ManageEngine
DataSecurity Plus

GDPR Compliance

Satisfy EU GDPR Data Protection Requirements with DataSecurity Plus

www.datasecurityplus.com

Become GDPR compliant using DataSecurity Plus

DataSecurity Plus helps you strengthen your organization's security posture, prevent data leaks, and avoid compliance-related penalties. Meet the GDPR's stringent requirements using the various reports generated by DataSecurity Plus.

Let's take a look at some of the common GDPR articles, and learn how DataSecurity Plus can help you comply with these requirements easily:

What the GDPR article say:	What you should do:	How DataSecurity Plus helps:
Article 5(1)(c) Personal data should be adequate, relevant, and limited to what is necessary.	Remove redundant, obsolete, and trivial data, i.e. unnecessary files from your data stores.	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) Personal data should be protected against accidental loss, destruction, or damage.	Bring in the right technical and organizational measures to ensure the integrity, security, and confidentiality of personal and sensitive data.	**To help maintain data integrity:** 1. Audits file and folder actions including create, rename, delete, copy, and more, in real time. 2. Triggers instant email alerts to admins about monitoring suspicious file actions, such as excessive permission changes, renames, etc. 3. Tracks failed attempts to access your critical data. 4. Maintains a foolproof audit trail of all file accesses to aid forensic investigations. **To help maintain data security:** 1. Detects and contains potential ransomware infections instantly to prevent devastating data loss. 2. Detects and prevents the leakage of business-critical files via USB devices, or as an email attachment.
Article 15(1) The data subject has the right to request what information about them is being processed.	Locate and share all information about the data subject stored by your organization.	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) The controller shall provide a copy of the data undergoing processing.	Share an electronic copy of all data relevant to the data subject stored by the organization.	Identifies the location where personal/ sensitive personal data is stored to facilitate further processes.
Article 16 The data subject can request the controller to rectify inaccurate information concerning him/her.	Locate and revise all instances of inaccurate information about the data subject.	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) 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.	Find and delete all instances of the data subject's personal/ sensitive personal data.	Locates all the files containing instances of the data subject's information by matching keywords.
Article 24(2) Appropriate data protection policies are to be implemented to protect the rights of data subjects.	Implement necessary technical and organizational measures to ensure high standards of data privacy.	1. Uses predefined policies to help prevent unwarranted data transfers to USB devices, monitor file integrity, and more. 2. Uses automated threat response mechanisms to shut down infected systems, disconnect rogue user sessions, and more.
Article 25(2) Practice data minimization and ensure that personal data is not accessible by an indefinite number of individuals.	Locate and roll back excessive privileges and permissions given to users.	1. Find users with full control access to your Windows shares. 2. Locate all the files and folders that have been shared with everyone.
Article 30(1) 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.	Figure out which data is sensitive, who can access it, and set up auditing so that you have a foolproof record of what is happening to your data. Maintain accurate details on the measures taken to ensure data security.	1. Locates instances of personal/sensitive personal data stored across Windows file servers and failover clusters utilizing a dedicated GDPR data discovery policy. 2. Scans for national identification numbers, credit card details, license number, and more. 3. Finds who has what permission over files containing sensitive personal data. 4. Audits user activity in files with details on who accessed what, when, and from where.

Article 32(2) 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.	Implement preventive and detective measures to protect the data being processed from a security incident.	**To address the risk of potential data leaks:** 1. Monitors the use of removable storage devices such as USBs in your organization. 2. Blocks the movement of files containing personal data to USB devices, or via email as attachments. 3. Provides contextual warnings using system prompts about the risk of moving business-critical data to removable storage devices, or via email as attachments. 4. Reduces incident response times with instant alerts, and an automated threat response mechanism. **To address the risk of unauthorized accesses or disclosure:** 1. Alerts and reports on unwarranted accesses, or sudden spikes in file accesses and modifications, including permission changes, deletions, and more. 2. Spots files with security vulnerabilities such as: * Files owned by stale users. * Critical files that allow full control access to users. * Overexposed files, or files accessible by everyone. 3. Tracks sudden spikes in failed attempts to access your files/folders. 4. Reviews access rights and file permissions periodically. **To address the risk of accidental or unlawful destruction:** 1. Maintains a complete record of all file and folder deletions, along with details on who deleted what, when, and where. 2. Uncovers and quarantines possible ransomware infections.

Article 33(3) 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.	Analyze and investigate the potential causes and consequences of a 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.
Article 35(7)(d) A data protection impact assessment should include measures envisaged to address risks including safeguards and safety measures to ensure the protection of personal data.	Identify and assess risks to your sensitive personal data. Evaluate the risk and implement measures to mitigate the risk.	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. 2. Identify files that are vulnerable due to permission hygiene issues.

Disclaimer: Fully complying with the GDPR requires a variety of solutions, processes, people, and technologies. This page is provided for informational purpose only and should not be considered as legal advice for GDPR compliance. ManageEngine makes no warranties, express, implied, or statutory, as to the information in this material.

DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It analyzes file storage and security permissions, deletes junk files, and detects security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI). It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage. Together, these capabilities ensure the all-round protection of data at rest, data in use, and data in motion.

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

Download free trial $ Get a quote

Explore DataSecurity Plus' capabilities

File server auditing

Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

Learn more

File analysis

Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

Learn more

Data risk assessment

Discover and classify files containing sensitive data such as PII, PCI, and ePHI by combining content inspection and contextual analysis.

Learn more

Data leak prevention

Detect and disrupt data leaks via USBs, email, web applications, and printers; monitor endpoint file activity; and more.

Learn more

Cloud protection

Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

Learn more