Scrut Automation | tsaaro

Best Practices for **Automating GDPR Compliance**

Contents

Overview

The General Data Protection Regulation (GDPR) was put into effect on May 25, 2018, by the European Union (EU) to protect the data privacy of individuals within the EU and the European Economic Area (EEA).

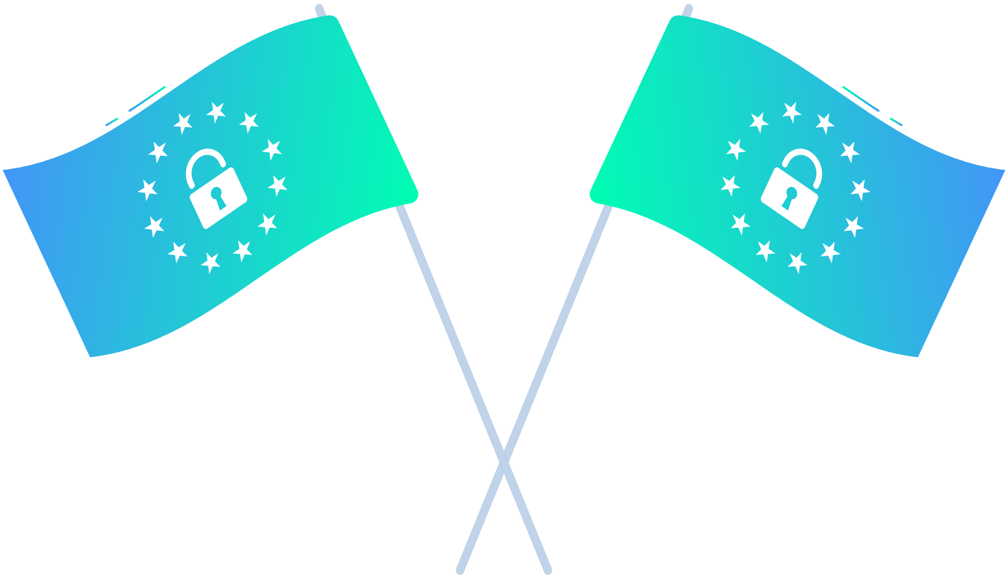
It is considered to be one of the strictest data protection laws in the world and is applicable to people and organizations located not only in the EU but anywhere in the world that process the personal data of EU residents.

GDPR enforces the concept of "privacy by design," which implies that security and regulatory compliance can no longer be treated as bolt-ons or afterthoughts. It results in a better cybersecurity posture since the organization follows stringent policies and procedures for tighter security.

Organizations that fail to comply with the GDPR can face a number of sanctions, including fines of up to €20 million or 4% of global annual turnover, whichever is greater.

An effective method most organizations are adopting to avoid penalties and achieve compliance is through automation. Organizations can reduce risk while enabling speed to market and competitive advantage by applying continuous automation to GDPR regulations.

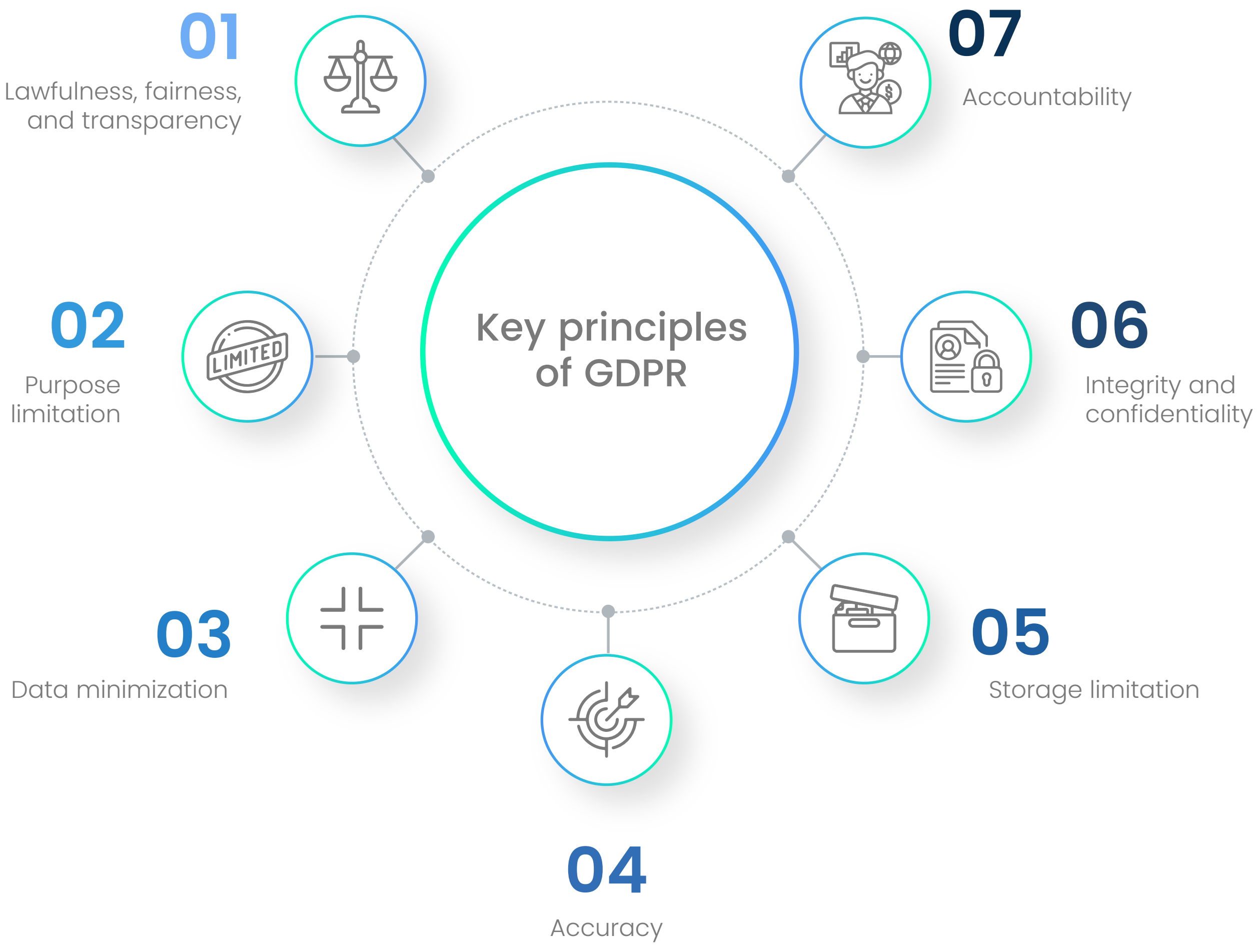
This ebook will delve into the key principles of GDPR, how automation can accelerate compliance with GDPR requirements, and its benefits.



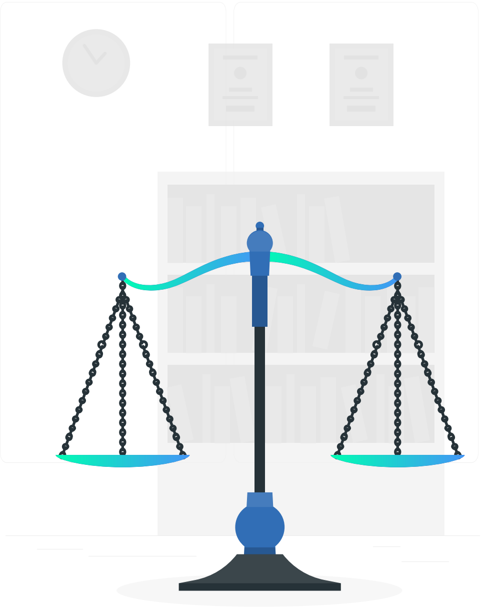
Key principles of GDPR

At the core of GDPR, there are seven principles that serve as a wireframe to the regulation. These principles play a crucial role in ensuring the protection of an individual's privacy rights and establishing a secure and transparent environment for handling personal data.

Adhering to these principles is not only essential but is also a mandatory requirement. Let's look at the seven key principles of GDPR in some detail.



Lawfulness, fairness, and transparency



Lawfulness means the organization has a legal basis for processing the data of the subject. One of the legal basis for processing data can be valid legal consent. It is also the most common way to obtain a legal basis for data processing.

Fairness refers to the processing of personal data in the best interests of the data subject and is in accordance with the scope that can be reasonably expected by a person.

Transparency involves clearly communicating the reason behind data processing, the type of data processing, and the method of processing communicated to the data subject. The data subject should easily understand the scope and method of data processing.

Purpose limitation

The purpose limitation principle says that the organization cannot use the data for any other purposes except the purpose for which it was originally intended and permitted. The organization can only process the data for which the data subject has consented.

Data minimization

Data minimization is a concept that discourages organizations from storing data that it has no need for. They should only keep the data until there is a need for service and only the amount of data needed. If the particular data field is not needed, the organization should not collect or store it.

Accuracy

The accuracy principle states that the data should be accurate and up to date. As a data controller, an organization must ensure that the data remains so by taking reasonable measures.

Storage limitation

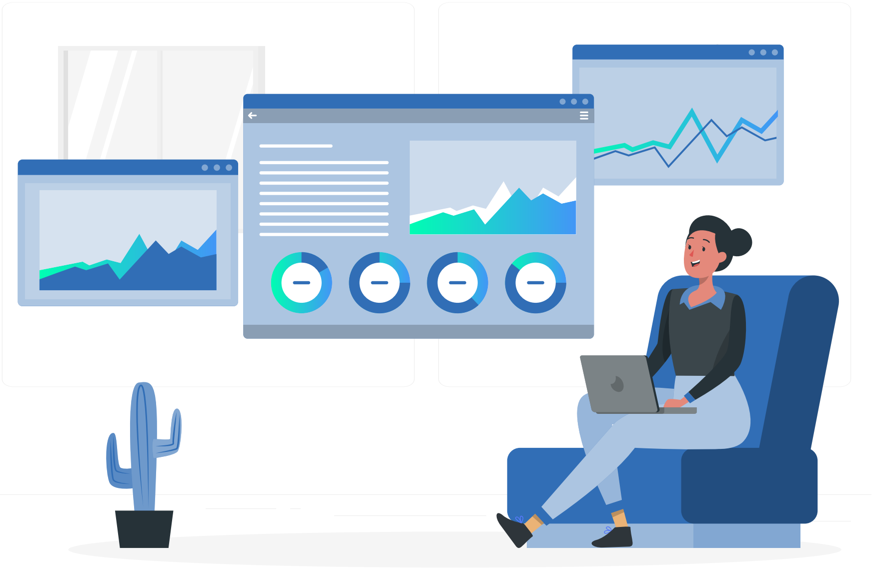
It refers to the time limit for which the data can be stored. If the organization does not need it, it should delete the data immediately. Although it is very similar to the data minimization principle, it relates to time rather than fields, as with data minimization.

Integrity and confidentiality (security)

In relation to information security, data should follow the CIA triad - confidentiality, integrity, and availability. Data should have integrity - meaning, data should not be tampered with in any way. Second, data should be handled with confidentiality. That means data should be shared with people with proper authorization only. And third is availability, which means data should be available when the authorized person needs it. The GDPR requires organizations to follow the CIA triad.

Accountability

As the name suggests, the organization is accountable for the data processing it does. It must follow the rules and regulations of GDPR while processing data. It should also document its processes and procedures to prove adherence to the regulations.



What is GDPR automation?

GDPR automation refers to the use of technology, tools, and software solutions to streamline and automate processes related to compliance with the General Data Protection Regulation (GDPR). It involves leveraging automation to manage and protect personal data in a manner that aligns with GDPR requirements.

Organizations may better handle the complexity of data protection and privacy rules with the aid of **GDPR automation**. Large amounts of data can be handled effectively, requests from data subjects can be answered quickly, data breaches can be detected and mitigated in advance, and strong compliance processes can be established.

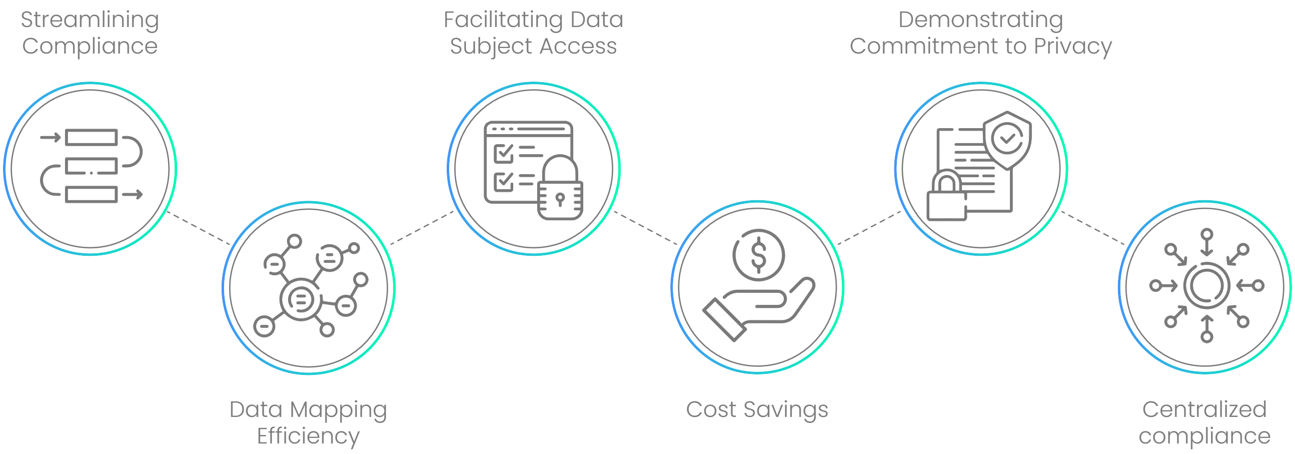
Tools for automation can carry out several tasks, including data discovery and classification, consent management, processes for dealing with requests from data subjects, automated data breach detection and reporting, and the creation of privacy policies - efficiently.

How Automation Helps in Achieving GDPR Compliance

Utilizing modern cutting-edge GRC tools to understand, categorize, and manage personal data is a key component of GDPR compliance automation. This enables organizations to efficiently and accurately keep track of the data they gather, retain, and use for each individual.

At the very core, a GRC automation tool for GDPR helps organizations identify compliance gaps and comply with GDPR requirements more effectively and efficiently. Automating GDPR compliance can help organizations streamline processes, reduce errors, and ensure ongoing adherence to regulations. But that’s just the crust of it - there are several reasons why automating GDPR compliance can help organizations in the long run.

Why is it important to automate GDPR compliance?



Streamlining Compliance

Data Mapping Efficiency

Facilitating Data Subject Access

Cost Savings

Demonstrating Commitment to Privacy

Centralized compliance

Streamlining Compliance

Automating GDPR compliance processes helps identify and manage personal data falling under GDPR regulations. It efficiently analyzes data, identifies patterns, and alerts the compliance team to areas requiring attention.

Data Mapping Efficiency

Automation reduces manual errors and saves time in tracking and organizing data, enabling organizations to meet GDPR requirements more effectively.

Facilitating Data Subject Access

Automation aids in fulfilling data subject access requests by maintaining an organized and up-to-date inventory of personal data that can be easily accessed when needed.

Cost Savings

By reducing manual labor in data management and compliance processes, automation can lead to cost savings for organizations.

Demonstrating Commitment to Privacy

Utilizing GDPR automation showcases a business's dedication to data protection and privacy, fostering consumer trust and enhancing its reputation in a competitive market.

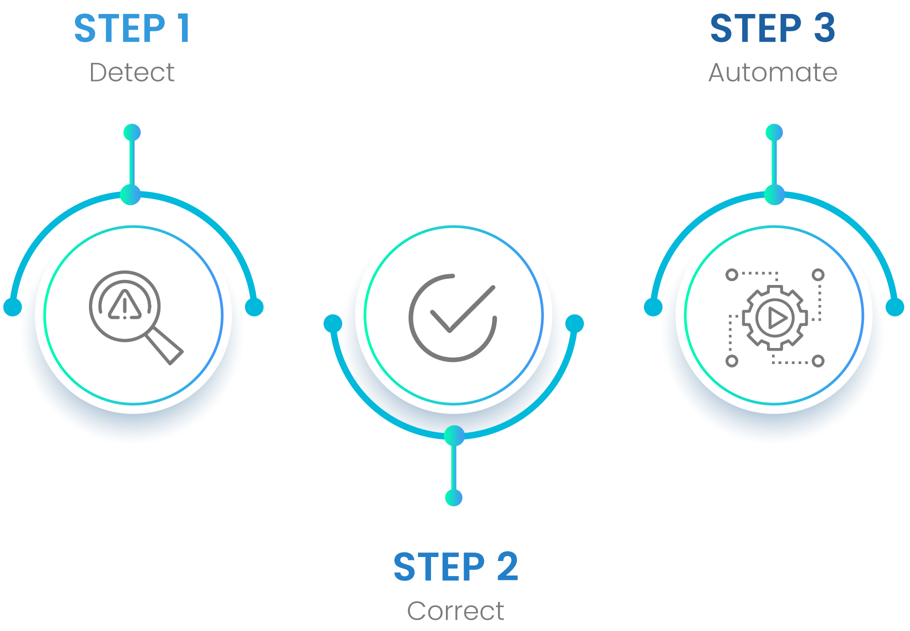
Centralized compliance

Automation is not just limited to GDPR compliance, it allows you to map controls to various security frameworks in one go, reducing the need to perform the same processes again and again. By implementing compliance automation, you can get compliant with multiple security frameworks at once.

In summary, GDPR automation optimizes compliance efforts, improves operational efficiency, and reinforces an organization's commitment to data privacy.

How to kick-start your GDPR automation journey?

A detailed and widely disseminated roadmap is essential for each new initiative. The same is true for automated GDPR compliance. A tried and tested roadmap that most organizations are following in their approach to automate GDPR compliance includes the following steps.



STEP 1
Detect

STEP 3
Automate

STEP 2
Correct

DETECT

Conduct a comprehensive data mapping exercise to identify the personal data your organization collects, processes, stores, and shares. This includes understanding the types of data, sources, recipients, and transfers of personal data. Create a data inventory that documents these details.

CORRECT

Then, you will be required to evaluate your existing processes, procedures, and policies against the requirements of the GDPR. Identify any gaps or areas that require improvement or automation to ensure compliance. Implement corrective measures consistently and broadly by prioritizing areas that need the most attention. Consider factors such as the volume of data, the complexity of processes, and potential risks associated with specific activities. This will help you determine which compliance processes should be automated first.

AUTOMATE

The last step in this model is to automate the detection and correction processes. Say goodbye to repetitive and duplicate tasks, reduce manual intervention, and implement corrective measures in one go - using automation tools.

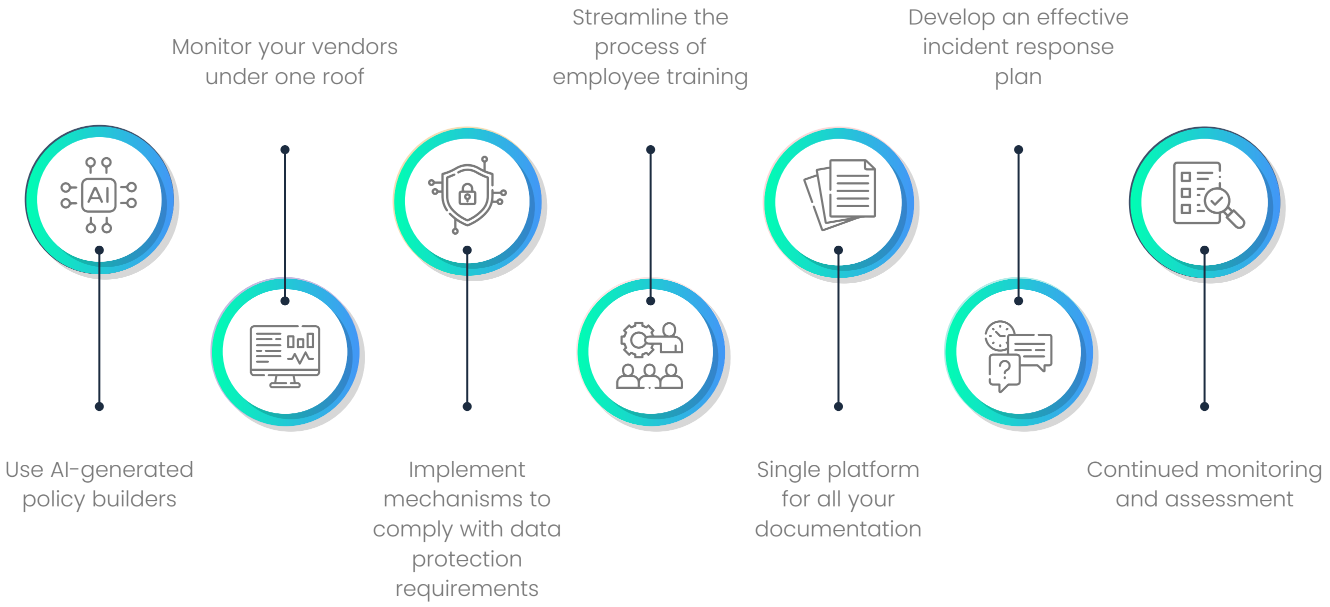
Research and evaluate automation tools or software solutions that align with your organization's needs. Look for tools that offer features such as data mapping, consent management, data subject request handling, breach detection, and policy management. Consider factors like scalability, integration capabilities, and user-friendliness.

Create a detailed plan for implementing the chosen automation tools. Define the roles and responsibilities of the team members involved, set timelines and milestones, and allocate necessary resources for the implementation process.

Best practices to follow for Automating GDPR Compliance

Policy creation, evidence collection, control monitoring, and vendor management are some of the processes an organization is required to implement under GDPR compliance. But manually meeting all these requirements can be time and resource-consuming. The key here is to automate these processes. But how?

Below are certain practices that an organization can adopt and implement to streamline compliance and build a strong security culture.


Use AI-generated policy builders
Monitor your vendors under one roof
Implement mechanisms to comply with data protection requirements
Streamline the process of employee training
Single platform for all your documentation
Develop an effective incident response plan
Continued monitoring and assessment

Use AI-generated policy builders

Reduce the manual effort required in policy development by using modern policy-building mechanisms that analyze the regulatory requirements and organization-specific factors to create policies that align with the organization's data processing activities. These AI-powered policy builders can also monitor changes in GDPR regulations and automatically update policies accordingly. This proactive approach helps organizations stay up to date with regulatory requirements without relying on manual monitoring processes.

Monitor your vendors under one roof

Automate the process of assessing and managing data processors and third-party vendors. Ensure they meet GDPR requirements and have appropriate data protection measures in place. Implement mechanisms to monitor and enforce compliance throughout the vendor relationship.

Implement mechanisms to comply with data protection requirements

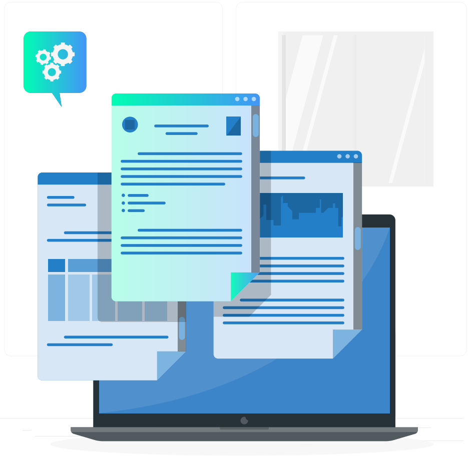
Establish automated processes to handle data subject requests, such as the right to access, rectify, erase, restrict processing, and data portability. Implement mechanisms to verify the identity of data subjects and respond to requests within the specified timelines. You can also use automated mechanisms to enforce data retention periods and securely delete personal data when it is no longer needed.

Streamline the process of employee training

By automating employee training for GDPR compliance, organizations can ensure consistent, scalable, and efficient delivery of essential knowledge, track progress, and maintain up-to-date training content. It strengthens the overall compliance culture within the organization, reducing the risk of data breaches and non-compliance.

Single platform for all your documentation

One of the best practices you can follow to automate GDPR compliance is streamlining documentation collection and storage. Having a single platform for all your documentation ensures that you have all the right reports and evidence at hand, which helps demonstrate compliance efforts during audits or regulatory inquiries without any extra effort.



Develop an effective incident response plan

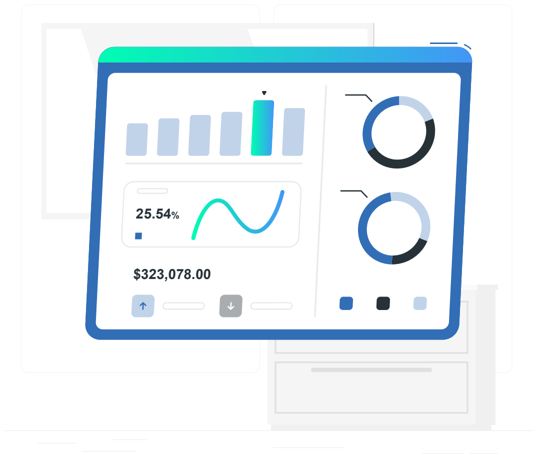
Under GDPR, a data breach is defined as a security incident where there is unauthorized or accidental access, disclosure, alteration, loss, or destruction of personal data. Developing an effective incident response is, therefore, integral for organizations in order to comply with GDPR.

This is why organizations are advised to implement automated systems to detect and respond to data breaches promptly. This includes setting up alerts for suspicious activities, logging access to personal data, and conducting regular security audits.

	Timeframe	Information to include	Justification for delay
Notification to the supervisory authority	Within 72 hours of becoming aware of the breach	● Detailed information about the breach ● The categories and number of affected individuals ● The types of data involved ● The potential consequences ● Measures taken or proposed to address the breach	If the organization is unable to meet the 72-hour timeframe, it should provide reasons for the delay along with the notification, explaining the reasons for the delay and providing updates as more information becomes available.
Notification to data subjects	If a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, organizations must also communicate the breach to the affected individuals without undue delay.	● Nature of the breach ● Clear and understandable information about the potential consequences ● Suggest measures individuals can take to mitigate the risks.	If the data breach is unlikely to result in a risk to the rights and freedoms of individuals, notification to data subjects may not be required. However, the organization must document its assessment of the risk and be able to demonstrate compliance with this exception. If the organization has implemented appropriate technical and organizational protection measures that make the data breached unintelligible or protected the data in a way that renders it inaccessible, notification to data subjects may not be necessary.

Continued monitoring and assessment

Implement automated monitoring systems to track data processing activities, system access, and security events. Regularly audit and review the effectiveness of your automated compliance processes, including evaluating data protection policies and procedures.



Start your automated GDPR compliance journey today!

While automation can help streamline GDPR compliance, it is essential to regularly assess and adapt your processes as the regulatory landscape evolves. It is also recommended to consult legal professionals or data protection experts to ensure your automated compliance efforts align with the specific requirements of your organization and jurisdiction.

This is where Scrut and Tsaaro come in. Scrut's single window compliance automation platform, paired with Tsaaro's high-end expertise in data protection services, provide organizations with end-to-end compliance monitoring.

Organizations can accelerate GDPR compliance using continuous control monitoring and automated risk management and develop a robust security posture by integrating privacy by design using Scrut's and Tsaaro's automation and consultancy services.

Schedule a call with us today to learn more about how our platform can aid your organization in streamlining your data protection journey.