Data Privacy Framework** (TADPF).

This new framework ensures (or should ensure) that data protection and privacy requirements are complied with in data transfers between the EU and the USA.

This means that data exchange in accordance with Article 45 Paragraph 1 of the GDPR is now (for the time being) possible without special approvals. It also means the US is no longer considered an unsafe third country.

However the data is not fully secure.

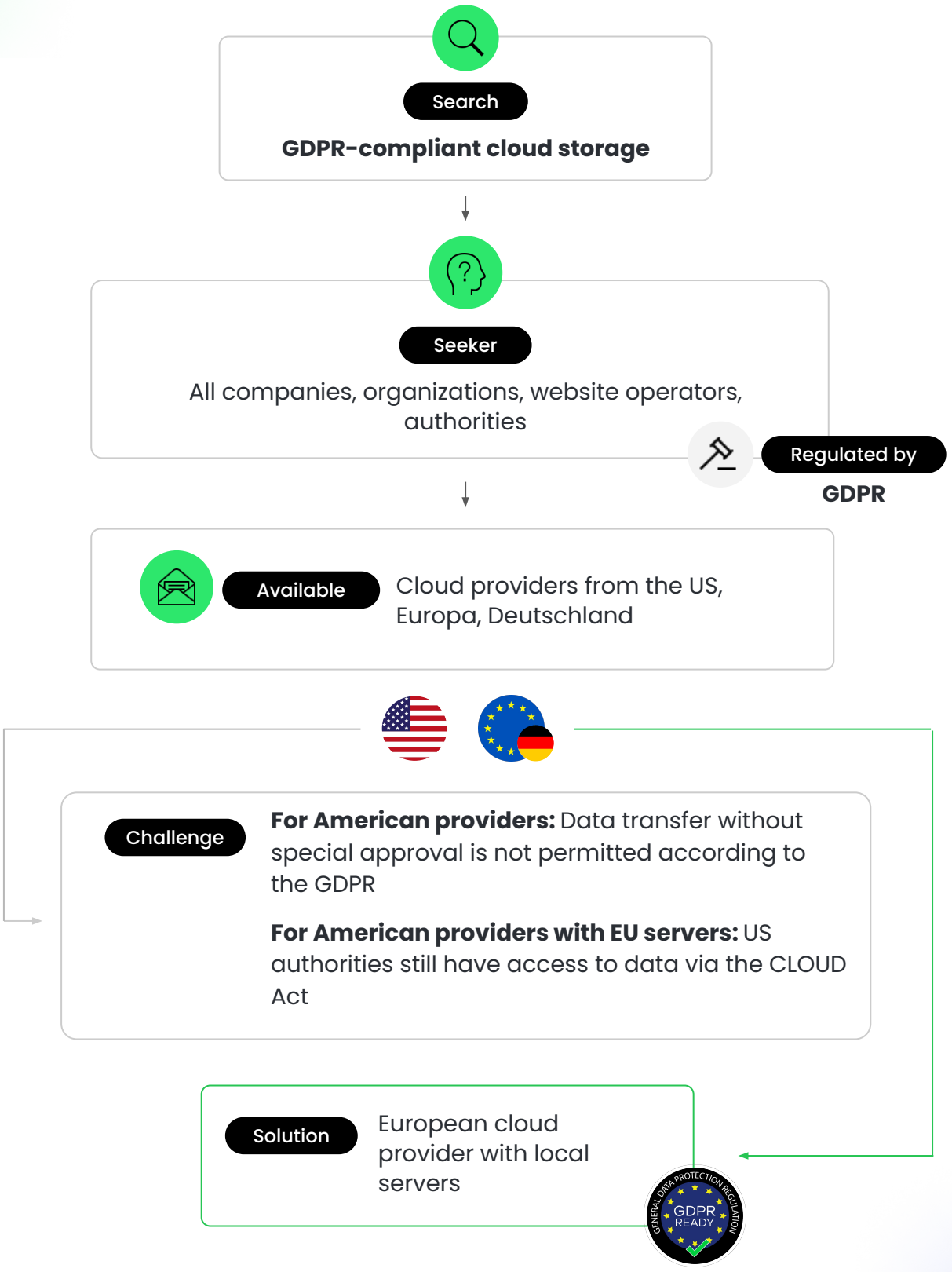
Because US providers are subject to the CLOUD Act (Clarifying Lawful Overseas Use of Data Act), they must - if push comes to shove - **allow the US authorities access to data** saved abroad. This not only formally violates the GDPR, it also violates the spirit of GDPR given that many people are reluctant to allow third parties to arbitrarily view their data.

As shown, a major problem with the previous regulations was the access options of the US intelligence services, which conflict with European data protection. In the TADPF, the options for monitoring and access are severely restricted. This means that US providers such as AWS or Azure could be used in a legally secure manner.

However, this legal security is controversial. There are already voices saying that TADPF is a copy of the Privacy Shield and the Safe Harbor and are predicting its failure. As with its predecessors, access by intelligence services cannot be ruled out.

+

Therefore, the simplest and safest option for every company, organization, or authority is to rely on a European cloud operator within the EU.



05 How much weight does GDPR carry?

European case law repeatedly shows how important it is to comply with the GDPR.

The EU has imposed a record fine of **1.2 billion euros** on Facebook parent company Meta for forwarding user data to the US. The **Irish Data Protection Commission** (DPC) imposed this penalty for breaching the GDPR. Even though the legal dispute will likely ultimately end up before the European Court of Justice, Meta announced at the beginning of August that in the future it will only process certain data from European users for personalized advertising **with their consent**. However, data protection advocates view this commitment with skepticism.

+

ChatGPT was also temporarily banned in Italy because the regulator believed the AI chatbot violated the GDPR. The trigger was an incident in which there was a data leak. Both user data and payment information were affected. There was also a lack of clarity on the part of the data protection authorities as to which user data the ChatGPT operating company Open AI had collected and to what extent and how the protection of minors was guaranteed.

06 Checklist for choosing a cloud storage provider

Even if all political attempts and currently valid resolutions are taken into account, one thing remains certain: companies and organizations **must ensure that the data is processed in accordance with the principles of the GDPR.**

Because the GDPR is based on principles that represent a minimum criteria for everyone, there isn't a valid excuse in the event of violation.

The choice of cloud provider is therefore very important, not least because violating the data protection regulation may result in high fines.

The strict recommendation is therefore: to carefully assess who is entrusted with the data for processing and storage. Some of the crucial points are listed below.

Impossible Cloud

- **Point 1:** When deciding on a cloud provider, a typical desired criteria is: *We do not want to allow US intelligence services to access our data.* This criteria means the first decision has already been made. The logical conclusion in this case is that a European company can only work with a European cloud operator.

- **Point 2:** It's extremely important that the provider is demonstrably able to ensure compliance with all relevant legal requirements. Data center certification is a crucial step to ensure compliance with all legal requirements and regulations that apply to its operations.

- **Point 3:** Encryption plays a central role in GDPR compliance. Care should be taken to ensure that the data is encrypted before it is uploaded to the data center and is only decrypted again when retrieved on site by the customer. The data must also be available at all times, meaning that the provider protects its network from cyber attacks.

- **Point 4:** GDPR compliance doesn't have to be expensive: The costs for cloud storage should be appropriate for your company (or association or authority).

- **Point 5:** In a legally regulated and technically demanding arena such as data processing, communication and support in local language is a significant relief for many companies and organizations. So relying on a European provider is certainly one of the safest and easiest solutions.

07 Impossible Cloud: Reliable, GDPR-compliant cloud storage

If you want to check every item on the checklist, get to know Impossible Cloud.

With Impossible Cloud you can ensure GDPR-compliant data protection. Only our users have access to their data and all data is stored in first-class data centers that are highly secure, fully redundant, and have all common compliance certificates.

+ Impossible Cloud is headquartered in Germany and its cloud storage solutions are "Made in Europe".

Impossible Cloud's modern storage architecture **protects data from ransomware and cyber attacks**.

We use **multi-layer encryption**: By default, every file is encrypted in transit, at rest and on the server side.

Our decentralized network of data centers and a continuous testing process mean that we can limit the vulnerability of the network so that our customers' **data is always available and secure**.

Impossible Cloud storage is also faster and more efficient than leading cloud solutions. The decentralized architecture and parallel multi-threaded structure delivers unparalleled performance and **millisecond throughput speeds** from any location.

Impossible Cloud is designed to provide the **lowest total cost of ownership** in the industry. We minimize ongoing costs by purchasing capacity from top tier data centers and employing a secure, intelligent storage algorithm that minimizes backend redundant storage volume and increases storage efficiency.

As a German service provider, we offer direct, **personal service** in German and English.

Impossible Cloud

08 Conclusion

In summary, the careful selection of a cloud provider that meets the required standards of the GDPR is a crucial step for future-oriented companies, associations and authorities.

Working with a European cloud provider is a sensible precaution to ensure that legal requirements are met and sensitive data is protected.

It's important to note that choosing the right cloud provider is not only a legal necessity, but also a commitment by every company to responsible data processing and the security of sensitive personal information.