HOW TO USE SAFETICA TO COMPLY WITH GDPR

safetica®

TABLE OF CONTENTS

INTRODUCTION

What is GDPR?

GDPR is European Union regulation 2016/679 on the protection of natural persons related to personal data handling and on the free movement of such data. GDPR comes into force throughout the EU on 25 May, 2018. It will replace both the current directive 95/46/ES as well as the current personal data protection laws across the Union in every EU country.

The most important requirements of GDPR

- Establish a legal basis for the processing of personal data.
- Specify the purpose of processing personal information.
- Set appropriate data retention time and access rights for handling personal data.
- Maintain records of data handling.
- Ensure personal data security.
- Generate complete documentation of all organizational procedures that can be used as a user guideline and which will serve as a starting point during a security incident.
- Provide employee education on all organizational data processes and how to work securely with sensitive data.
- Ensure the rights of all data subjects are being addressed.
- Under certain conditions, assign a Data Protection Officer (DPO).
- An Impact Assessment (DPIA) (Chapter 4, Section 3) might be needed in the event that a company performs extensive automated data processing or behavior profiling.
- Have entered into contracts, revised according to GDPR, with persons with whom personal information is shared.
- Give a written notice to data subjects (employees) about processing their personal data according to the Right for information.

DATA SECURING AND NECESSARY STEPS TO GDPR COMPLIANCE

What is handled by Safetica?

Safetica is built on technology that collects records logged on endpoint stations. It includes information about computer use, about applications, websites, connected devices, email messages, printing, network traffic, file operations, etc. Because these records are saved in a database, it is necessary take steps to ensure Safetica and the environment in which it is used are GDPR compliant.

Key Steps to GDPR Compliance

Security of the environment

It is highly recommended to use a dedicated server for Safetica Management Service (SMS) in order to increase security and reduce risks of possible threat.

We recommend that administrator access to Safetica databases be limited to the minimum number of necessary administrators, who maintain the smooth operation and availability of services.

After installing Safetica, it is necessary to define individual user accounts and rights according to company roles and recommended principles:

- Principle of Least-Privilege – All users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more.
- Roles distribution – Each user should play a specific role in the system. Administrator should have privileges to configure the product, not to view records. Manager the exact opposite
- We do not recommend using the Safetica system account for any other purpose than assigning roles.

Safetica uses a third-party product (Microsoft SQL server) to store its data. Its functionality and data retention must be managed properly and security has to be set up in a way which minimizes any risks of breaching the personal data stored in it. You can find more details in the document "Post-implementation Recommendations".

General recommendations for ensuring data security:

- Secure physical access to all database files and servers
- Ensure the CIA (Confidentiality, Integrity, Availability) of the processed data
- Optional: MSSQL Enterprise Edition
- Optional: Use of IEEE 802.1X protocol

Legal obligations and responsibilities under GDPR

If a company meets the conditions below, the company must appoint a DPO (Data Protection Officer). A DPO is responsible for overseeing both the data protection strategy and implementation in order to ensure compliance with GDPR requirements. The appointment of a DPO is only mandatory in three situations:

- The organization is a public authority
- The organization's core activities consist of data processing operations that require regular and systematic monitoring of data subjects on a large scale

- There is large-scale processing of special categories of data (i.e. sensitive data such as health, religion, race, sexual orientation, etc.) and personal data relating to criminal convictions and offences.

The Safetica solution may, in exceptional cases, require the appointment of a DPO, depending on the type of company and the scope of use. For a specific assessment, we recommend consulting a corporate lawyer.

In the event of extensive automated data processing or profiling, an Impact Assessment (DPIA) (Chapter 4, section 3) is recommended to determine the severity of impact. We recommend that the DPIA be implemented in consultation with legal representation. In selected cases where it is not possible to sufficiently reduce the risks, the data controller is obliged to inform the supervisory authority. Safetica may, depending on the scope of use (under Article 35 (3) (a)), require the implementation of DPIA. For a specific assessment, we recommend consulting with legal counsel.

GDPR Required Documentation

- If Safetica data is processed by an external entity, such as a Safetica partner, you should sign a data processing contract, as discussed in Article 28 of the GDPR. The contract should address all the necessary stipulations described there.
- As with any security software used in a company, information on Safetica should be included in the company's security policy.
- The company must provide written notice to employees prior to using Safetica. This notice should contain the information described in Article 13 of GDPR.
- Where applicable, it is also mandatory to keep records of personal data processing under Article 30 of the GDPR.

Individual user access and configuration modifications are automatically recorded in Safetica in the Maintenance -> User Accounts, visualization mode.

The rights of data subjects

a. The right to information and the right to access (Chapter 3, Section 2, Articles 13-15)

- If a data subject claims the right to information, you can create a structured table for him/her. An example of such a table can be found in the "Appendix" chapter. The request for information can also be handled by providing written notice (as previously discussed in section 6 c) of "Required Documentation").
- In addition to providing an overview of any processed data, you must also include contact information for the person who is responsible for data processing.

	Title	Last name	First name	Email	Phone
Administrator					
Deputy Administrator*					
DPO*					

*Where applicable

- For a time within the retention period, you can exercise the right to access by providing specific data processing information to the data subject in the form of a Safetica report, or by showing the data in Safetica console.

b. The right to data portability (Chapter 3, Section 2, Article 20)

   This right does not apply to Safetica due to the legal basis that applies (legitimate interest in the protection of a company's intellectual property, falling under Article 6 (1) (f) on the basis of preamble (49)).

c. The right to restrict processing (Chapter 3, Section 3, Article 18)

   An administrator may remove the permissions to view Safetica data subjects' processed data for all user accounts that are affected by the request.

d. The right to rectification (Chapter 3, Section 3, Article 16)

   Data is linked to the data subject by his/her domain name and computer name. An administrator can rename the data subject in the user tree.

e. The right to erasure (Chapter 3, Section 3, Article 17)

   To comply with this right, you must remove users from the user tree in the Safetica Console. Archived data should be deleted when the retention period expires. A retention time of six months is recommended. Other limitation and revocation periods can be established, with a period of up to 15 years or more in some countries.

f. The right to object (Chapter 3, Section 4, Article 21)

   Safetica partners may provide services (such as conducting a security analysis) to Safetica clients. This is a contractual relationship that allows the third party (the partner) to access Safetica data in order to provide their service.

   This relationship must be described in a security policy or written notice.

   In the event that a data subject claims the right to object to the related data, we recommend pointing out the company security policy and discussing the primary goal of the product, which is to protect company assets and support the requirements of GDPR.

ATTACHMENT: SAMPLE TABLE OF PERSONAL DATA PROCESSING

Subject of data processing		Company employees / Modify according to your company details
Description		Descriptive data, records about accessed data and software on company hosts, internet and network usage in general, printer usage and other I/O devices, operations performed on company hosts, error and debug logs from company hosts and software
Purpose of data handling		Legitimate interest of protecting company assets, including but not limited to intellectual property and improving company security
Legal basis (licenses) according to Articles 6 and 9		6(1) f) Legitimate interest
Owner (internally responsible person)		Specify according to your company
Retention period		During the duration of the work contract + 6 months / specify according to your company
Data retention method		Safetica system, database system, backups, archives
Process of data handling		Collecting data from user hosts using the Safetica product. Transferring the collected data using a secured connection to a server and storing in a database. Collected data can be accessed from the Safetica Console and directly from the databases themselves.
External data processors		May be used in case of maintenance or other services provided by a 3rd party / specify according to your company
Transferring data outside of the EU		May occur in case of maintenance or other services provided by a 3rd party / specify according to your company
Company's role (Controller / Processor)		Controller
DPIA necessary?		Specify according to your own data processing
Profiling?		Specify according to your own processing
Processed automatically?		Yes
Right to	Access	Relevant
	Rectification	Relevant
	Erasure	Relevant
	Portability	Not relevant according to the legal basis (see the relevant section in the text above)
	Restrict processing	Relevant
Applied security		Access control, configuration of SQL server, responsible persons, access logs / specify according to your company

Prague | Czech Republic | 23. January 2018.