General Data Protection Regulation (GDPR) FAQ

Last Modified on 06/08/2018 12:50 pm EDT

Trice Imaging is prepared for the EU General Data Protection Regulation (GDPR), which goes into effect across Europe on May 25th, 2018.

We have updated our policies and procedures to support our customers in meeting the new requirements.

What is GDPR?

GDPR replaces the Data Protection Directive in Europe with the intent to strengthen data protection and the rights of data subjects. GDPR stipulates that any organization collecting personal data must implement the appropriate "technical and organizational measures" to ensure that data is secured, accessible, and handled with transparency (processed using only methods approved by the data subject).

Data Processor versus Data Controller

GDPR identifies two types of organizations: Data Controllers and Data Processors.

- **Data controllers** collect personal data from data subjects
    - Medical clinics and hospitals are data controllers
- **Data processors** process, store, or handle data that is collected from a controller
    - Trice is a data processor

👉 www.tricefy.help/help/processors

Data Processing Agreement

We have updated our Terms and Conditions (Business Agreement), as well as added a Data Protection Agreement that details how we will process and protect your data. These new agreements will be shown next time you log into Tricefy - you may need to log out if you are already logged into the system.

👉 Go to Tricefy to Accept Agreements

You can view agreements by selecting **Business Agreements** within your Account Settings .

Data Protection Policy

Trice Imaging has implemented enhanced policies to show our commitment to preserving the

confidentiality and integrity of all information we hold in our possession.

👉 View our Data Protection Policy

What is included GDPR?

GDPR introduces multiple new requirements for the handling of patient data:

Data Breaches

Notification of data breaches are required to be communicated to data subjects by their controllers within 72 hours. To facilitate this, Trice Imaging is committed to notifying our customers of any security threats or data breaches "without undue delay" so that they can immediately inform their patients.

Data Protection Officer

Trice Imaging has created the position of the Data Protection Officer (DPO) to oversee all data processing activities and is committed to ensuring the most effective technology and policies are in place to keep data secure.

👉 Trice Imaging's Security White Paper

👉 Trice Imaging's Security Policy

Any questions or support calls regarding data security will be immediately transferred to our DPO.

Right to Access and Transfer

GDPR mandates that controllers provide their data subjects access to their data. Tricefy makes it easy for our customers to download data so that it can be given to their patients upon request. This data can be downloaded in DICOM format, allowing it to be transferred to new clinic/controller.

👉 Instructions for downloading data

Accurate Data and "Right to be Forgotten"

Every reasonable step must be taken to ensure data is correct and that incorrect data is erased. Patients also have the right to request their data be deleted (a principle known as the "right to be forgotten").

Trice Imaging does not have the ability to modify or delete our customer's data. However, Tricefy makes it easy for clinics to correct and delete data as needed:

👉 Correcting and deleting patient data

Data Minimization

Trice Imaging will only process data as stated in written instructions by the controller, otherwise known as the contract between us and our customers. We will not process data outside of what is required to meet our contractual agreement, nor will we engage with another processor unless stipulated in our contract .