GDPR Security & Compliance Resource Guide

CHOICE CYBERSECURITY

Table of Contents

CHOICE CYBERSECURITY

GDPR COMPLIANCE OVERVIEW

What is GDPR?

The General Data Protection Regulation (GDPR) enables individuals to better control their personal data within the European Union (EU). The regulation focuses on the export of personal data outside of the EU. The regulation applies to any organization that collects or process data belonging to an EU citizen or resident, including those organizations located outside of the EU.

GDPR aims to provide data protection through data control, data security, the right to erasure, risk mitigation and due diligence, and breach notification However, GDPR cannot be reduced to a simple checklist. It often speaks in terms of broad standards rather than specific rules, requiring organizations to take "appropriate" measures to protect privacy. Going forward, the most important aspects of GDPR compliance to focus on through implementation and maintenance are the internal and external data flow maps along with the policy and procedures.

GDPR Founding Principles

The General Data Protection Regulation (GDPR) is founded on six primary principles for data processing of sensitive and personal data. The regulation specifies that all sensitive or personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Limited to what is necessary to meet the organization's needs
- Accurate and, where necessary, kept up to date

10065 Red Run Boulevard, Suite 120 Owings Mills, Maryland 21117
info@choicecybersecurity.com
choicecybersecurity.com
(410) 205.4980

- Kept in a form that permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal data

Who oversees it?

The Commission is the overarching authority behind GDPR and its implementation. However, each member state my appoint an independent public authority, also known as a Supervisory Authority. The Supervisory Authority is responsible for monitoring the application of the regulation throughout the many applicable organizations.

Who does it apply to?

The regulation applies to any organization operating within the European Union, including any organization outside of the EU that offers goods and services to customers or businesses within the EU. The regulation applies to organizations:

- Operating in the EU
- Located outside of the EU
    - Selling goods or services to data subjects within the EU
    - Monitoring the behavior of EU residents

What are the penalties for non-compliance?

The GDPR imposes stiff fines, administered by the individual member state advisory authorities, to data controllers and processors for non-compliance. If an organization is not in compliance, they can be fined up to 20 million Euros or 4% of global annual revenue, whichever is greater.

The monetary value of the fine for data processors and controllers are determined based on a variety of criteria such as the damage incurred, number of individuals affected, nature of the infringement, and intention. Learn more about how administrative fines here.

CHOICE CYBERSECURITY

What is considered GDPR Personal and Sensitive Data?

An organization may collect, store or transmit various forms of personal and sensitive data. Personal data is defined as any type of data that could be used to identify a person. According to GDPR, consent to obtain, store and process personal and sensitive information must be a "freely give, specific, informed and unambiguous indication of the data subject's wishes by which [they], by statement of by clear affirmative action, signifies agreement to the processing of personal data."

According to GDPR, personal and sensitive information is defined as the following:

Sensitive Information	Personal Information
Racial or Ethnic Origin	Dates of Birth
Political Opinions	Address/ Phone Numbers
Religious of Philosophical Beliefs	Passport Information
Trade Union Membership	Driver Licenses
Genetic Data	Health Insurance Card Information
Biometric Data for the Purpose of Uniquely Identifying a Person	Health Records
Data Concerning Health of a Natural Person's Sex Life/ Sexual Orientation	National Identification Numbers
Web Data Tracking: Devices, Applications, Tools & Protocols such as: IP Addresses, Cookies or RFID Tags	Bank Account Numbers
	Credit Card Numbers

10065 Red Run Boulevard, Suite 120 Owings Mills, Maryland 21117
info@choicecybersecurity.com
choicecybersecurity.com
(410) 205.4980

CHOICE CYBERSECURITY

What is Web Data Tracking?

Web Data Tracking is defined by the EU as data collected on web traffic, such as IP addresses, browser versions, registered names and email addresses, cookies or RFID tags. In order to be compliant, organizations must ensure that consent for processing or tracking sensitive web data is "freely given." This rule also applies to email tracking and monitoring including services that allow anybody subscribing to it, to know if an email sent by the subscriber:

1. Has been read by the addressee(s),
2. When it was read
3. How many times it has been read (or at least opened),
4. If it has been transferred to others and
5. To which email server, including its location.
6. Type of web navigator
7. Operating system the recipient of the email uses

Learn More about Web Data Tracking:

- Cookies and Consent
- Email Tracking
- Email Monitoring

What do you need to be GDPR Compliant?

Organizations must ensure that personal data is gathered legally and under strict conditions. Whoever collects it will be obliged to protect it from misuse or theft or face penalties for not doing so. Companies with more than 250 employees must have documentation of why peoples information is being collected, processed or stored. Additionally, they must document the technical security measures put into place. Companies with regular monitoring of sensitive and personal data must employ a Data Protection Officer (DPO). Finally, the organization must clearly explain the consent that is being provided when they are collecting data.

10065 Red Run Boulevard, Suite 120 Owings Mills, Maryland 21117
info@choicecybersecurity.com
choicecybersecurity.com
(410) 205.4980

CHOICE CYBERSECURITY

What is a Data Breach?

A breach is not just losing personal or sensitive data. It's also a breach of security that can lead to the destruction, loss, alteration and unauthorized disclosure of, or access to, personal data. A breach must be reported to an organization's supervisory authority within 72 hours of the organization being aware of it.

GDPR Roles & Responsibilities

European Union (EU) Representative

The EU Representative is a person who serve as the contact person for all questions on data protection from, both EU citizens and the data protection supervisory authority. The whole premise behind establishing the GDPR is to protect EU citizens/ customers from the misuse of their data and allow them to request that their data does not get used in any unapproved way. An EU Representative will be that person that your customers contact should they have any questions or concerns about their data. Another important aspect of GDPR is having an entity to answer to should an organization not take appropriate steps towards compliance. In addition to answering to the citizens and supervisory authority, EU Representatives maintain customer processing records (or records of customer requests & questions about their data).

Data Controller

A person or entity in charge of personal or sensitive data belonging to citizens of the European Union. The Data Controller is responsible for the security of processed and stored data within the organization. The company, as a whole, must assure GDPR compliance.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is a dedicated individual responsible for the management of the organization's data security. They are responsible for:

1. Educating the company and employees on important compliance requirements

2. Training staff involved in data processing
3. Conducting audits to ensure compliance and address potential issues proactively
4. Serving as the point of contact between the company and GDPR Supervisory Authorities
5. Monitoring performance and providing advice on the impact of data protection efforts
6. Maintaining comprehensive records of all data processing activities conducted by the company
7. Interfacing with data subjects to inform them about how their data is being used

Under the GDPR, certain private and most public-sector organizations will be required by law to appoint a data protection officer ("DPO") to oversee their data processing operations. Private-sector controllers and processors must designate a DPO if their core activities consist of:

- Processing operations which, by virtue of their nature, scope and/or purposes require regular and systematic monitoring of data subjects on a large scale; or
- Processing on a large scale of special categories of data and data relating to criminal convictions and offences.

All public authorities or bodies, except courts acting in their judicial capacity, must designate a DPO. Even if organizations are not required to appoint a DPO, doing so might be beneficial for many reasons. To name just a few, appointing an experienced and business-savvy DPO (even on a temporary basis):

- Might be the most practical and cost-efficient solution to achieve GDPR compliance - remember, even if the DPO appointment does not apply to your organization, various other GDPR requirements are very likely to apply;
- Will most likely put the organization in a better position when negotiating privacy-relevant contracts or when dealing with supervisory authorities; and
- Will streamline and optimize your privacy-relevant processes across the EU allowing your other personnel to focus on revenue-raising and other key tasks.

An organization may choose to outsource its DPO responsibilities. Outsourcing DPO responsibilities is an option, especially for small organizations. It is an alternative to

hiring a full-time position or adding to an existing employees' responsibilities. Due to the nature of the position and the duties of reporting to the Supervisory Authority, it is not advised to hand off the DPO responsibilities to a current staff member who works closely with or makes decisions on data and data protection. An outsourced DPO will have the same responsibilities of all DPOs and work under the Data Controller, If this is the case, the responsibilities remain the same and the acting DPO would be brought on as if they were an employee of the organization.

GDPR Data Rights

Consent

Consent must be voluntarily provided . The individual providing the consent must be provided a choice for doing so. The individual must be made aware that they have the ability to retract their consent. The retraction must be easy to do as the granting of the consent itself. There is an additional consent or agreement requirement from those with parental rights for those who are under the age of 16.

Right of Access

The Right of Access is an essential component of GDPR that provides all data subjects the right to access their processed personal or sensitive data upon request. There are two primary stages in requesting data:

1. The data controller must be able to verify if there is any personal or sensitive data being processed by the organization. During this stage, the only required information is a yes or no response to the requesting individual.
2. If there sensitive or personal data being processed by the organization, the data controller must disclose all information such as:
    a. Processing purposes and Data Origin
    b. Category of personal or sensitive data
    c. Recipients including Third Parties and
    d. Intended storage duration
    e. Information about the rights of those impacted
    f. Process to object to all processing

CHOICE CYBERSECURITY

Right to be Forgotten

The Right to be Forgotten, also known as the the Right to Erasure, is defined by GDPR as: The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

1) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
2) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
3) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
4) the personal data have been unlawfully processed;
5) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
6) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Right to Data Portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

1. The processing is based on consent
2. The data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. The right to data portability shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. This right shall not adversely affect the rights and freedoms of others.

Additional GDPR Resources

- https://gdpr-analysis.choicecybersecurity.com
- https://www.gdpreu.org/
- https://gdpr-info.eu/
- https://www.eugdpr.org/
- https://www.skyhighnetworks.com/cloud-security-blog/top-10-questions-to-test-your-gdpr-readiness/
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://www.dmnews.com/retail/article/13034543/cookies-and-consent-how-gdpr-impacts-online-tracking

10065 Red Run Boulevard, Suite 120 Owings Mills, Maryland 21117
info@choicecybersecurity.com
choicecybersecurity.com
(410) 205.4980