ManageEngine
DataSecurity Plus

Data discovery:

# Your first step towards **GDPR compliance**

www.datasecurityplus.com

# Table of contents


# Introduction

Organizations collect and process a huge amount of personal data for their daily operations. Most of the time, individuals have little or no awareness about how much of their personal data resides in various organizations' databases. As an organization stores more and more personal data, its risk of data loss or a data breach goes up. To avoid these security risks, many groups are calling for regulations that:

- Set high standards of privacy and security in personal data processing and retention.
- Offer individuals more visibility and control over who has their personal data, how it's collected, how long it will be retained, and what it will be used for.

# The GDPR—A revolutionary move in data privacy

The General Data Protection Regulation (GDPR) is Europe's newest data protection law , designed to unify and improve the privacy of personal data across Europe. The GDPR intends to provide European Union (EU) residents with more visibility and control over the way their personal data is collected and processed.

There are 99 articles and 173 recitals in the GDPR that establish all obligations and requirements that organizations will have to comply with when the GDPR goes into full effect on May 25, 2018.

**British Airways (2019)** — **€204,600,600**

Over 500,000 customers personal data was compromised when British Airways' official website redirected users to a fraudulent site.

The company was fined for its outdated and negligent security practices.

**Marriott International (2019)** — **€110,390,200**

Personal data of over 300,000,000 users was leaked in a hack dating back to 2014 that began when the Starwood Hotels' systems were compromised.

Though Marriott International acquired Starwood Hotels in 2016, the lack of stringent security measures led to the hack going undetected till the end of 2018.

**Google Inc (2020)** — **€50,000,000**

Google was fined for violating Articles 5, 6, 13, and 14 of the GDPR.

The lack of transparency on how personal data was used to target users for paid ads and failing to procure proper consent were some of the reasons for which Google was fined.

Figure 1:Top GDPR penalties so far

# Who does the GDPR apply to?

**The GDPR applies to all businesses that:**,

- Operate in the EU.
- Process the personal data of EU residents (regardless of location).
- Provide goods or services to people in the EU (regardless of where processing takes place).

# What data does the GDPR protect?

The GDPR focuses on securing and ensuring the privacy of EU citizens' personal and sensitive personal data. So what's the difference between personal data and sensitive personal data?


### Personal data

Any data that can be used to identify an individual directly or indirectly is classified as personal data. Examples: Name, location, identification number, online identifier, income, and localization.

### Sensitive personal data

Special categories of personal data that must have additional protection are classified as sensitive personal data. Examples: Biometric data, sexual orientation, race, genetic data, political opinion, and medical conditions.

# How should personal data be processed?

The GDPR has defined six important principles on how personal data should be processed. It mandates that personal data shall be:

- Processed lawfully, fairly, and in a transparent manner **(Lawful, fair, and transparent).**
- Collected only for specified, explicit, and legitimate purposes. Data should not be further processed in a manner that conflicts with these initial purposes **(Purpose limitation).**
- Adequate, relevant, and limited to what is necessary **(Data minimization).**
- Accurate and, where necessary, kept up-to-date **(Data accuracy).**
- Processed in a way that data subjects can't be identified once their data has been used for its original purpose **(Storage limitation).**
- Processed in a manner that ensures security of personal data. This includes protection from accidental loss, destruction, or damage by implementing required technical and organizations measures **(Data integrity and confidentiality).**

**GDPR TIDBITS**
FACT vs. FICTION

**Myth:**

All organizations need to have a data protection officer (DPO).

**Fact:**

**Only a few types of organizations must have a DPO, including:**

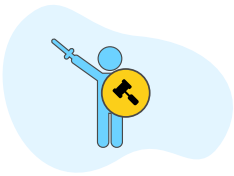
- Public authorities.
- Organizations performing large-scale systematic monitoring.
- Organizations involved in large-scale processing of sensitive personal data.

**Reference: Article 37**

# What are the consequences of not complying with the GDPR?

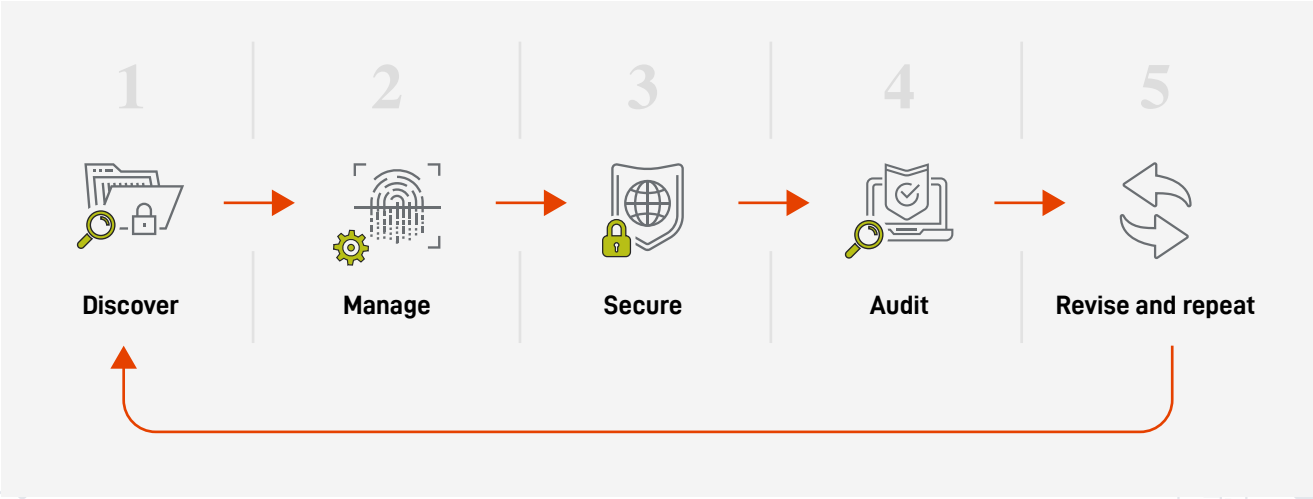
Once the GDPR is enforced, organizations could face a few different penalties for non-compliance depending on the infraction. Possible consequences include:

- Suspending all data processing.
- Paying a fine of up to four percent of their annual worldwide turnover or 20 million euros—whichever is higher.
- Other sanctions including warnings, reprimands, and corrective orders.



# A five-step action plan for your GDPR compliance journey

The GDPR aims to regulate how organizations collect, store, process, and transfer personal data. The following five-step action plan provides a holistic approach to help you on your journey towards GDPR compliance.



## Discover

### Know where personal data lies.

The first step towards GDPR compliance is identifying where personal data resides. An inventory of your organization's personal data is a prerequisite for GDPR compliance. During the data discovery phase, you need to know:

- Where and in what form personal data is stored.
- What types of personal data are stored.
- Who has access to personal data, including when, where, and how personal data is used.

## Manage

### Govern how personal data is shared and used.

After data discovery, the next step is to establish accountability in the flow of personal data within your organization. Enforce policies, rules, and regulations to ensure data handling, sharing, and storage techniques are in compliance with the GDPR. Some important questions organizations should answer during this phase include:

- What's the lawful basis for holding this personal data?
- Is any personal data shared with third parties? If so, why?
- How is personal data processed?
- How long can personal data be stored?
- How do we track a data subject's personal data?

## Secure

### Protect data from loss, misuse, and breaches.

The GDPR mandates that data be stored, processed, and shared in a manner that ensures its security. Depending on the type, context, location, and volume of personal data that your organization stores, you may need to implement measures such as encryption, pseudonymization, and anonymization to reduce the risk of data exposure. During the securing phase, you need to ask yourself:

- What technical and organizational measures are in place to safeguard personal data?
- Can you detect and respond to system infiltrations or data breaches in real time?
- Are regular data protection impact assessments being carried out?
- What are your organization's provisions for handling the data breach notification process?
- Is there a data security incidence response plan in place?

## Audit

### Generate reports to prove GDPR compliance.

The GDPR mandates that organizations document all data processing, sharing, and retention activity. Depending on your organization's industry and size you might have different levels of documentation requirements to comply with. Your organization needs to verify if:

- It can ensure the confidentiality, integrity, and availability of personal data.
- It can provide audit trails to establish accountability and empower forensic analysis.
- It can handle requests for erasure and other demands from data subjects.

## Revise and repeat

### Regularly check and adapt the compliance process.

GDPR compliance isn't a one-shot exercise; it's a continuous process of keeping up with a consistently evolving compliance environment, changing technologies, and data privacy requirements to demonstrate compliance at any point of time.

# Data discovery: Your first step towards GDPR compliance

**What is data discovery?**

Data discovery is the process of collecting data from various databases, identifying hidden patterns, and extracting actionable information from these trends.

**How important is data discovery to the GDPR?**

Data discovery is an implicit prerequisite to meeting multiple GDPR compliance requirements. To categorize, catalog, monitor, and secure personal data such as names, SSNs, biometric data, and more, data discovery has to be the first step. Your organization needs to develop and maintain a data inventory map of all personal data; the easiest way to achieve this is with the help of an effective data discovery solution that can help you identify:

- Where personal data is stored.
- What type and volume of personal data is stored.
- When stored personal data was last modified.
- Who has access to stored personal data.
- Why personal data is being stored.

**Which GDPR requirements does data discovery help meet?**

Data discovery helps address the following GDPR requirements, as well as many others:

**Article 15**
Exercising access rights of data subjects

> *"The data subject shall have the right to obtain...the categories of personal data concerned...to whom personal data have been or will be disclosed..."*


**Myth:**

All consent must be acquired explicitly.

**Fact:**

Consent is one among six of the GDPR's lawful bases of processing. Legitimate interest, performance of a contract, etc. may also be considered appropriate reasons for processing personal data without getting consent.

**Reference: Article 9(2)**

**Article 16**
Right to rectification

> *"The data subject shall have the right to obtain...the rectification of inaccurate personal data concerning him or her..."*

**Article 30**
Record keeping of processing activities

> *"...The record shall contain all of the following information...categories of personal data..."*

**Article 32**
Security of processing

> *"...the controller and the processor shall implement appropriate technical and organizational measures...to ensure security...of personal data"*

**Article 35**
Data protection impact assessment

> *"...Data protection impact assessment...shall in particular be required in case of...processing on a large scale of special categories of data...or of personal data relating to criminal convictions and offences..."*

Recital 13 | Recital 39 | Recital 82

**GDPR TIDBITS**
FACT VS. FICTION

**Myth:**

All security breaches will have to be reported within 72 hours to the Information Commissioner's Office and any affected individuals.

**Fact:**

Organizations are only required to report a data breach under the GDPR if the breach is likely to result in a "risk to an individual's rights and freedoms." And the breach notification clause only gets triggered after the controller becomes aware of the breach.

**Reference: Article 33**

**Myth:**

Personal data that's already stored in an organization's database need not be GDPR-compliant.

**Fact:**

The GDPR will apply to all personal data stored in an organization, regardless of when it was collected.

**Reference: Article 3**

# Meet your data discovery needs with **DataSecurity** Plus

DataSecurity Plus' data discovery capability helps you create and maintain an inventory of personal data scattered across your file servers. It helps locate various types of personal data such as credit card details, names, ages, locations, online identifiers, and other personally identifiable information (PII). Knowing where, how, and why personally identifiable information is stored helps not just with the GDPR, but also with compliance standards like HIPAA and PCI DSS.

# Phases of **DataSecurity** Plus' data discovery solution

**Find personal data.**
Locate the files, folders, or shares that store PII.

**Understand personal data.**
Gain visibility into the type of personal data your company holds (e.g. names, ages, banking details, and SSNs) to see which files and folders are most important security-wise.

**Track personal data.**
Monitor who accesses personal data, including when, where, and how the personal data is used.

**Secure personal data.**
Monitor file activities for sudden spikes in usage, as these can indicate potential ransomware attacks and unauthorized modifications.

**GDPR TIDBITS**
FACT VS. FICTION

**Myth:**

Consent is the only way through which personal data can be processed.

**Fact:**

Consent is one way to comply with the GDPR, but not the only way. An organization can legally process personal data without gaining consent if they need to:

- Comply with a legal obligation.
- Fulfill a contract.
- Perform a task carried out in public interest.
- Meet a legitimate interest.
- Protect the vital interest of data subjects.

**Reference: Article 6**

# Key GDPR requirements that DataSecurity Plus' data discovery functionality helps address

| GDPR Article | How DataSecurity Plus helps |
|---|---|
| **Article 15(1)**<br>The data subject has the right to request what information about them is being processed. | Finds the personally identifiable information (PII) of a specific user using RegEx or by matching a unique keyword, e.g. customer ID, name, etc. across Windows file server and failover cluster environments. |
| **Article 15(3)**<br>The controller shall provide a copy of the data undergoing processing. | Identifies the location where personal/sensitive personal data is stored to facilitate further processes. |
| **Article 16**<br>The data subject can request the controller to rectify inaccurate information concerning him/her. | Uses data discovery to find instances of data subject's personal/sensitive personal data using a unique keyword set, e.g., national identification number, credit card details, license number, etc. |
| **Article 17(1)**<br>In compliance with guidelines mentioned in the law, the data subject has the right to request the controller to erase all information concerning him/her. | Locates all the files containing instances of the data subject's information by matching keywords. |
| **Article 30(1)**<br>A record of all processing activities along with details on the sensitive data processed and the technical measures used to safeguard the data shall be maintained. | 1. Locates instances of personal/sensitive personal data stored across Windows file servers and failover clusters utilizing a dedicated GDPR data discovery policy.<br>2. Scans for national identification numbers, credit card details, license number, and more.<br>3. Finds who has what permission over files containing sensitive personal data. |
| **Article 35(7)(d)**<br>A data protection impact assessment should include measures envisaged to address risks including safeguards and safety measures to ensure the protection of personal data. | 1. Calculate the risk score of files containing personal sensitive personal data by analyzing their permissions, volume and type of rules violated, audit details, and more. |

## Additional GDPR requirements that DataSecurity Plus help address

| GDPR Article | How DataSecurity Plus helps |
|---|---|
| **Article 5(1)(c)**<br>Personal data should be adequate, relevant, and limited to what is necessary. | Finds and deletes junk data including stale, duplicate, and orphaned files, and helps ensure that only required, relevant data is stored. |
| **Article 5(1)(f)**<br>Personal data should be protected against accidental loss, destruction, or damage. | **To help maintain data integrity:**<br>1. Audits file and folder actions including create, rename, delete, copy, and more, in real time.<br>2. Triggers instant email alerts to admins about monitoring suspicious file actions, such as excessive permission changes, renames, etc.<br>3. Tracks failed attempts to access your critical data.<br>4. Maintains a foolproof audit trail of all file accesses to aid forensic investigations.<br><br>**To help maintain data security:**<br>1. Detects and contains potential ransomware infections instantly to prevent devastating data loss.<br>2. Detects and prevents the leakage of business-critical files via USB devices, or as an email attachment. |
| **Article 24(2)**<br>Appropriate data protection policies are to be implemented to protect the rights of data subjects. | 1. Uses predefined policies to help prevent unwarranted data transfers to USB devices, monitor file integrity, and more.<br>2. Uses automated threat response mechanisms to shut down infected systems, disconnect rogue user sessions, and more. |
| **Article 25(2)**<br>Practice data minimization and ensure that personal data is not accessible by an indefinite number of individuals. | 1. Find users with full control access to your Windows shares.<br>2. Locate all the files and folders that have been shared with everyone. |
| **Article 32(2)**<br>Technical and organizational measures to address the risk in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted or stored shall be implemented. | **To address the risk of potential data leaks:**<br>1. Monitors the use of removable storage devices such as USBs in your organization.<br>2. Blocks the movement of files containing personal data to USB devices, or via email as attachments.<br>3. Provides contextual warnings using system prompts about the risk of moving business-critical data to removable storage devices, or via email as attachments.<br>4. Reduces incident response times with instant alerts, and an automated threat response mechanism. |

| | |
|---|---|
| | **To address the risk of unauthorized accesses or disclosure:**<br>1. Alerts and reports on unwarranted accesses, or sudden spikes in file accesses and modifications, including permission changes, deletions, and more.<br>2. Spots files with security vulnerabilities such as:<br>* Files owned by stale users.<br>* Critical files that allow full control access to users.<br>* Overexposed files, or files accessible by everyone.<br>3. Tracks sudden spikes in failed attempts to access your files/folders.<br>4. Reviews access rights and file permissions periodically.<br><br>**To address the risk of accidental or unlawful destruction:**<br>1. Maintains a complete record of all file and folder deletions, along with details on who deleted what, when, and where.<br>2. Uncovers and quarantines possible ransomware infections. |
| **Article 33(3)**<br>In case of a personal data breach, the notification should include measures taken to address and mitigate the possible adverse effects of the personal data breach. | Helps analyze the root cause and the scope of the data breach using extensive records on all file and folder related activities in Windows file\ servers, failover clusters, and workgroup environments. Provides details on who accessed what, when, and where. |

# DataSecurity Plus

ManageEngine DataSecurity Plus is a data visibility and security solution. It tracks and alerts on critical file modifications and movement across file servers, failover clusters, workstations, and USBs. Users can locate and analyze files containing PII/ePHI stored in Windows file servers, failover clusters, and OneDrive environments using built-in data discovery rules. Its data leak prevention (DLP) capability helps detect and respond to the exfiltration of sensitive data via USBs, email, printers, and more. It also provides detailed audit reports that help organizations streamline compliance with multiple IT regulations.

To explore these features and see DataSecurity Plus in action, launch the online demo.
To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

Download free trial  $ Get a quote

## Explore
## **DataSecurity Plus' solutions**

**File server auditing**

Audit, monitor, report on, and alert on all file accesses and modifications made in your file server environment in real-time.

Learn more

**Data leak prevention**

Detect, disrupt, and respond to sensitive data leaks via USB deivces, emails, printers, and more through real time security monitoring.

Learn more

**Data risk assessment**

Perform content inspection and contextual analysis to discover sensitive data in files, and classify it based on vulnerability.

Learn more