



How Safetica Helps to Comply With GDPR

Version: 2022-08-08

Introduction to **GDPR**

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).

The GDPR is an important component of EU privacy law and of human rights law, in particular Article 8(1) of the Charter of Fundamental Rights of the European Union. It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business. Superseding Data Protection Directive 95/46/EC, the regulation contains provisions and requirements related to the processing of personal data of individuals (formally called data subjects in the GDPR) who are located in the EEA, and applies to any enterprise regardless of its location and the data subjects' citizenship or residence that is processing the personal information of individuals inside the EEA.

The regulation became a model for many other laws across the world, including those in Turkey, Mauritius, Chile, Japan, Brazil, South Korea, South Africa, Argentina, and Kenya. As of 2021, the United Kingdom retains the law in its identical form despite no longer being an EU member state. The California Consumer Privacy Act (CCPA), adopted on 28 June 2018, has many similarities with the GDPR.

Related **Challenges** and how **Safetica** helps to meet them

1. Comply with Controller's Instructions for Personal Information Processing

It is necessary to establish, monitor, and enforce the rules and instructions on how the processor can operate with personal information.

Safetica enables monitoring of user operations across an entire organization. It can recognize personal information and provide reports on how personal information is processed.



Additionally, Safetica can enforce security policies and desired user behavior whenever users interact with personal information, helping them adhere to best practices or preventing unsecured or prohibited methods of storing and working with personal information.

2. Limit Access to Data to Authorized Employees

Only those who need access to personal information to perform their job have access.

For selected user groups or individual users, Safetica can limit file operations with sensitive/personal information, e.g., uploading, moving/copying, printing, and screenshots.

Safetica provides organization-wide management of storage encryption (Microsoft BitLocker) to ensure that data-at-rest is not accessible to outsiders.

Sensitive data can be blocked from leaving protected devices with encrypted storage. Data flow can be managed to ensure that outgoing data leaves through secure and approved channels.

3. Data Loss Prevention (DLP)

According to GDPR, organizations, whether they are a controller or processor of personal information, are held liable for the loss of any personal data they collect.

With Safetica, personal and other sensitive data are subject to automated classification, which is then used to enforce DLP policies and desired behavior.

Using content inspection, risk analysis, and DLP policies set for all data channels, Safetica solutions can recognize when somebody makes a mistake or takes chances with your sensitive data.

Depending on the mode that the Safetica solution is set to, it can either block the risky activity, notify the user (and admin), redirect employees to the organization's security guidelines, or allow them to justify the restricted operation.

4. Encryption

Encrypting data at rest, in use, and in transit is one of the pillars of GDPR compliance.

Safetica helps organizations manage storage encryption (Microsoft BitLocker), thus protecting data at rest. The encryption is centrally managed in the Safetica management console, with encryption keys distributed securely across secure endpoint devices, eliminating the need to share them between users.

For the encryption of files in use and in transit, an additional solution is needed.

5. Threat Detection

In the event of an attempt to misuse personal information, there must be a mechanism to red flag the activity and inform delegated employee(s) about the situation.

An affected organization is obliged to report any occurred PII data incident to authorities within 72 hours.

Actual or attempted data security incidents are flagged within the Safetica solution. Automated reporting and real-time email alerts promptly notify the appropriate personnel, inform them of the incident, and provide sufficient detail to assess the impact of the situation.

Based on the incident alerts and detailed logs (records), you can report the incident to the [data protection authorities](#) in time and provide them with any necessary documentation.

6. Know the Personal Information Flow

It is necessary to understand where and how personal information flows through internal company processes, where it is stored, and how it is communicated and shared with external parties.

Safetica's detailed file and user operation monitoring and audit provide an overview of information flows, critical sensitive data storage, and detailed information about:

- which exact external parties and storage have been contacted
- which of these received the organization's sensitive data.

Key Use Cases

Real Estate Development

Network of building material warehouses P.H.U. BROKER Sp. providing development services (construction, sale, and rent of housing and commercial investments) needed to comply with data protection regulations, especially GDPR, and protect its employees and customers.

- **Problem:** Need to comply with all the regulations concerning data protection (especially GDPR) and to protect employees and customers.
- **Solution:** Safetica ONE provides monitoring of computers throughout the company, branch offices, and commercial outlets. Safetica also monitors database servers and external storage. Safetica ONE Discovery provides a thorough analysis of data traffic and the flow of information in the organization. DLP rules and reports on security incidents allow for a faster response in the event of data protection policy violations and reduce the risk of accidental data leakage.



- **Results:** In addition to regulatory compliance, Discovery can be used prior to DLP deployment to identify potential sources of a data breach. IT specialists also value the intuitive interface, which makes day-to-day work much easier.

Healthcare clinic


Private healthcare clinic Gyncentrum specializes in clinical research and specialist training, and they needed to protect sensitive patient data and comply with GDPR.

- **Problem:** Owner/DPO needed to protect sensitive patient data, employee personal data, mailing databases, internal procedures, confidential reports, and results of clinical research.
- **Solution:** Deploying Safetica made it possible to perform an audit and reveal all potential threats, so they could implement a complex data leakage prevention policy.
- **Result:** Employees' activities are reported, and patients' data protected. Safetica's DLP solution was deployed across three separate locations with one central console. Moreover, the company can remotely manage Bitlocker for data encryption.

Audit, tax & advisory

The audit company PP&C Auditores Independentes needed to protect their sensitive client data and be LGPD (Brazilian version of GDPR) compliant.

- **Problem:** The IT manager needed to protect clients' personal, financial, and other sensitive data.
- **Solution:** Safetica makes it easy for PP&C to analyze all users' computers, primarily to see how data is manipulated and to understand users' data-handling behavior. The company can adapt the system with the necessary controls to comply with the new Brazilian General Data Protection Law (LGPD), in addition to updating all standards and IT procedures. Using both content inspection and a context-aware approach, Safetica ONE can classify almost any type of data. Using these classification methods, PP&C was able to get an overview of what is happening with the data in their company.
- **Results:** The company is compliant with LGPD. PP&C's Channel Communications Control, which transfers customer data to electronic environments outside the company, will only work when the data is adequately protected. The management gets weekly summary reports on users' internet activities, use of applications, and printed documents. Monitoring files on the file server helps to better understand and improve the use of company assets. Furthermore, PP&C management is immediately notified if a security incident occurs.



Excellent Data Protection Made Easy

safetica

© Copyright All rights reserved. Safetica and the Safetica logo are registered trademarks. All trademarks are the property of their respective owners.

www.safetica.com