ManageEngine
EventLog Analyzer

GDPR

compliance guide

www.eventloganalyzer.com

Index

What is GDPR?

The General Data Protection Regulation (GDPR), approved by the European Union (EU) Parliament in April 2016 and effective since May 2018, is a transformative regulation aiming to protect the personal data of EU citizens. Its intent is twofold:

1. Harmonize data privacy laws across EU member states.
2. Strengthen individuals' rights with respect to their personal data.

This unified regulation, superseding the Data Protection Directive 95/46/EC, mandates stringent rules on how organizations collect, store, and process personal data. Personal data, under GDPR, must be safeguarded against damage, destruction, unlawful processing, or accidental loss. GDPR's core principle, "Data protection by design," implies that data privacy should be at the forefront of an organization's operations, rather than an afterthought.

Understanding GDPR compliance requires familiarization with the following key definitions:

- **Personal data**: Any information relating to an identified or identifiable natural person (a "data subject").

- **Data controller:** A natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- **Data processor:** A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

- **Data protection officer (DPO):** An appointed individual responsible for ensuring compliance with data protection laws, monitoring processes, and collaborating with supervisory authorities to protect personal data.

- **Recitals:** Numbered from 1 to 173, these outline the objectives and principles behind the regulation, explain the reasons for specific provisions, and provide clarifications on various concepts and terminology.

Who must comply with GDPR?

GDPR compliance has a vast scope, affecting organizations that hold data on EU citizens, irrespective of where the organization or the data resides. It has a broad interpretation of what is classified as personal data which includes names, photos, email addresses, bank details, social media posts, medical information, IP addresses, and more.

The following parties must adhere to GDPR guidelines:

- **Organizations within the EU:** Any organization, regardless of size or type, operating within the EU must comply with GDPR.

- **Organizations outside the EU:** If an organization is not based in the EU but deals with the personal data of EU residents, it is subject to GDPR. This could apply when goods or services are offered to EU residents or while monitoring their user behavior.

- **Large and small businesses:** If the organization employs over 250 personnel, or if the organization employs fewer than 250 but their data processing activities can impact the rights and freedoms of EU data subjects.

This broad spectrum means almost all organizations must comply. Essentially, even if an organization does not have a physical presence in the EU, it can still fall under the scope of the GDPR if it allows EU residents to access its website or contact details. Blocking access from EU IP addresses or rejecting emails from EU servers is the only way for an organization to establish that they do not fall under the scope of GDPR.

Consequences of GDPR non-compliance

The GDPR governs all EU nations, but its implementation lies with each respective member state. Typically, organizations breaching GDPR compliance are penalized by the country of their establishment, or in the case of non-EU firms, the nation where their EU delegate resides. The European Data Protection Board (EDPB) aids these states in enforcing GDPR, guaranteeing the consistent application of data privacy norms throughout the EU.

Understanding the consequences of non-compliance with the GDPR is crucial for organizations of all sizes and sectors. Non-compliance can result in severe financial penalties, loss of reputation, and potential business disruption.

The GDPR imposes a two-tiered structure for fines that can be levied on organizations for non-compliance:

- **Lower tier fines:** Non-compliance may warrant a fine of up to €10 million or 2% of the company's global annual revenue, whichever is higher. These are typically applied to organizations that fail to establish proper data protection policies, do not cooperate with data regulators, have not appointed data protection officers, or do not promptly inform data subjects when their data has been compromised.

- **Higher tier fines:** Harsher violations may be penalized with a fine of up to €20 million or 4% of the company's global annual revenue, whichever is higher. These are given to companies that commit serious violations, such as breaching the data and privacy rights of EU data subjects, not following the principles of data protection, or ignoring demands and requests of data regulators.

However, these fines are discretionary and take into account multiple factors including but not limited to:

- **Gravity and nature:** This involves the scale of the violation, including the number of data subjects harmed, the extent of their harm, and the duration of the violation.

- **Intention:** To determine whether the violation was intentional or accidental.

- **History:** Past infringements, adherence with prior corrective recommendations, and violations of data protection laws outside the EU.

- **Data category:** Pertains to the types of personal and sensitive data involved.

- **Aggravating and mitigating factors:** Financial gains earned or losses saved due to the violation, among other factors.

- **Notification:** Timeliness and sufficiency of breach notification to the supervisory authority and affected data subjects.

In conclusion, non-compliance with GDPR carries significant consequences, potentially damaging a firm's reputation and financial status. Therefore, it is important to understand the requirements of GDPR and ensure compliance.

GDPR requirements for compliance

Organizations in the digital landscape must understand and comply with GDPR requirements to maintain security and compliance. Each chapter of the GDPR has specific requirements that organizations need to follow.

Chapter 1 (Articles 1–4)

General provisions

This chapter sets the groundwork for the GDPR, defining its objectives and applicability. It presents the scope of the GDPR within and beyond the EU, outlines the rules for processing personal data, and explains certain exemptions. It provides definitions for terms like "personal data," "processing," "controller," "processor," and "consent," establishing a language to further discussions on data protection.

Chapter 2 (Art. 5–11)

Principles

This chapter of the GDPR elaborates on principles for processing personal data. It discusses lawful bases for processing, rules for obtaining consent, and conditions for children's consent in relation to information society services. It also addresses the processing of sensitive and criminal data, as well as situations where identification isn't necessary.

Chapter 3 (Art. 12–23)

Rights of the data subject

This chapter of the GDPR clarifies the fundamental rights of data subjects, including rights to access, rectification, erasure, processing restriction, data portability, objection to processing, and rejection of automated decisions. All of which are crucial for both organizations and users.

Chapter 4 (Art. 24–43)

Controller and processor

This chapter sets forth the responsibilities of data controllers and processors. It emphasizes maintaining data protection, designates the role of the DPO, establishes the protocol for data breaches, discusses the importance of impact assessments, and advocates for the establishment of codes of conduct and certifications.

Chapter 5 (Art. 44–50)

Transfers of personal data to third countries or international organizations

This chapter governs the transfer of personal data to third countries (a non-EU country or territory where its citizens do not have the right to freely move within the European Union, as stated in the Schengen Borders Code) or international organizations. It mandates pre-transfer approval, ensures adequate data protection laws are in place, prescribes methods for handling international data-related legal disputes, setting of strict data handling rules for non-EU entities, and cooperation with nations outside the EU.

Chapter 6 (Art. 51–59)

Independent supervisory authorities

This chapter details the structure and functions of independent supervisory authorities. It includes provisions on their establishment, independence, member qualifications, and professional secrecy. It also demarcates their competence, tasks like enforcing the GDPR and processing complaints, powers, and the need to provide annual activity reports.

Chapter 7 (Art. 60–76)

Cooperation and consistency

This chapter underlines the principles of cooperation and consistency among supervisory authorities for GDPR enforcement. It provides guidelines for cooperation processes, dispute resolution mechanisms, and urgency procedures. Additionally, this chapter also establishes the EDPB, its independence, responsibilities, annual reporting, procedural norms, and confidentiality rules.

Chapter 8 (Art. 77–84)

Remedies, liability, and penalties

This chapter outlines the legal remedies, liabilities, and penalties under the GDPR. This includes data subjects' rights to lodge complaints, the framework for judicial remedies, and regulations for representation. It also details the conditions for suspending proceedings, compensation eligibility, guidelines for administrative fines, and the potential for additional penalties by member states.

Chapter 9 (Art. 85–91)

Provisions relating to specific processing situations

This chapter focuses on data processing scenarios such as journalistic freedom, government document handling, national ID processing, employment data, public archives, intelligence agency protocols, and religious institution exemptions, with space for individual member state laws.

Chapter 10 (Art. 92–93)

Delegated acts and implementing acts

This chapter outlines the European Commission's rights to adopt delegated acts and form a committee to facilitate GDPR implementation, both these powers being subject to parliamentary and council oversight.

Chapter 11 (Art. 94–99)

Final provisions

This final chapter initiates the GDPR enforcement phase. It covers the repeal of Directive 95/46/EC, clarifies GDPR's relationship with other existing regulations, and the validity of prior international agreements. It also sets a four-year cycle for commission reports to keep regulations current with technological evolution.

Organizations can effectively navigate the complex landscape of data protection and privacy by adhering to the guidelines provided in each chapter. This will in turn help with establishing a robust data protection practice and building trust with customers while avoiding penalties and legal consequences.

GDPR roadmap

Understanding GDPR and DPO appointment

Understand the GDPR principles and key concepts such as lawful, fair, and transparent processing, personal data rights, and privacy by design and privacy by default. If an organization processes special categories of data, conducts regular and systematic large-scale monitoring, or processes large volumes of personal data, designating a DPO for overseeing GDPR compliance is required.

Personal data inventory

Performing an inventory to determine the personal data an organization collects, processes, and stores, the lawful basis for processing, and how this data is transferred within and outside the organization is required.

Privacy impact assessment (PIA)

Conducting a PIA to identify potential risks involved with personal data processing and devising strategies to mitigate them is a crucial action. This step entails assessing the processing impact on individuals and identifying risk-minimizing measures.

Data minimization policy and technical measures

Establishing a data minimization policy and outlining data retention periods strengthen the path to achieving GDPR compliance. Implement technical measures that consider the risk level required to safeguard personal data, including strategies to avert unauthorized access, accidental loss, or data destruction.

Consent and data subject rights

Obtaining explicit and unambiguous consent prior to processing personal data is the next step of the process, although it is important to note that consent is only one of several lawful bases for processing. Facilitating consent withdrawal at any point is equally important. Organizations can additionally implement mechanisms to comply with GDPR's individual rights, such as access, rectification, erasure, and processing restriction.

Processing operations register

Maintaining a register of processing operations for all data processing activities is essential for compliance with GDPR Article 30. This step mainly applies to organizations with over 250 employees.

Monitoring, auditing, and breach notification

The core processes for maintaining compliance with GDPR involve conducting periodic audits to identify areas of non-compliance, and implementing remedial actions.

Organizations must maintain an accessible breach register. In case of a data breach, a relevant supervisory authority has to be notified within 72 hours of becoming aware and affected individuals need to be informed where necessary. Compliance certification under GDPR (Article 42) can be obtained from a competent supervisory authority or accredited certification bodies.

GDPR best practices A checklist

By adopting these best practices, organizations can meet GDPR compliance requirements and strengthen their cybersecurity defenses.

- **Information audit for EU personal data:** Determine if the organization handles personal data belonging to EU citizens. If the data processing activities involve people from this region, the organization will fall under the GDPR.

- **Transparency and consent:** Article 12 of GDPR emphasizes the need for transparency in data processing activities. In instances where consent is sought as the legal basis for data processing, it is crucial to obtain explicit and well-informed consent from customers, ensuring clear communication about the purpose behind processing their data. The privacy policy should be updated to reflect these requirements.

- **Data protection impact assessment (DPIA):** The execution of a Data Protection Impact Assessment (DPIA) facilitates the identification of risks linked to data security and privacy. To mitigate these risks, it is recommended to implement data security practices, such as end-to-end encryption and organizational safeguards.

- **Data processing agreements (DPAs):** In order to maintain the GDPR compliance of vendors, data controllers are advised to establish DPAs with all third-party providers involved in the processing of personal data. This ensures that personal data is handled appropriately.

- **EU representative:** Non-EU organizations need to appoint a representative based in one of the EU member states.

- **Cross-border transfer laws:** If transferring personal data to non-EU countries, comply with stringent requirements stated in GDPR Article 45. The organization might need certification under the Privacy Shield Framework.

- **Compliance training:** Training employees on GDPR compliance requirements and practices is essential.

- **Data breach response plan:** Establishing a robust plan to effectively respond to potential data breaches is crucial. This plan should outline clear protocols and responsibilities for employees in the event of a data breach, ensuring quick and coordinated action to mitigate the impact and protect sensitive information. (Ref: Articles 33 and 34).

GDPR: Key subcategories to consider

GDPR Control	Code definition	Compliance recommendations
GDPR ARTICLE 5(1B)	"[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')."	• Organizations should identify and document the explicit and legitimate purpose for which personal data is collected. • Avoid processing personal data for purposes other than the original intended purpose. • If further processing is undertaken for public interest, scientific research, or statistical purposes, it must comply with Article 89(1).
GDPR ARTICLE 5(1D)	"[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')."	• Implement an efficient system to maintain the accuracy of personal data by regularly updating it. Additionally, tools or software that checks for inaccuracies in personal data is recommended. • Steps must be taken promptly to correct or erase inaccurate data.
GDPR ARTICLE 5(1F)	"[Personal data shall be] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')."	• Adopt robust technical measures to prevent unauthorized or unlawful processing, accidental loss, destruction, or damage to personal data. • Regular training should be provided to employees about data security protocols and practices. • Data encryption techniques and backup systems should be used to safeguard personal data.

GDPR ARTICLE 25(2, line 3)	"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."	• Personal data should only be made accessible after obtaining explicit consent from the individual. • Employ privacy-enhancing techniques like anonymization.
GDPR ARTICLE 32(1B)	"[T]he ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services."	• Regular audits should be conducted to check the robustness of all services and systems. • Implement a comprehensive disaster recovery and business continuity plan.
GDPR ARTICLE 32(1D)	"[A] process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing."	• Regular testing and evaluation of the technical and organizational measures for ensuring data security should be in place. • Conduct annual or bi-annual cybersecurity audits to test the effectiveness of security measures. • Continuous monitoring and reporting mechanisms should be employed to identify and rectify any gaps in security measures.
GDPR ARTICLE 32(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, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed."	• A formal risk assessment strategy should be implemented to identify and mitigate risks associated with data processing. • Adhere to security measures proportional to the risk level and the sensitivity of the personal data being processed.

The GDPR has ushered in a new era of data protection, securing the rights of individuals to control their personal information. Being more than just a set of stringent rules, it represents a shift towards a "data protection by design" approach, embedding privacy within every facet of an organization's operations. Since its enactment in 2018, GDPR has shown promising results in reducing data breaches within the EU, marking its effectiveness.

Despite this, many organizations are still on the journey towards achieving complete compliance. Whether it is an organization operating in the EU or a website handling EU visitors' data, compliance with GDPR is not only mandatory but also a trust signal to one's customers. Lastly, it is important to note that this is not a one-time process, but a continuous commitment to protect customer data.

Comply with GDPR with EventLog Analyzer

ManageEngine EventLog Analyzer enables GDPR compliance through meticulous log management, auditing, and IT compliance management. It leaves no log unturned, collecting and analyzing log data from various sources, enabling organizations to safeguard against unlawful data processing, loss, or damage.

EventLog Analyzer's security event management capabilities are significant for GDPR compliance. The tool analyzes insights from security events across networks, providing robust threat response techniques. Application log analysis features can detect data theft and track potential breaches, and server log management helps monitor servers for critical changes, enhancing data security.

Another GDPR compliance facilitator is EventLog Analyzer's file integrity monitoring feature. It tracks real-time changes to files or folders containing confidential data, ensuring data integrity, which is a core GDPR requirement. The event correlation engine and augmented threat intelligence features detect potential security threats, helping to mitigate risks to personal data.

Finally, the integrated compliance management feature simplifies GDPR auditing. Predefined GDPR report templates and log archival ensure that organizations can meet GDPR's stringent reporting and record-keeping requirements. With EventLog Analyzer, organizations can comfortably navigate the GDPR compliance landscape, protecting personal data and enhancing cybersecurity.