Information on the admissibility of data processing outside Germany in connection with the review procedure of the BfArM pursuant to Section 139e German Social Code Book V (SGB V)

Status 11.10.2023

Note: This English translation is provided for informative purposes only. In case of deviations from the German version of this document, the German version shall be considered as the authoritative version.

The following information presents the current legal position of the BfArM in the context of the procedure for assessing the reimbursability of digital health applications (DiGA) pursuant to Section 139e paragraphs 3 and 4 SGB V. This assessment is not binding for data protection authorities. Should data protection authorities take a different legal view in course of their supervisory activities, a technical adjustment may be necessary to ensure proper data processing within a DiGA to avoid the deletion of the application from the directory.

The General Data Protection Regulation (GDPR) generally permits data processing of personal data within the European Union (EU). Processing outside the EU in a so-called third country is permissible, if a comparable level of protection exists in the third country (adequacy decision under Article 45 GDPR).

The Digital Health Applications Ordinance (DiGAV) limits the location of data processing for the data processed by the DiGA pursuant to Section 4 paragraph 2 DiGAV to the Federal Republic of Germany, the Member States of the EU, the contracting states to the Agreement on the European Economic Area (EEA) and Switzerland. The Ordinance also permits data processing for states for which there is an adequacy decision pursuant to Article 45 GDPR in accordance with the regulations applicable to health insurance funds (Section 80 German Social Code Book X, SGB X). Processing of personal data outside of the EU only based on Article 46 GDPR (Standard Contractual Clauses) or Article 47 (Binding Corporate Rules) is not permitted for DiGA (cf. Section 4 paragraph 3 DiGAV).

With the adoption of the adequacy decision for the EU-US data protection framework by the European Commission, personal data can be transferred from the European Union (as well as from Norway, Liechtenstein and Iceland) to the USA as of July 10th 2023. However, the respective US companies must sign up to the EU-US data protection framework by committing to comply with detailed data protection obligations. The website of the U.S. Department of Commerce lists the US companies as "*active*" that have sign up to the EU-US data protection framework.

References

- **List of the U.S. Department of Commerce of US companies that have sign up to the EU-US data protection framework**
  Online at:
  https://www.dataprivacyframework.gov/s/participant-search

Service providers (e.g. operators of data centres) from the USA, with an (independent) branch in the EU but a parent company in the USA, that have not joined the EU-US data protection framework can only be used for the processing of personal data under certain conditions due to the ECJ ruling and the requirements of the DiGAV: A usage is only possible if strict requirements are met that provide sufficient guarantees to prevent a data transfer from the scope of the GDPR to the parent company (see FAQ). In the case of a transfer of personal data to the USA, the requirements set out below must also be met for any tools that may be used in the context of the use of a DiGA.

The manufacturer of a DiGA is responsible at all times for ensuring that all data protection and data security related as well as other legal requirements for his medical device are met. It is also the responsibility of the manufacturer to ensure that these requirements are complied with when using the DiGA in accordance with the current state of legal and technical requirements and that he confirms this truthfully to the BfArM as part of the application procedure. Any subsequent change with reference to this topic is to be regarded as a significant change within the meaning of § 18 paragraph 1 DiGAV and must immediately be reported to the BfArM accordingly.

References

- **List of states for which an adequacy decision is available**
  Online at:
  https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

As a DiGA manufacturer, we have concluded a contract for data processing (data processing agreement, DPA) with a service provider with a branch in the EU but a parent company in the USA (e. g. Google Limited Ireland or AWS Luxembourg) or we would like to use the services of such a provider. Are there conditions under which this data processing is permitted?

Service providers based in the US may be used for the storage and processing of personal data, provided that they join the EU-US data protection framework, which requires them to comply with detailed data protection obligations.

For service providers based in the US, that have not joined the EU-US data protection framework, the following rules appy:

- Provided that the personal data are encrypted according to Article 25 and 32 GDPR and the keys are managed and stored by the DiGA manufacturer in the EU itself or states for which an adequacy decision according to Article 45 GDPR exists, service providers with a branch in the EU but a parent company in the USA may be used. The keys can also be stored by a third party (trust service provider) if its registered office is in the EU or a third country with an adequacy decision. Storage of the keys by the service provider with an US parent company itself is explicitly excluded. In addition, the respective service provider of the DiGA manufacturer must assure that no data transfer to the USA and also no data processing in the USA will be carried out.
- Under the condition that both parties confirm that even in the case of a surrender request by US authorities, no data will be made available and also not surrendered to the parent company, personal data processing is permissible. The service providers must affirm that they will take legal action and exhaust it in the event of a demand for surrender. Even in the event of a supreme court decision confirming an obligation to surrender, Article 48 GDPR must be considered, according to which data may only be transferred even in the case of a final judgment if they are based on an international agreement in force, such as a

mutual legal assistance agreement between the requesting third country and the Union or a Member State.

- In any case of a request for surrender, the service provider shall immediately inform the DiGA manufacturer about the existence of the request as well as the remedial measures and any legal disputes and their procedural status and progress. This must be contractually assured in advance. In addition, the DiGA manufacturer must report a request for surrender by a US authority to the BfArM.

References

- **Information on encryption methods**
  Online at:
  https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Kryptografische-Vorgaben/kryptografische-vorgaben.html

I use SCCs (Standard Contractual Clauses) for the transfer of data to a service provider based in the US, that have not joined the EU-US data protection framework. What should I do now?

A solution via standard contractual clauses is not permitted according to DiGAV.

I use Binding Corporate Rules (BCR) with a company in the US, that has not joined the EU-US data protection framework. What should I do now?

A solution via binding internal data protection regulations is not permitted according to DiGAV.

What about other transfer instruments according to Article 46 GDPR?

Other transfer instruments pursuant to Article 46 GDPR (appropriate safeguards) are excluded according to DiGAV.

Can I rely on one of the exemptions from Article 49 GDPR to transfer data to the US?

No, this is not permitted according to DiGAV. Consent schemes are not accepted. Only the adequacy decision according to Article 45 GDPR applies.

Can I use Standard Contractual Clauses (SCCs) or BCRs to transfer data to a third country other than the US?

No, according to Section 4 paragraph 3 DiGAV this is not permitted.

As a DiGA manufacturer, how do I deal with the fact that an insured person may be physically present in the USA when using the app and that personal data (possibly health data) may pass through US servers of service providers, that have not joined the EU-US data protection framework via their internet connection?

In this case, US law applies to the insured persons. This also applies in particular to the processing of personal data. It is then no longer the responsibility of the DiGA manufacturer that personal data then flows via US servers.

As a DiGA manufacturer, I always offer my app via app stores such as Apple Store. Given that Apple has not yet joined the EU-US data protection framework, is this nevertheless permissible?

Yes, one of the important issues is data separation of login data from health data of the app. Data for registration in the store is data collected for other purposes than the use of the DiGA. In the store, merely the app software can be downloaded and updated. The actual personal data of the DiGA is not held in the store. However, the DiGA manufacturer must always ensure strict data separation. Push messages from the DiGA may only be sent if they do not contain any health data.

I am a US manufacturer based in the USA, do not plan to join the EU-US data protection framework and would like to apply for listing in the directory of my DiGA operated in the USA. What does this mean for the collection and processing of personal data in my DiGA? Am I generally excluded from the Fast-Track Process?

In principle, a US manufacturer, that has not yet joined the EU-US data protection framework, with sole headquarters in the USA is currently excluded. A solution would be conceivable via a constellation with a European subsidiary and a corresponding authorised representative under the conditions as listed in the answers described above.

Change history compared to the version from 24.08.2023

Page	Explanation of change
1-4	Adjustments regarding the regulations on data processing in the USA for companies that have not joined the EU-USA data protection framework.

Change history compared to the version from 13.04.2023

Page	Explanation of change
1-2	Adjustments regarding the rules on data processing in the U.S. following the adoption of the adequacy decision for the EU-U.S. data protection framework by the European Commission on 10.07.2023.

Change history compared to the version from 31.05.2021

Page	Explanation of change
2	Editorial adjustment: With regard to the storage location of the keys, the misunderstanding could arise that these may be managed by the manufacturer but stored by the service provider itself. The new wording is intended to make it unambiguously clear that the keys must be managed and stored by the manufacturer itself when using service providers with a US parent company. With regard to the storage location, any countries with an adequacy decision can be considered.
3	The link “Information on encryption methods” to the BSI website was outdated and has been renewed with a current link.

Change history compared to the version from 28.01.2021

Page	Explanation of change
2	Editorial adjustment: With regard to "any tools that may be used in the context of the use of the DiGA", “the requirements set out below must also be met” was added. This is to make it unambiguously clear that the corresponding prerequisites mentioned in the FAQ also apply to any tools.
2	The link “Information on encryption methods” to the BSI website was outdated and has been renewed with a current link.

2 / 3	Editorial adjustment: The cumulative requirements to be fulfilled (manufacturer-side encryption, assurances and obligation to notify in the event of a request for surrender) were split into two questions in the last version. Therefore, the misunderstanding could arise that these are two options for action. The requirements were therefore combined into one question.