fastroi
— Caring together —

Fastroi GDPR White Paper

Published 16 April 2020

fastroi

Table of contents

Disclaimer

The purpose of this white paper is to introduce the key concepts of the GDPR and offer materials to support Fastroi's Clients in their efforts determining Fastroi's compliance.

Bear in mind that nothing on this document is intended to provide you with, or should be used as a substitute for legal advice. You should also seek independent legal advice relating to your status and obligations under the GDPR, as only a lawyer can provide you with legal advice specifically tailored to your situation.

Any questions you may have about this GDPR White Paper or Fastroi's GDPR compliance, you can contact our Information Security & Privacy Team at privacy@fastroi.com.

1 Introduction to GDPR

On 25 May 2018, the EU General Data Protection Regulation ("GDPR"), the most significant piece of European data protection legislation came into force. The GDPR became directly applicable in all EU member states and it replaces the old 1995 EU Data Protection Directive seeking to unify data protection laws across Europe.

The aim of the GDPR is to strengthen the rights that individuals have regarding "personal data" (any information relating to an identified or identifiable natural person, so called "data subjects") relating to them. The GDPR applies to any company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed. Please note that "processing" means any operation performed on personal data, such as collection, storage, transfer, dissemination or erasure.

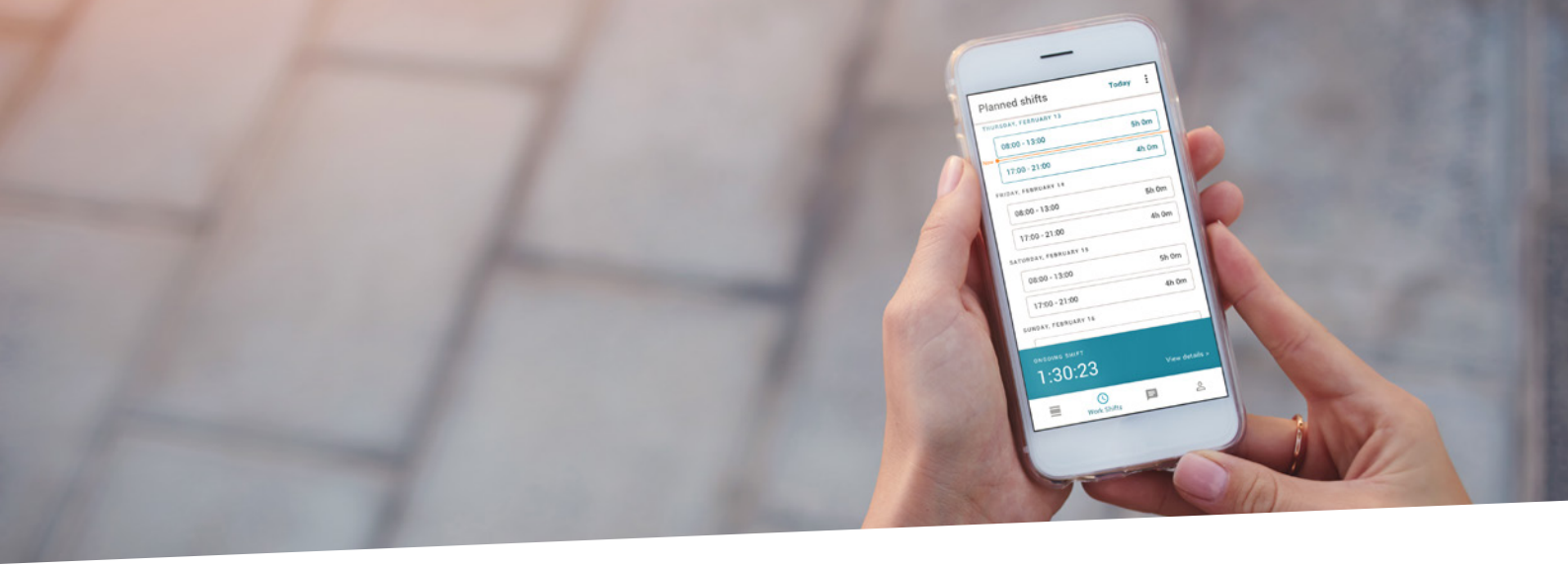
There are two specific roles defined within the GDPR that are important to keep in mind as you look at your compliance efforts.

The GDPR defines two roles, controller and processor, which both have specific obligations under the GDPR:

Controller: refers to a natural or a legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Processor: refers to a natural or a legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Fastroi's Clients will typically act as the Controllers for any personal data they provide to Fastroi in connection with their use of Fastroi's Services. Fastroi is a data Processor and processes personal data on behalf of it's Clients when they are using Fastroi's Services.



2 What are your responsibilities as Fastroi's Client?

Please note that this document aims to be a broad overview of the GDPR and it does not provide you with specific legal advice. We urge you to consult with your own legal counsel and to familiarize yourself with the requirements that govern your specific situation.

In general, Controllers bear the primary responsibility for ensuring that personal data processing activities are compliant with the GDPR. Among other things, you as a Controller, are required to only use Processors that provide sufficient guarantees to you that they have implemented 'appropriate technical and organisational measures' in such a manner that their processing will meet the requirements of the GDPR. This white paper aims to provide you with some aspects you may want to consider when determining whether Fastroi has implemented appropriate technical and organisational measures and thus, is capable of provide you with 'sufficient guarantees'.

In addition, the GDPR allows Data Subjects to exercise various rights related to their personal data. While Fastroi is committed to assist its Clients to respond to those Data Subject requests, the primary obligation to respond and facilitate Data Subject requests and the implementation thereof is your responsibility. You can find more information about managing Data Subject requests related to Fastroi's Services below.

3 What has Fastroi done to prepare for the GDPR

Fastroi welcomes the GDPR as an opportunity to deepen our commitment to data protection. Similar to other legal requirements, compliance with the GDPR requires a partnership between Fastroi and our Clients in their use of our Services. We are dedicated to help our Clients comply with the GDPR. We are continually improving to make enhancements to our products, services and documentation to help support our Clients' compliance with the GDPR. Below your will find some aspects you may want to consider when conducting your assessment of Fastroi's Services.

3.1 ISO 27001 compliant Information Security & Privacy Management System

At Fastroi, we have implemented an ISO 27001 compliant Information Security & Privacy Management System ("ISMS") to demonstrate that protection of our Clients' data is a high priority at Fastroi and to ensure we maintain appropriate level of information security. Further, we are committed to continually improve our compliance efforts.

3.2 Data Protection Officer and an Information Security Officer

Fastroi has decided to nominate a Data Protection Officer ("DPO") to ensure better level of compliance, and an Information Security Officer (ISO) to ensure the highest possible level of information security. You can reach both of Fastroi's DPO and ISO at privacy@fastroi.fi

3.3 Confidentiality commitments

All Fastroi Employees are required to sign a Confidentiality Agreement and regularly complete mandatory confidentiality and privacy training, as well as job related information security training. Our Information Security Policy specifically addresses responsibilities and expected behavior with respect to the protection of information.

3.4 Data Processing Agreements

We have specifically updated our Contractual Terms to reflect the requirements of the GDPR and to facilitate our Clients' compliance assessment and GDPR readiness when using Fastroi as a Service Provider.

Any data that a Client and its Users put into our systems will only be processed in accordance with the Client's instructions, as described in our Data Processing Agreements.

3.5 Our use of third parties

As any other business, we engage some third parties to assist us providing our Services. Each third party goes through a rigorous selection process to ensure it has the required expertise and can deliver the appropriate level of security and privacy. We make information available about our current sub-processors in our updated Data Processing Agreements.

3.6 We help our Clients to facilitate Data Subject rights

As a Data Processor and taking into account the nature of our Services, Fastroi is committed to assist its Clients in fulfilling their obligations to respond to requests for exercising Data Subject rights guaranteed in the GDPR. We have implemented certain technical measures, such as functionalities as well as organisational measures and processes into the services we offer, to help our Clients to access, rectify, restrict the processing of and delete personal data put into our systems.

3.7 Client Data locations and transfers to other countries

By default all Client data is stored within the EU area and Clients may specify the country where Client data will be stored, such as Dublin, Frankfurt, London and Paris.

In certain cases, when necessary to provide the services, Client data may be accessed from a country outside EU or European Economic Area by Fastroi or it's subcontractors. The European Commission has approved the use of model contract clauses as a means of ensuring adequate protection of data when transferring it outside of the EU/EEA area. Fastroi offers these model contract clauses for it's Clients. Details of Fastroi's Data transfers regarding the Services and use of model contract clauses can be found in our Data Processing Agreements.

3.8 Security of the Services

We have conducted several risk assessments and Data Protection Impact Assessments (DPIA) to ensure that we have implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The risk based approach is part of our commitment to the ISO 27001 standard. We provide a separate information security white paper upon request.

4 Frequently asked questions

What is ISO 27001?

ISO 27001 is the best-known and globally recognized standard for implementing an information security management system (ISMS) in an organization. An ISMS is a systematic approach to managing information so that it remains secure. This approach includes personnel, processes and IT systems by applying a risk management process.

More information about ISO 27001 standard can be found from International Standardization Organisation (ISO) website.

Where can I find more information about my obligations under the GDPR?

You can find the official text of the GDPR from EUR-Lex.

More in depth information can be found from the websites of different supervisory authorities, such as UK's Information Commissioner, French Information Commissioner or Irish Data Protection Commission.

What is DPIA?

A Data Protection Impact Assessment, or DPIA, is a systematic approach and process to help companies to identify and minimise data protection risks of a project or new business initiative. A key part of a DPIA is to create a systematic description of data processing activities, ensure compliance with mandatory legal obligations as well as make sure implemented information security controls are appropriate to the risk.

Where is user data of Fastroi's Real-Time Care software stored?

By default all Client data is stored within the EU area and Clients may specify the country where Client data will be stored, such as Dublin, Frankfurt, London and Paris. If our client is located in the UK, the data is located in the Amazon Web Services (AWS) London region datacenters.

fastroi

— Caring together —