ManageEngine

How IT security solutions can help meet the

GDPR's Requirements with Ease

- A solution book for IT security admins

www.manageengine.com

ManageEngine

Table of Contents

The GDPR and its role in resolving security issues

With the advent of more sophisticated data breaches targeting enterprises, a stringent regulatory mandate was inevitable. The EU's General Data Protection Regulation (GDPR) serves this purpose rightfully. The GDPR aims to unify and standardize personal data collection and processing methods across the EU. The GDPR extends its territorial scope. This regulation is applicable to all the enterprises that collect and process EU citizen's personal data, irrespective of its location. Organizations are liable to comply with the GDPR before May 25, 2018, even if the data processing is happening outside the Union.

What makes the GDPR special?

Apart from the hefty compliance violation penalties, the GDPR' rules on data collection and processing make it one of the most stringent regulatory mandates. With the advent of zero-day attacks, advanced persistent threats (APT), and other sophisticated attacks, the GDPR insists that organizations that handle personal data adopt proper technical measures and risk assessment techniques to protect their data. However, the EU's regulatory bodies have also realized that protecting data from breaches is not always possible. Despite adopting and deploying proper security measures, there's still a high chance of security attacks happening in network premises. Therefore organizations must be instructed on what to do and what not to do in the event of a data breach.

In this solution book

This solution book elaborates on the GDPR's requirements concerning the security measures that organizations should adopt while handling personal data. It also illustrates how solutions from ManageEngine can help organizations fulfill these requirements with ease.

Meeting the GDPR's requirements with ManageEngine's solutions

Log360 and FileAudit Plus, two IT security solutions from ManageEngine, help organizations seamlessly meet the requirements that are concerned with keeping personal data safe and auditing data processing methods

Log360 is a comprehensive SIEM solution that collects, processes, and analyzes log data from sources across a network. It audits critical changes to Active Directory in real time and notifies administrators instantly about anomalous security incidents, data breach attempts, or security attacks. Log360 is an integration of two of ManageEngine's powerful auditing tools, EventLog Analyzer and ADAudit Plus. While EventLog Analyzer resolves any log management woes and helps detect and fight external security attacks, ADAudit Plus audits Active Directory extensively to monitor user activities and thereby prevent internal threats.

FileAudit Plus, a real-time and in-depth Windows file monitoring and auditing solution, ensures the integrity of confidential files and folders by generating instant notifications whenever critical file changes—such as creation, deletion, modification, renaming, and permission changes—happen.

Apart from these solutions, ManageEngine also has the below solutions that can help enterprises meet the auditing and monitoring requirements specific to the technology and platforms they use.

ADManager Plus, a web-based Active Directory management and reporting solution that helps checking the permissions assigned to users to access the personal data

Exchange Reporter Plus, a comprehensive Exchange server reporting, auditing, and management solution that helps to keep an eye on the personal data transmission over emails.

O365 Manager Plus, an extensive Office 365 auditing and reporting tool that helps ensuring all activities happening in the Office 365 are in accordance with the requirements of the regulation.

Sneak peek!

ManageEngine's tools help organizations comply with multiple GDPR articles, including:

- Chapter 2
  - Article 5 - 1(b), 1(d), and 1(f), and 2
- Chapter 4
  - Article 24 - 1
  - Article 25 - 2
  - Article 32 - 1(b), 1(d), 2, and 4
  - Article 33 - 1, 2, and 3(a)

Adopting technical measures for the GDPR compliance

The GDPR insists enterprises take "technical measures to ensure data safety." Why is the GDPR's wording is generic here? Because enterprises don't all have the same network architecture.

Depending on the business, every organization's network is unique. Some may be a Windows shop using Microsoft Active Directory to manage their computer resources and user accounts, while others may be non-Windows shops as well. Some enterprises may use Exchange servers to manage their mailboxes, whereas others might host them in the cloud.

Organizational networks can never be generalized. That's why the GDPR states that irrespective of the technology they adopt or systems they use, enterprises should adopt proper technical measures to ensure personal data safety. Which leaves one option for every enterprise: monitoring and auditing the systems and processes that store or interact with personal data. But don't worry! We've got you covered.

ManageEngine has a number of solutions that can help organizations meet the auditing and monitoring requirements specific to the technology and platforms they use.

- ADManager Plus, a comprehensive reporting and management tool for Active Directory, helps audit and manage the permissions given to users to access personal data.
- If you use Office 365, then O365 Manager Plus, our extensive Office 365 monitoring and auditing tool, can help you monitor the flow of personal data to keep it secure.
- Are you using Exchange servers to host your emails? Do you want to keep an eye on email transactions and ensure that personal data is not transferred over email? Exchange Reporter Plus, a complete analysis and reporting solution for Exchange, can help you with that.

The requirements and feature mapping

This section elaborates on the GDPR's data security requirements, the steps organizations need to take to meet those requirements, and how ManageEngine's solutions can help.

Article 5 - Principles relating to the processing of personal data

Requirement	How to comply	How ManageEngine can help
1 (b) "Personal data shall be: Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')..."	In most enterprises, personal data is collected and stored in a database or a file server. To ensure that the data is being processed only for the purpose it had been collected for, it is necessary to monitor accesses to these systems and to the personal data itself. Enterprises should watch out for anomalous personal data access, modification, and deletion, which could result in the data being processed in a way that was not originally intended. Notifications should be sent to concerned authorities for such anomalous activities.	In the case of personal data stored in databases, **Log360** help enterprises monitor critical changes with its real-time alerting console. With prepackaged alert profiles, Log360 can generate instant email or SMS notifications whenever there's anomalous activity. Further, Log360 also has bundled reports that provide information on changes to the database table, including: • Selection • Creation • Alteration • Deletion If the data is stored in any Windows file servers, **File Audit Plus** provides access audit reports on:

		• Content and location changes (created, modi- fied, overwritten, moved, restored, renamed, and deleted files/folders). • Security permission changes (changes to file/folder permissions, owner, and SACL). • Failed access attempts (file/folder read, write, or delete). FileAudit Plus' reports help detect unsanctioned data processing.
1 (d) "Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')..."	Enterprises should gather insights on their data storage. That includes implementing proper systems that provide information on how long data has been stored so it can be deleted as soon as the threshold time period for storage is reached.	**FileAudit Plus** provides information on old files with its **File Analysis** and **Storage Analysis** reports that ensure data accuracy as well as help with the erasure process stated in requirement 1 (d). Further, **Log360** helps monitor the "accuracy" of the personal data stored in databases and alert administrators in real time if the data is tampered with. FileAudit Plus' reports, mentioned above, and Log360's database auditing capability help ensure the accuracy of personal data and watch out for any unauthorized modifications to personal data stored in file servers (including EMC servers and NetApp filers) and databases (including Oracle and MS SQL).

1 (f) "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."	Deploy solutions that warn data protection officers or security administratorswhenever the integrity of personal data is compromised.	**Log360** helps confirm the integrity and confidentiality of collected and stored personal data. With prede fined alert profiles, Log360 sends out real-time alert notifications whenever the file, folder, or database table in which the personal data is stored is: Accessed in an unau thorized way (unauthor ized login failures, permission changes, database server account creation, or database schema changes). Modified. Deleted. Further, Log360 provides detailed information on who did the unauthorized change, when, and from where. This helps in submitting an incident report if necessary. **Related reports in Log360:** • File access • File modified • File deletion • Database table deleted • Modified (DDL query execution) • Unauthorized login failures • Permission changes for file or folder • Database account creation • Database schema change

Article 24 - Responsibility of the controller

If you are a controller (a person, public authority, agency, or other body who can determine the purpose and means of processing the personal data), then you must meet the following data processing requirements of the GDPR.

Requirement	How to comply	How ManageEngine can help
1. "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation. Those measures shall be reviewed and updated where necessary."	**Ensure that you:** Provide access to personal data only to those who are intended to access it. Allow only authorized users to access systems or services in which the personal data is stored. And to prove there's no unlawful or unauthorized access or mishandling of data, controllers need to perform extensive and continuous auditing. Monitor user activities and deploy solutions that demonstrate that only users with valid permissions are accessing personal data.	If you're a Windows shop, then you probably use Active Directory to grant users permissions to resources and data. **ADManager Plus** can help manage and audit the permission granting process. The following ADManager Plus reports provide insights on who can access personal data and also help identify any unauthorized access to the personal data that might disrupt its integrity: • Users in groups • Groups for users • Shares in the servers • Permissions for folders • Folders accessible by accounts • Servers accessible by accounts • Server permissions These reports also help review the process of permission granting whenever it's required.

Article 25 - Data protection by design and by default

Requirement	How to comply	How ManageEngine can help
2 "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."	Deploy solutions to validate the access permissions granted to users. Audit permission change events in order to identify illegal or unauthorized permission changes related to personal data.	Workflow in **ADManager Plus** helps with this. ADManager Plus also has notification rules which update the workflow agents on requests that have been raised, reviewed, or approved. Basically, ADManager Plus maps the type of action (request is created, reviewed, approved, or executed) to workflow agents for notification reasons. It also allows you to communicate request information to technicians and other stakeholders through email and SMS.

Article 32 - Security of processing

Requirement	How to comply	How ManageEngine can help
1(b) "The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services..."	Continuously monitor and audit the storage systems that store personal data as well as the services (or applications) that process personal data. Watch out for unauthorized access attempts and anomalies in user activities on these systems and services.	If you store personal data in databases such as MS SQL and Oracle, **Log360** can help detect any anomalies in your databases to identify: - Unauthorized access attempts to the database servers or any server wherein the personal data is stored. - Privileged user account changes on the system wherein confidential data is stored. If you store personal data in any Windows file servers, then **FileAudit Plus** can help ensure the integrity of these systems by watching out for: - Permission changes to files and folders. - File server storage and disk space to ensure availability. These reports **ensure that only authorized users access the personal data.** That way, they help maintain the integrity and availability of the systems and services in which the data is stored.

1(d) "...a process for regularly testing, assessing and evaluating the e□ectiveness of technical and organisational measures for ensuring the security of the processing."	To ensure the security of processing, enterprises should watch out for any network anomalies that could turn out to be a potential data breach. Deploy security solutions that can: 1. Audit and send out real-time alerts when any changes to critical resources such as firewalls, Active Directory, databases, and file servers are detected. 2. Centralize and correlate security data from di□erent sources to identify potential data breaches instantly andavoid data loss.	As a comprehensive SIEM solution, Log360 collects log data from all devices including firewalls, vulnerability scanners, b u s i n e s s - c r i t i c a l applications that processes personal data, file servers, databases, Linux/Unix machines, IBM AS400 systems, and more. It correlates collected data and generates real-time alerts for any potential data breach events. Security administrators can then mitigate the attack or take proper steps to prevent data loss. Log360 also provides reports and real-time alerts on: - Firewall configuration changes, which could cause a data breach. - Unauthorized access to file servers, databases, and other critical servers. - Critical changes to Active Directory, including changes to attributes, GPOs, and security groups, that can result in unauthorized access to personal data. - Permission changes to the files/folders wherein the personal data is stored. - Anomalous user activities including user logon/logo□ activities during non-business hours, logon failures, and more.

2. "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."	Deploy solutions and audit changes to personal data (e.g. modification, deletion, renaming, or even permission changes). Keep an eye on mailboxes to detect when personal data is transmitted via email.	If you store personal data in a Windows file server, use **FileAudit Plus** to generate detailed reports and **real-time alerts** on: - File access/change events. - Content and location changes (modified, overwritten, moved, restored, renamed, and deleted files/folders). - Security permission changes (changes to ile/folder permissions, owner, and SACL). - Failed file/folder process or access attempts (file/folder read, write, or delete). **For personal data stored in a database** Enterprises using MS SQL or Oracle databases to store personal data need to audit any changes or access to those databases. With Log360, get exhaustive predefined reports for database change auditing—who did what change, when, and from where. Quickly generate incident reports from predefined change report templates. Get real-time alerts for any unauthorized or unlawful activities such as: • Database table deleted • Database table modified (DDL query execution) • Unauthorized login failures • Permission changes for files or folders • Database account creation • Database schema changes

Further, enterprises that use other file servers such as NetApp filers, EMC cluster, and file server cluster, can also get information on critical file and folder changes (including changes to folder permissions) from Log360.

Log360's reports and real-time alerts help organizations detect unauthorized access and disclosure, as well as data loss.

Auditing data transmission via email

Enterprises using Exchange servers for mail communication can use Exchange Reporter Plus to detect and report on unauthorized or unlawful transmission of personal data. Identify personal data sent via email using the Attachment by Filename Keyword report and the Attachment by File Extension Keyword report.

View permission changes using the Mailbox Permission Changes report.

Use the Mails Deleted or Moved report to identify any breach of your data protection policies. This report shows details such as the subject of the message.

4 "The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law."	Deploy solutions that help detect when users access personal data without proper permissions.	Use ADManager Plus to keep track of permission records. Review the permission given to users using reports that provide information on: • Users in groups • Groups for users • Shares in the servers • Permissions for folders • Folders accessible by accounts • Servers accessible by accounts • Server permissions Generate alerts if any person who does not have explicit permission attempts to access the data.

Article 33 - Notification of data breach

1. "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

2. "The processor shall notify the controller without undue delay after becoming aware of a personal data breach."

3. "Controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

ManageEngine's SIEM solution, Log360, can help organizations meet all the above requirements. With a built-in real-time alerting console and correlation engine, Log360 detects any data breach in the network instantly.

With predefined alert profiles and correlation rules, Log360 can detect and contain known attack patterns such as:

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS)** attacks that bring down the system or services that contain personal data.
- **SQL injection** attacks that can alter, expose, or delete personal data stored in SQL databases.
- **Ransomware attacks** that can expose or transmit personal data without proper permissions.

In addition, Log360 also comes with an intuitive **custom correlation rule builder and alert profile creator** that can create new correlation rules and alert profiles for detecting unknown attack patterns, keeping personal data safe.

Incident report extraction with Log360

As per the requirement outlined in Article 33 #5, the controller is liable to document the data breach providing information on the impact of the breach and the remedial action taken.

Log360 caters to this need with its powerful **log search engine** that helps perform forensic analysis. Log360 comes with various search options, including boolean, range, group, and wildcard searches, that help enterprises narrow down the root cause of a breach with ease. Forensic analysis provides information on:

- When the breach occurred.
- Systems that were affected by the data breach.
- Data that was tampered, deleted, exposed, or transmitted.
- Who was responsible for the breach.

Further, all this forensic information can be exported as reports, helping organizations construct an incident report to be submitted to the ICO in case of a breach.

Brace yourself for the implementation of the GDPR with ManageEngine's IT security solutions Audit your network, detect breaches, and prove that you're on track with the regulation's requirements. For more information on deploying any of the solutions mentioned in this guide, please feel free to write to us at itsecurity-solutions@manageengine.com

ManageEngine

ManageEngine's IT Security Solutions for GDPR Compliance

Log360

An integrated SIEM solution that combines ADAudit Plus and EventLog Analyzer, our two most powerful auditing tools, to resolve all log management and network security challenges. Thwart internal security attacks, defend your network from external attacks, protect confidential information, and meet the demanding growth of compliance.

Get 30-day free trial | Know more

FileAudit Plus

A real-time file integrity monitoring, auditing, and reporting solution for Windows servers. Get alerted about every critical change made to confidential files and folders. Generate detailed analysis reports on file storage and access attempts to ensure protection of sensitive data from attacks.

Get 30-day free trial | Know more

ADManager Plus

A simple yet efficient solution to manage and report on your Windows Active Directory environment. Ensure that only specific users get access to personal data with this solution's carefully structured workflow and automation capabilities. Manage and track the permissions granted to and revoked from users and ensure that the personal data is securely processed.

Get 30-day free trial | Know more

ManageEngine

As the IT management division of Zoho Corporation, ManageEngine prioritizes flexible solutions that work for all businesses, regardless of size or budget. ManageEngine crafts comprehensive IT management software with a focus on making your job easier. Our over 90 products and free tools cover everything your IT needs, at prices you can a□ord. From network and device management to security and service desk software, we're bringing IT together for an integrated, overarching approach to optimize your IT.