GDPR-compliant to the Cloud after Schrems II

The Schrems II judgement - Now finally clear guidelines

In July 2020, the European Court of Justice issued the judgment “C-311/18” (Schrems II judgment), overturning the US Privacy Shield. Until then, this regulated the exchange of data from Europe to third countries, such as the USA.

After this ruling, there was widespread uncertainty regarding the use of American cloud services. Finally, in June 2021, the European Data Protection Board (EDPB) published its final recommendations on the transfer of personal data following the Schrems II ruling.

European Data Protection Board

This has created clear and reliable guidelines to which companies must adhere.
In summary, this means that

- the use of American cloud services is not GDPR-compliant without further measures (even if the servers are located in Europe).
- standard contractual clauses are no longer sufficient to achieve GDPR-compliance.
- the security solutions offered by cloud providers (such as Microsoft E5 license) are not sufficient to achieve GDPR compliance.

In this document, you will learn what will now change for companies and what options are available for using cloud applications in a GDPR-compliant manner.

In its ruling, the European Court of Justice (ECJ) reminds us that the protection afforded to personal data in the European Economic Area must travel with the data - wherever it goes.

Definitions

GDPR

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business. Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements related to the processing of personal data of individuals (formally called data subjects in the GDPR) who are located in the EEA, and applies to any enterprise — regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of individuals inside the EEA.

Source

Cloud Act

With the so-called CLOUD Act, a US law has been in force since the end of March 2018 that also allows US authorities to access data stored abroad by US IT service providers or Internet companies. Contrary to the title of the law, it does not necessarily have anything to do with cloud services. In this case, CLOUD stands for "Clarifying Lawful Overseas Use of Data Act". The law ensures that it no longer matters whether data is stored "in the cloud" or in a specific data center- whether at home or abroad.

Source

Privacy Shield

In the past, data transfers from European companies to the U.S. were initially based on the so-called Safe Harbor agreement between the EU and the U.S. from 2000. However, the European Court of Justice declared the decision of the EU Commission, in which it was determined that the U.S. ensures an adequate level of protection of transferred personal data, invalid.

With the so-called EU-U.S. Privacy Shield, a new basis for data transfers to the U.S. has been available since August 1, 2016.

Source

Schrems II Judgement

On July 16, 2020, the ECJ issued a judgment (Case C-311/18) that has far-reaching consequences for the transfer of personal data to processors in third countries. First and foremost, data transfers to the USA are affected. This is because the Schrems II ruling overturns the European Commission's "Privacy Shield" adequacy decision. This proclaimed that the U.S. provides a level of protection for the data of natural persons that is adequate to the European General Data Protection Regulation (GDPR) under certain circumstances. Only in this way was it possible to transfer data between the USA and the European Union (EU) in a manner that complied with data protection requirements.

Source

Standard contractual clauses are not sufficient in countries whose legislation obliges data importers to disclose data when ordered to do so by authorities (e.g., USA).

Action requirements and their implications for companies

Are standard contractual clauses still valid?

In general, standard contractual clauses remain valid. However, the EDPB explicitly points out that "standard contractual clauses do not operate in a vacuum". What is meant by this is that standard contractual clauses alone do not enable a GDPR-compliant data transfer.

Contractual measures cannot eliminate the application of the legislation of a third country!

In its recommendations, the EDPB states that standard contractual clauses can complement legal regulations of third countries in some cases.
However

- standard contractual clauses are never binding on the authorities of the third country. This is because the country is not a contracting party.
- contractual measures can never eliminate the application of the legislation of a third country.

Especially when transferring data to countries with a lower security level than Europe, companies are therefore obliged to take additional technical measures. The EDPB describes the encryption or pseudonymization of data before it is transferred to the cloud as an adequate measure for achieving GDPR compliance.

For companies that use US cloud services such as Microsoft 365, this means that nothing stands in the way of the continued use of these tools. However, the data controller must prove that it fully meets its responsibility for handling personal data in accordance with the law. Compliance with these requirements must be checked, for example, by the state data protection authorities.

If - as recommended by the EDPB - an external encryption solution is used without the possibility of access by third parties such as the cloud provider, this proof is provided.

Due to the Cloud Act, the penetration of, for example, Microsoft US also on European instances could be ordered.

This cannot be brought in line with the GDPR.

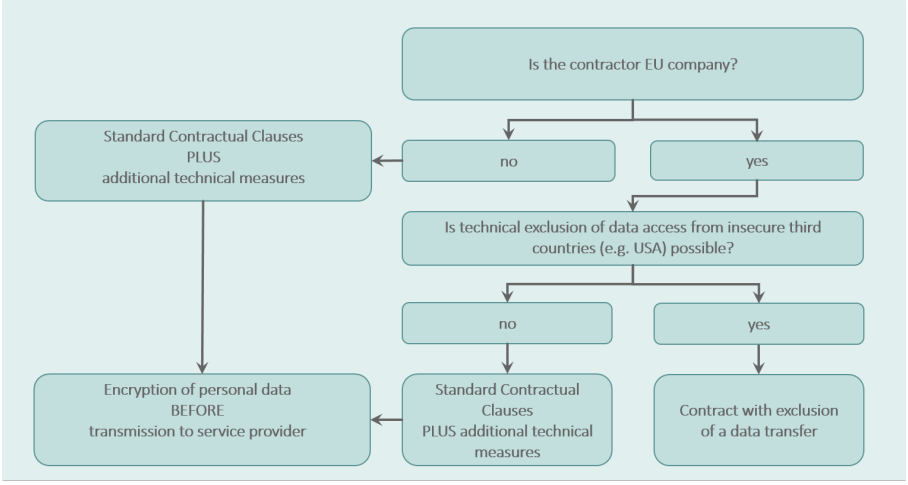
What does “data exchange with insecure third countries” mean?

Countries outside the scope of the GDPR are referred to as third countries. Countries whose level of data protection is below that of Europe are considered insecure- in the sense of the GDPR. This applies, for example, to the USA.

A decisive criterion for classification as an “insecure third country” is the official request for disclosure (e.g. based on the US Cloud Act). Taking Microsoft as an example, this means that Microsoft can be forced to disclose personal data at the request of US authorities.

This obligation to surrender data is not limited to data storage on US servers, but applies regardless of where the data is stored. The decisive factor here is that Microsoft is an American company. An official order can even prohibit the customer from being informed about the surrender of the data. Even if Microsoft exhausts all legal and technical means to protect personal data and prevent its release, the American authorities ultimately have the applicable law on their side.

For European companies, using cloud services from insecure third countries without the right additional measures is a clear violation of the GDPR and can be penalized accordingly.



The only way to counteract this is to encrypt or pseudonymize the data before it is transferred to the cloud. This is the only way to ensure that the cloud provider does not have access to the data in plain text at any time. Accordingly, the cloud provider can only provide encrypted data when enforcing the surrender request.

It is important in this context that control of both keys and encryption must lie solely with the so-called data controller. The cloud provider must not have any access options here.

Recent Developments in Germany

> BvD Herbstkonferenz Datenschutz & Behoerdentag

The following key statements were made during the October 2021 meeting of data protection officers on state level.

Higher Penalties
Penalties imposed for violoations of the GDPR are to be seen as a reminder an are inteded to have a deterrend effect (Art 83(1) EU-GDPR).

Post-Pandemic
Since March 2020, state and federal privacy officials have tolerated limited data breaches out of consideration for the challenges of the pandemic.

In the education sector in particular, the right to education has been placed ahead of the right to data protection. However, after two years of the pandemic, data protection experts are largely in agreement that sufficient time has passed to introduce data protection-compliant solutions. Accordingly, the official tolerations of e.g. Microsoft Teams are gradually expiring in the federal states.

International Data Transfer
In the past, the topic of international data transfer had its focus on the storage of personal data abroad. Now the data transfer is moving into the center of attention. The interpretation during the meeting states that access by a US administrator already constitutes an international data transfer - regardless of the location of the data center (e.g. Germany/EU).

EU Subsidiaries / Dependencies
The establishment of EU subsidiaries or dependencies is not considered sufficient to comply with the provisions of the GDPR, as there is an econonomic dependency on the parent company and the parent company is bound by instructions. Furthermore, access or penetration by American three-letter agencies is not prevented. According to the American understanding, data belongs to the American company, regardless of where it is located.

> Data Protection Officer Bavaria

In December 2021, data protection Bavaria published a briefing note on the topic of office applications from third countries at Bavarian public agencies. There, the recommendations of the EDPB are explicitly reiterated. Standard contractual clauses are only considered sufficient if the controller provides proof that the personal data to be transferred cannot become subject to the access rights of US authorities. If this proof is not possible, an appropriately strong encryption method, special protection of the keys and the use of a state of the art encryption method are required.

What is the legally compliant solution?

Encryption before the cloud
The EDPB describes encryption or pseudonymization of data as a suitable technical measure for using American cloud services in a GDPR-compliant manner.

The prerequisite for this is that the encryption or pseudonymization of the data takes place before it is transferred to the cloud.

This means that most of the cloud providers' native security solutions are not suitable measures per se for achieving GDPR compliance. This is because the cloud provider can only encrypt or pseudonymize the data once it has already left the control of the data controller and been transferred to the cloud.

No access to keys & encryption by cloud provider
Whoever has access to the encryption inevitably also has access to the unencrypted data. For this reason, the EDPB continues to stipulate that cloud providers must not have access to keys and encryption at any time.

Conversely, this means that the Data Controller must have sole control over the keys and the encryption.

This regulation accordingly excludes BYOK (Bring your own Key) and HYOK (Hold your own Key) solutions from the cloud providers as suitable technical measures. It also reinforces the argument for encryption before the cloud. This is the only way to ensure that the cloud provider does not have access to unencrypted data at any time.

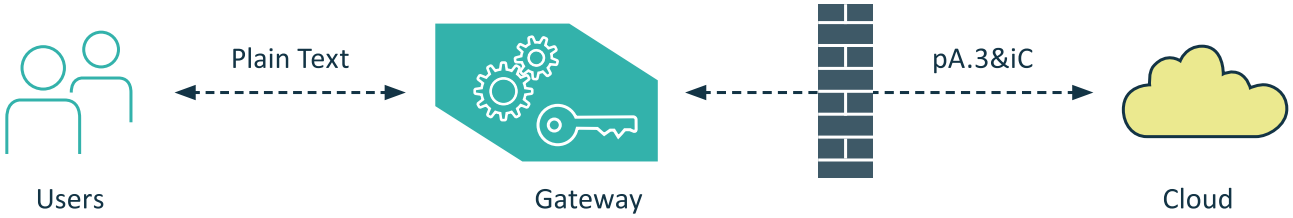
State of the art
According to the EDPB, suitable technical measures must comply with the so-called "state of the art in IT security". ENISA and TeleTrusT have published a handout on this subject.

This lists so-called encryption gateways as the state of the art for encrypting or pseudonymizing data before it is transferred to the cloud in compliance with the GDPR.

The eperi solution
Data protection officers at state and federal level describe the eperi Gateway as a suitable technical measure for storing personal data in the cloud in compliance with the GDPR. The eperi Gateway thus enables the legally compliant use of American cloud services such as Microsoft 365 incl. Teams.

The data controller retains sole control over keys and encryption at all times. Critical data is encrypted or pseudonymized before it is transferred to the cloud.

For users, the eperi Gateway is completely transparent as a proxy. Familiar work processes remain in place.



GDPR compliant cloud usage summarized

GDPR-compliant cloud use is also possible after Schrems II - and not at all as complicated as first impressions might suggest. With the right technical measures, users work as usual while personal data is encrypted and decrypted in the background.

Even companies in highly regulated industries such as banks can migrate to the cloud without hesitation and benefit from the advantages of modern multi-cloud environments.

Thanks to the EDPB's recommendations for action on the Schrems II ruling, which have now finally been formulated very clearly, it is clear what requirements a solution must meet in order to be GDPR-compliant. Simply summarized, a suitable solution must

- encrypt data before it is transferred to the cloud.
- not allow the cloud provider access to keys and encryption at any time.
- correspond to the state of the art.

With the patented multi-cloud approach, the eperi Gateway covers all these points. But a suitable solution must not only meet legal requirements. The workflow of the users must not be interrupted, the accustomed efficiency must be maintained. In addition to GDPR compliance, the eperi Gateway offers

- a completely transparent solution for the user.
- maintaining familiar and efficient workflows.
- the preservation of important application functions such as search, sorting and collaboration.

In summary, this means: Every company can take advantage of the cloud!

Get more information or book a live demo. Our cloud encryption experts look forward to hearing from you!

The eperi Gateway

- Encryption before the cloud instead of in the cloud
- No access by cloud provider
- State of the art encryption gateway
- Appropriate technical measure according to GDPR
- Transparent for users

Sources & Related Links

https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

(ii)Additionally, the Court affirmed the validity of the SCC Decision and held that SCCs donot, perse, present lawful or unlawful grounds for data transfer (no panacea). The CJEU also stipulates that data controllers or operators that seek to transfer data based on SCCs, must ensure that the data subject is afforded a level of protection *essentially equivalent* to that guaranteed by the GDPR and CFR – if necessary with *additional measures* to compensate for lacunae in the protection of third-country legal systems. Failing that, operators must suspend the data transfer. Supervisory authorities must check transfers and are *required* to prohibit transferswheretheyfindthatdatasubjectsarenotaffordedessentiallyequivalentprotection.

84. A data exporter uses a hosting service provider in a third country to store personal data, e.g. for backup purposes.

If

1. the personal data is processed using strong encryption before transmission, and the identity of the importer is verified, (...)

then the EDPB considers that the encryption performed provides an effective supplementary measure.

Final Recommendation 18.06.2021

https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

Legal background

Ruling C-311/18 (Schrems II)
Final Recommendation EDPB
ENISA/TeleTrusT state of the art
Monitoring of the implementation of the ECJ ruling “Schrems II” in companies by state data protection authorities (example of Lower Saxony)

Further information and press articles

Briefing note of Bavarian data protection officer (december 1st, 2021)
Information and links to statements by data protectors at the state, federal, and EU levels (eperi)
Press article: Validity of standard contractual clauses (Security Insider)
Video interview on the consequences of the Schrems II ruling (eperi and SEPPmail)
Blog article: Using Microsoft Teams in a GDPR-compliant way (IT-Techblog)

Further sources

Definition GDPR
Definition Cloud Act
Definition Privacy Shield
Definition Schrems II