ManageEngine

All you need to know and do to comply with the EU General Data Protection Regulation

Table of contents

Introduction

Increases in the number, scale, and cost of data breaches have made governments across the globe enact stringent compliance laws to protect citizens' personal data. Europe is no exception. Since 2012, the European Commission has been framing new data protections that can improve data processing methods, enhance data security, and also bring harmonization in protecting sensitive data across all European nations.

With a lot of changes being made to the existing data protection rules, the new General Data Protection Regulation (GDPR) is attracting more attention. The EU GDPR framework is complex to implement, with new accountability policies, breach notification procedures, and strict rules for international data flows. With just a few months left to comply with this new regulation, it's high time for organizations to revisit their security strategies.

This guide highlights the key changes, challenges, and action plans organizations should take to ensure compliance with the GDPR.

Changes, requirements, and action plans

GDPR is borderless

The GDPR is a global data protection law that extends beyond companies that operate only in the EU. Any organization that targets consumers in the EU, processes the personal data of EU citizens, or monitors the behavior of EU data subjects must comply with the requirements of GDPR.

Requirements:

- It's time to revisit the security frameworks and policies of companies. Organizations that are not operating within the EU but are dealing with EU data will need to take the steps to comply with the new GDPR.
- Organizations that are operating in the EU and are complying with the existing EU data protection law should also revisit their security framework to ensure they meet the stringent requirements of the new GDPR.

The action plans

- If your organization supplies goods or services or monitors the behavior of EU-based citizens, you need to comply with the requirements of GDPR on or before 25th May 2018.
- Revisit your security policies and ensure that you take the proper steps as outlined below when handling personal data.
- Draft proper privacy notes and other documents that can be used to get explicit and clear consent from individuals to process their personal data. If you already have such documents, consider revising and reviewing them in accordance with the new regulation.
- Monitor the technical and organizational measures taken to ensure the privacy and security of personal data collected.
- If necessary, appoint officials who can monitor the data processes and who are accountable for the security of personal and sensitive data.

Broadened personal data scope

The new regulation widens the definition of personal data and sensitive personal data.

According to the GDPR, personal data is "any information relating to an identified and an identifiable natural person.". It also includes "online identifiers" such as IP addresses and cookie identifiers.

Apart from defining personal data, the GDPR categorizes some of the personal data as sensitive personal data. According to the GDPR, sensitive personal data is "any data relating to the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life and genetic and biometric data."

The new requirements also impose that organizations get valid consent from the "data subjects" before processing their personal data.

Challenges:

- This broad definition of personal data and the inclusion of the "online identifier" forces organizations dealing with data analytics, behavioral analysis, advertising, and social media to comply with the GDPR.

The action plans

- Define the scope of the data your organization deals with.
- If the data fits into the GDPR's definition of "personal data," then prepare a privacy note or document that requests explicit and clear consent from individuals for further data processing.
- If you're already seeking consent to process the data, consider revising and reviewing it in accordance with the new compliance requirements.

Data protection principles redefined

The data protection principle that forms the backbone of the GDPR requirements remains the same as stated in the Data Protection Act, the earlier compliance regulation, with a few more elements added to its basket.

The six data protection principles outline that personal data and sensitive personal data must be,

- Processed fairly, lawfully, and in a transparent manner.
- Collected for specified, explicit, and legitimate purposes and shouldn't be processed in a manner that is incompatible with the above-stated purposes. Further archiving of the data for public interests or scientific, historical, or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purpose for which it's processed.
- Accurate and up to date. Steps have to be taken to erase or rectify personal data that is inaccurate.
- Maintained in a form that permits identification of data subjects for no longer than is necessary for the purposes for which it is processed. It can be archived for a longer period only if the archival supports public interests or scientific, historical, or statistical purposes. Further, organizations have to take technical measures in order to safeguard the rights and freedom of the individuals.
- Processed with proper technical and organization measures that ensure appropriate security including protection against unlawful process, accidental loss, destruction, or damage.

The new GDPR outlines strict accountability requirements that make data controllers a) responsible for ensuring data protection principles are in place and b) demonstrate that the organization complies with the GDPR.

Requirements:

- Apart from meeting the data protection principles as such, companies should clearly define their role in data processing (viz., controllers or processors) and embrace their responsibilities in accordance with the new regulation.
- Organizations should revise their data audit flow to meet the new accountability requirements of the GDPR.

- A new, risk-based approach should be adopted by companies if they are processing personal data of high-risk. Data controllers must carry out data protection impact assessments (DPIAs) to ascertain the risk associated with the personal data even before it's processed. The DPIA also allows identification and mitigation of data breaches at an early stage so as to reduce the cost damage which might occur.
- When a project dealing with personal data is being initiated, organizations should embrace a privacy-by-design approach to reduce the risk of data breaches.

The action plans

- Document all information related to data processing, including:
    - What kind of personal data is being collected.
    - How it's collected, used, transmitted, and stored.
    - How it's protected from disclosure at each step.
- Apart from documenting information including where the data is being stored and who owns the data, companies should constantly monitor activities such as:
    - Who accesses personal data.
    - With whom the data is being shared.
- Continuously monitor the file or folder where the data is stored, so as to instantly identify and report any unauthorized or illegal access attempts.
- Maintain a record of how long the data is to be stored. And while being stored, ensure the data is encrypted and tamperproof.

Responsibility and accountability

Every organization that is processing personal or sensitive data acts either as a controller or as a processor. To ensure accountability, the GDPR strikes the right balance between the roles of controllers and processors, making them equally responsible for being compliant.

Data controllers

- According to the GDPR, "Controllers are any entity that, alone or jointly with others, determine how and why personal data are processed."
- Controllers are responsible for:
    - Reviewing all data processing activities.
    - Maintaining relevant documentation of all data processing activities.
    - Conducting data protection risk assessments for high risk processes.
    - Implementing the data protection by design and by default.
    - Appointing data processors and defining instructions on how to process the data.
    - Notifying authorities in case of any data breach.

Data processors

- According to the GDPR, a data processors is "any person (other than the employee of data controller) who processes the data on behalf of the data controller."

  Data processors do the following:
    - Process data only upon documented instruction from the controller.
    - Employ security and organizational measures to avoid data breaches.
    - Delete all personal data at the end of processing and upon instruction from the controller.
    - Maintain a written record of processing activities carried out on behalf of the controllers.
    - Designate a Data Protection Officer (DPO) where required.
    - Notify controllers immediately upon data breach.
    - Provide all information to controllers that are necessary to demonstrate compliance and allow audits to be conducted by the controller.

Requirements:

- Businesses should carefully revise and review their existing data processing contracts to meet the changed accountability requirements. Any new contracts should adhere to the new GDPR requirements.
- Both processors and controllers should revisit their security, auditing, and data breach policies to meet the new requirements of GDPR.
- Organizations have to retain records of actions taken to prevent data breaches.

The action plans

- Maintain a clear record of data flow inside the organization—how the data is being collected, accessed, shared, and who the owner is.
- Frame security policies that could avoid data breaches. This includes:
    - Monitoring the organization's network to detect any anomalies.
    - Tracking user behaviors, especially privileged users who have access to process the personal data.
    - Auditing the file and folder in which the personal data is being stored. Get instant information whenever there is any inappropriate or unauthorized access attempts to the personal data.
    - Ensure proper organizational and technical measures to safeguard the company's network from attacks and threats.

Data breach notification

The GDPR defines a personal data breach as "a breach of security leading to destruction, loss, alteration, unauthorized disclosure of, or access to, personal data."

This explains that a data breach is more than just the loss of data. The regulation also forces organizations to report data breaches "without undue delay, and where feasible," within 72 hours.

Requirements:

- Enterprises should have a proper internal breach reporting procedure.
- Organizations must conduct supply chain reviews and regular audits to ensure that they meet the new security requirements.
- Companies should deploy a proper technical and security system that facilitates instant data breach detection. The system should also provide in-depth information to speed-up the response or contain the breach at an early stage.

The action plans

- Identify the indicators of compromises (IOC) that cause security breaches in the network and prepare security policies to defend them.
- Deploy security systems such as firewalls and IDS/IPS that could help prevent security attacks.
- Consider implementing security solutions for organizations that can instantly detect, alert, and report on security breaches. Also, the solutions should be able to alert in real time whenever any mishaps or breach attempts occur.
- Enact security policies that help ensure data integrity by identifying unauthorized:
    - Access or access attempts
    - Deletion
    - Sharing
    - Copying or attempts to copy personal data
- Monitor the behavior of privileged users (i.e., users who have access to personal data) to identify abnormal activities in case of identity theft, and report them immediately.

The rights of data subjects

Any action you can perform with data is deemed data processing. However, the GDPR defines strict boundaries on what organizations can do and can not do with the personal information that they collect.

Right to be informed: It starts from the point of data collection. Organizations must let the data subjects know that the information collected from them will be processed in a transparent and fair manner, through a privacy note. Also, it's a must for enterprises to get clear and valid consent from the data subjects for processing their personal information through a consent document laid out in simple terms.

Right to access: Data subjects or individuals should be given the right to access their personal information at any point in time. By this requirement, the GDPR ensures that the individuals have the right to check and validate their information is being processed fairly.

Right to rectification: If individuals feel their personal data is incomplete or inaccurate, they have the right to ask the enterprise to rectify their personal data. When a rectification request has been raised, it's the responsibility of the controller to provide information on actions taken on the request without undue delay to the concerned individuals.

Right to restrict data processing: When data processing is restricted, the controller can just store the personal data and cannot perform any kind of process over the data. Individuals can restrict their data processing if:

- The data is found to be inaccurate or incomplete.
- The data is being processed unlawfully.
- The controller no longer has any reason (in accordance with the data protection principles) to process the personal data.

Right to data portability: Individuals, at any point in time, without any hindrance, can obtain their data and transfer it to another controller for processing. This right allows individuals to move, copy, or transfer personal data easily from one environment to another in a secure way.

Right to be forgotten: The GDPR grants full rights to individuals to request deletion or removal of their personal data. The request for data erasure can be raised under these circumstances:

- Where storage of personal data is no longer necessary in relation to the purpose for which it was originally collected or processed.
- When the individual withdraws consent for data processing.
- When the data subject raises a request to stop data processing due to the unlawful processing of data or if there was a breach of data.
- If the data has to be erased in order to comply with a legal obligation.

The action plans

- Draft a proper consent-seeking form or privacy note which can obtain clear and explicit consent from individuals for processing personal data.
- Document data processing techniques and flows so you can provide individuals with them when they seek them through their right to access.
- Take technical measures to erase personal data automatically after its purpose has been fulfilled.
- While the data is being stored, ensure that it's integrity is preserved by encrypting the data.
- Document the encryption information to provide it to the data subjects, if necessary.

Compliance violation penalties

When organizations are not compliant with the GDPR or violate the GDPR requirements, the administrators can impose a penalty up to ***€10 million or 2% of the company's total worldwide annual turnover of the preceding financial year,*** whichever is higher. Controllers and data processors are liable for this huge fine when the below conditions are violated:

- Core data protection principles
- Non-personal data processing conditions
- Conditions for consent
- Sensitive personal data processing conditions
- Data subjects' rights

The data protection commissioner who imposes the fine takes into consideration the nature and intensity of violation, mitigation measures taken, technical and organizational measures implemented, and more to decide the penalty amount.

Meeting GDPR compliance requirements with ManageEngine's IT security solutions

ManageEngine's IT security solution portfolio has a wide range of tools that help organizations to comply with the GDPR. We have in our suite,

- **Log360,** a comprehensive SIEM tool that helps enterprises to detect data breaches, ensure security of the stored personal data, and tracks access to personal data thus confirming with the accountability requirements.

- **File Audit Plus,** a real-time file auditing and monitoring tool that helps to track any critical changes to the file and folder in which personal data is stored.

How our solutions help meeting the GDPR requirements

- **The technical and organizational measure to defend or mitigate security breaches:** Deploying Log360 and File Audit Plus can be the technical measure that organizations adopt to defend or mitigate security breaches. These solutions have the capability to monitor the activities of all devices and users in your network, and they report anomalies to the administrators instantly. The security professional can then probe the incident with the exhaustive reports, and if the incident is found to be a security breach (or breach attempt), they can take immediate steps to contain it at the early stage.

- **Data auditing:** File Audit Plus' real-time file integrity monitoring feature continuously monitors changes to critical data. It also provides exhaustive information on who accessed the data, when it was accessed, and from where. This detailed report helps provide information to data subjects on data accesses and also monitors data flows.

- **Conducting audit trails:** Log360's powerful log search capability helps conduct forensic analysis at ease. It's one of the requirements of GDPR to find out the root cause of the data breach or breach attempt so as to fix it instantly. Our solution can help find the root cause of a data breach by searching terabytes of log data within minutes. The solution also provides an option to export the search results as a forensic report so that it can be submitted to the DPOs. Also, the search query can be converted into an alert profile to mitigate future security attacks of the same kind.

- **Meeting the PIA/DPIA requirement:** Log360's exhaustive reports and alert profiles detect any network anomalies and security breach attempts instantly. This helps contain the data breach at an early stage and also minimize the data damage and cost that would incur otherwise, thus meeting PIA/DPIA requirement of the GDPR.

- **Breach notification requirement:** Log360 sends out real-time email or SMS alerts about data breaches to administrators. This helps them report the breach to higher officials without any undue delay. This solution comes bundled with over 600 predefined alert profiles that are based on various IOCs. This helps in detecting the breach attempts instantly without much effort. Further, the solution also provides an option to create custom alert profiles to meet internal security needs.

ManageEngine's IT Security Solutions for GDPR Compliance

Log360

An integrated SIEM solution that combines ADAudit Plus and EventLog Analyzer, the 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

An integrated SIEM solution that combines ADAudit Plus and EventLog Analyzer, the 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

ManageEngine

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-time services and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.

About the author

Subhalakshmi Ganapathy currently works as a Senior Product Marketing Analyst for IT Security Solutions at ManageEngine. She has in-depth knowledge in information security and compliance management. She provides strategic guidance for enterprises on Security Information and Event Management (SIEM), network security, and data privacy.

Reach out to Subha at **subhalakshmi.g@manageengine.com**.

Dial Toll Free:

US : +1 888 720 9500 UK : 0800 028 6590 AUS : +1 800 631 268

CN : +86 400 660 8680 Intl : +1 925 924 9500

Or

Visit www.manageengine.com/log-management
to learn more about **Log360**.

Visit www.fileauditplus.com
to learn more about **File Audit Plus**.