GE Healthcare

GDPR Frequently Asked Questions (FAQs)

1 What does GDPR stand for?

GDPR stands for General Data Protection Regulation and is the new Data Protection Regulation of the EU, designed to harmonize data privacy laws across Europe.

2 What are the major changes through GDPR?

The major changes brought on by GDPR are the following:

- Privacy by design and by default which calls for the inclusion of data protection from the onset of designing systems and processes.
- Data breach notifications will become mandatory and will have to be reported by a Controller to their lead authority (DPA) within 72 hours of having confirmed breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons
- Penalties for non-compliance with GDPR can reach up to 4% of annual global turnover.
- The right to access, which allows data subjects to obtain confirmation from the data controller whether their personal data is being processed, and the right to be forgotten which entitles the data subject to have the data controller erase his/her personal data.
- For some organizations, the need to appoint a Data Protection Officer who can be contacted with questions and who ensures internal record keeping requirements are fulfilled.
- The obligation to have a data processing agreement signed between Data Processors and Data Controllers.

3 To whom will GDPR apply?

GDPR will apply to every organization processing personal data of data subjects in the EU, whether as Data Controllers, Data Processors and the sub-processors. Healthcare organizations are fully in the scope of GDPR.

4 What is a Data Controller and what is a Data Processor?

A data controller compiles and uses data in the course of its operations, for example hospitals with their patient information. A data processor processes data as requested and under the control of the Data Controller, for example GEHC when providing on site or remote service.

5 What is GEHC's approach to GDPR?

GEHC has a dedicated team to work on the GDPR and is committed to deliver a full set of documentation and processes to comply with the GDPR by 25th May 2018. GEHC is also preparing a Data Processing Agreement template to be provided and signed by its Customers.

6 How will GEHC implement Privacy by Design and by Default?

- Privacy and Security requirements are integrated in product engineering development processes.
- Policy, training and tools for Service Engineers, e.g.: automatic De-Identification of DICOM files when downloaded.

7 What is a Data Processing Agreement?

A Data Processing Agreement (DPAgr) is a legal document which must be signed between every Customer and GEHC and which describes the types of processing performed by GEHC for its Customers.

8 Why do both parties need to sign the DP Agreement?

Customers' needs the document to show that as Data Controller they are in control of the data processing performed by external Data Processors.

GEHC as Data Processor needs that document to confirm that we are processing data in accordance with Customer requirements.

9 Does a separate DPAgr need to be signed for each Service provided by GEHC?

Just one DPAgr with GEHC is required to cover all Services provided to a particular customer and one DPAgr can also be signed with a customer's HQ to cover the entire group.

10 What happens if there is a Data Breach?

GEHC will investigate any incident related to data handling - for example the loss of disk drive or the unauthorized access to a database - to determine whether a breach has occurred.

If there is a Data Breach, GEHC must notify the affected Customer(s) as soon as possible. In some cases, Customers are required to report that breach to their authorities within 72 hours after becoming aware of the breach.

11 Why does GEHC need to process personal data to perform the services?

Data generated by medical devices may be processed by GEHC personnel engaged in providing support to Customers in such cases as issue resolution, application training, and product maintenance. It also applies when GE Healthcare performs system integration or data migration activities as part of the medical devices installation in the Customer specific environment. A limited number of IT or support personnel supporting the technology platforms used in providing Services to Customers may have access to components in which the information is maintained.

In addition, where a Customer requests certain additional enhanced or add-on Services, GEHC may also host or access data from Customer system when performing support for those services on the Customer's behalf.

These services very seldom require GEHC to process directly identifiable patient personal data, and data is typically pseudonymized/obfuscated either on the device itself or via GEHC service tools.

12 Where is GEHC processing the data?

As a general principle and for all modalities, all the resources that assist with local, national or European support in the field or remotely are located within the EU. Only in the case of L4 support (which typically requires of the assistance of Engineering teams for the Modality), the expertise centers are located in numerous countries within the European Union, but also outside the EU such as US, Japan, India or China, depending on the location of the Engineering main hubs.

13 How are GEHC global affiliates protecting customers' information?

A Global Privacy & Security Standard is in place and is binding on all GEHC Services staff. Training, processes and tools were provided globally for this purpose to all GEHC Services organization.

14 How are other suppliers and channel partners protecting customers' information?

GEHC obligations are carried-down contractually to GEHC suppliers which might have access to customers' personal information.