NAVIGATING THE DATA PRIVACY LABYRINTH:

A Guide to GDPR Compliance

fidelis INC

TABLE OF CONTENTS

Security and privacy: A basic necessity

Ensuring data security and privacy has become a top priority in an era where information flows freely across borders and digital footprints are ever-expanding. As companies collect and manage more sensitive information, their susceptibility to cyberattacks and data breaches also grows. To protect businesses as well as the clients whose data they handle, governing bodies have established regulations to ensure that data is adequately secured.

One of the most comprehensive and internationally recognized regulations is the European Union's General Data Protection Regulation (GDPR). The compliance initiative was created to give European citizens control over how their sensitive personal data is managed by different organizations. Since its inception in 2018, the GDPR has made great strides in setting a global standard for data security, and it has since been adopted by organizations around the world.

However, understanding and adhering to the complex requirements of the GDPR can often feel like traversing a labyrinth. To help you on your compliance journey, here's everything your business needs to know about the GDPR.

What is the GDPR?

The GDPR is a comprehensive data protection framework introduced by the European Union (EU) in May 2018. It was designed to modernize and harmonize data protection laws across EU member states, aiming to empower individuals with greater control over their personal information and ensure that organizations handle that data responsibly.

The compliance initiative applies to any organization that processes the personal data of individuals residing in the EU, regardless of the business's location. That means even if your business is based outside of the EU, you are still obligated to comply with GDPR requirements if you serve customers in the EU or process their information in any way. This can refer to a wide range of activities, including the collection, storage, transmission, and use of any type of personal data.

The GDPR evolved as a response to the increasing digitization of data and the need for stronger data protection measures. With the rise of data breaches, privacy concerns, and advances in technology, the GDPR is a guidepost to ensure that companies both inside and outside of the EU are managing personal data with a higher standard of security and privacy.

Personal data and the GDPR

Personal data is a core aspect of the GDPR. It refers to any information that identifies an individual such as their name, address, and contact details, as well as more sensitive information such as health data, racial or ethnic origin, religious beliefs, biometric data, and more. By understanding the broad scope of personal data, businesses can accurately assess their data processing activities and implement appropriate measures to safeguard their customers' personal data.

The responsibility of protecting personal data lies with two parties: controllers and processors. A **data controller** is an individual or organization that determines how and why personal data is processed. They get to determine the type of data to be collected and how it is handled. Meanwhile, a **data processor** is an entity that performs any operation on personal data (e.g., collection, structuring, storage, disclosure) on behalf of the data controller. Both entities must implement strong security protocols and approved data management principles to comply with the GDPR.

Key principles of the GDPR

The GDPR is organized around eight core data protection principles, which should be followed by data controllers and processors to ensure compliance.

1. Lawfulness and transparency

Organizations that collect and process personal data must do so lawfully by having legitimate grounds for collecting the data, and making sure that users are fully aware of the activities taking place. Ideally, companies should get written consent with clear information about data processing activities and ensure that processing aligns with the legal contracts and privacy policies they have in place. Should customers withdraw their consent, companies must be able to honor the request and remove the data from their systems.

2. Purpose limitation

Organizations should clearly define the purposes of data processing and ensure that any subsequent processing is compatible with those purposes. Data should not be processed in a manner that is incompatible with the original intent. For example, if data is collected solely for marketing purposes, it cannot be used for research or analytics.

3. Data minimization

Organizations should collect and process only the personal data that is necessary for the stated purposes. They should limit the amount of data collected, ensuring that it is relevant, adequate, and restricted to what is necessary for the intended processing activities.

4. Accuracy

Personal data should be accurate and up to date. If the personal information is inaccurate or incomplete, organizations must verify and update it. They should also have open channels where individuals can request data corrections if necessary.

5. Storage limitation

Personal data should be stored for no longer than necessary to fulfill the purposes for which it was collected. Organizations must establish retention periods and securely dispose of data once the retention period expires. It is important to regularly review and delete unnecessary data to minimize risks.

6. Integrity and confidentiality

Organizations must ensure the security, integrity, and confidentiality of personal data. This involves implementing appropriate security measures to protect against unauthorized access and data loss, including end-to-end encryption, role-based access controls, and geo-redundant data backups.

7. Accountability

Organizations are responsible for demonstrating compliance with the GDPR and being accountable for their data processing activities. This includes keeping records of processing activities, conducting data protection impact assessments when necessary, and cooperating with supervisory authorities. Organizations should also establish policies, procedures, and training programs to ensure employees understand their roles in protecting personal data.

8. Notification

Organizations must have mechanisms in place to notify individuals of any data breaches or security incidents where their personal data may have been compromised. This includes a duty to notify supervisory authorities and affected individuals within 72 hours of the breach being detected.

What are the consequences of GDPR noncompliance?

GDPR noncompliance can lead to costly penalties and a slew of other negative consequences.

Administrative fines

Supervisory authorities in each EU member state can impose administrative fines on organizations found to be in violation of the GDPR. Depending on the severity of the violation, fines can range from €10 million to €20 million (or 2–4% of the organization's global annual turnover) for serious infringements. A serious infringement may entail failure to obtain proper consent for collecting data, lax recordkeeping practices, and undisclosed data transfers.

Remedial measures and sanctions

In addition to fines, supervisory authorities have the power to impose other remedial measures and sanctions on organizations. These may include issuing warnings, reprimands, and orders to comply with GDPR requirements. Authorities can also impose temporary or definitive bans on data processing activities, effectively halting an organization's ability to handle personal data until compliance is achieved.

Data breach notifications

The GDPR mandates that organizations must notify supervisory authorities of personal data breaches without undue delay, and in certain cases, within 72 hours of becoming aware of the breach. Failing to notify the affected parties or authorities in a timely manner can result in even steeper administrative fines.

Lawsuits and compensation claims

Individuals whose rights under the GDPR have been violated have the right to seek legal recourse and may file claims for compensation against noncompliant organizations. This can result in additional legal costs, reputational damage, and potential financial liabilities for the organization.

Reputational damage

Noncompliance with the GDPR can have severe reputational repercussions for organizations. News of violations and fines can damage trust and undermine the confidence of customers, partners, and stakeholders. Negative publicity surrounding data breaches or privacy infringements can lead to a loss of customers, decreased market value, and long-term damage to an organization's reputation.

How can businesses achieve GDPR compliance?

Given the potential consequences and risks of noncompliance, organizations must take a proactive and measured approach to GDPR compliance. To achieve this, companies need to do the following:

Conduct a comprehensive data audit

The first step to compliance is to take stock of all the personal data you process and determine whether it falls under the scope of GDPR. You'll want to list the types of personal data you collect, such as names, email addresses, phone numbers, and IP addresses.

Document where this data is stored and why and how it's being used. If you collect names and email addresses, document whether this data is stored in a customer relationship management system, an email marketing platform, or another database. Log data retention periods and review procedures for deleting personal data once it's no longer needed. You should also note any third parties with whom you've shared data such as a cloud storage provider, as they could be a liability to your GDPR compliance.

Then, specify the purposes for which you use this data. Do you use them to send promotional emails, provide customer support, or analyze website traffic? Write down the legal basis for processing this data, whether it is based on consent, contractual necessity, or legal obligation. Use the lawful basis guidance tool for checking whether your data processing activities qualify for one of the legal grounds for processing. Having detailed documentation of all data processing activities will be especially helpful in demonstrating your organization's accountability and compliance with GDPR.

Be transparent with data collection and usage

It's crucial to be fully transparent with individuals about the data you're collecting and how it will be used. This involves notifying individuals at the time of data collection about the types of data you'll be collecting, why it's being collected, and who will have access to it as well as establishing clear procedures for obtaining consent.

Make sure that consent requests are clear and easy to understand. Include the details of your data processing activities in a privacy policy and make sure your contact information is prominently displayed. Individuals should also be able to withdraw their consent at any time, so make sure your service includes an easy-to-use opt-out mechanism.

Understand and respect data subject rights

Your business must be fully aware of the data subject rights under the GDPR, which include:

- **The right to be informed** – Organizations must provide clear and concise information about the data they collect.
- **The right of access** – Individuals have a right to obtain confirmation that their data is being collected and processed and access this information.
- **The right of rectification** – Individuals have the right to request that their inaccurate or incomplete data be updated.
- **The right of erasure** – Individuals can request for their personal information to be erased or deleted under certain circumstances.
- **The right to restrict processing** – Individuals can request for their data to be restricted from further use and only stored.
- **The right to data portability** – Individuals can request for their data to be delivered in a machine-readable format so they can transfer it to another service provider if necessary.

Your data management policies must uphold these rights so customers can exercise them when necessary. For example, when customers see an error in their data or wish to delete it, your organization should have the processes and tools to quickly address these requests. Tools could be as simple as a delete button within the user profile or an automated workflow that flags and processes requests for corrections or deletions.

Perform privacy impact assessments (PIAs)

PIAs evaluate the degree to which data processing activities might pose a risk to individuals' privacy. These assessments should be carried out whenever new procedures, projects, services, or systems that involve data processing are developed. Hiring an objective third party to perform the PIA can help ensure a more accurate assessment. By doing so, you can identify data risks early and develop an effective strategy for mitigating them.

Build privacy by design principles into operations

Privacy by design is an approach to data protection that puts data privacy first, rather than considering it as an afterthought. In the context of GDPR, this means that privacy settings should be configured to provide the highest level of data protection by default, without requiring users to take additional actions. Implementing privacy-friendly default settings empowers individuals to exercise control over their personal data and reduce the risks of unintended data disclosures.

Another important component of privacy by design is data and purpose minimization. These concepts involve collecting and processing only the personal data that is absolutely necessary for fulfilling a specific purpose. For example, if your organization sends marketing emails, you should only collect customers' names and email addresses, but not their home addresses or phone numbers.

Implement robust security measures and policies

GDPR compliance is all about protecting individuals' data from unauthorized access, alteration, and disclosure. This means organizations must have appropriate security measures in place to protect personal data from malicious attacks or other forms of unauthorized access. Companies generally need the following security measures to protect personal data:

- **Next-generation firewalls** – These inspect incoming and outgoing network traffic, detect malicious activity, and block unauthorized requests.
- **Anti-malware software** – This is designed to detect and remove malware that could be designed to access, steal, or alter sensitive data.
- **Role-based access controls** – These restrict access to personal data and storage systems based on user roles. Someone with access to customer data should only be able to view the information that is necessary for their job.
- **Multifactor authentication** (MFA) – With MFA, users are required to verify their identity with more than one factor (e.g., passwords, security tokens, biometrics), thereby making it more difficult for malicious actors to access business accounts and personal data.
- **End-to-end encryption** – This encodes personal data when it is transmitted between two or more devices, making data virtually unreadable by unauthorized third parties.
- **Anonymization** – This method replaces personal data with pseudonyms (or randomly generated values) so that sensitive data is not exposed.
- **Data backups** – Conducting regular backups provide an additional layer of protection for personal data in case the primary copy is destroyed or corrupted. Organizations should store backups in a secure off-site location that can be easily accessed in the event of an emergency.

Equally important is having a comprehensive set of policies in place to guide data processing activities. Such policies should cover areas like retention and disposal procedures periods, disclosure policies, data breach response and notifications, and more. By having a clear set of rules for handling data, organizations can ensure that their employees are aware of the necessary steps to follow in order to remain GDPR-compliant.

Train teams in compliant practices

It's one thing to set policies and procedures, but it's another thing to make sure your teams are aware of those protocols and understand how to use them. Organizations must provide training for their employees on data privacy and security.

Security training should cover topics such as GDPR requirements, data storage and transfer policies, acceptable usage of corporate devices and networks, and incident response procedures. At the very least, employees must practice good password habits and have a keen eye for recognizing suspicious emails, websites, and networks. These simple practices can go a long way in preventing security breaches and GDPR violations.

Clarify data processing agreements with third parties

Review and update your contracts and agreements with third-party service providers to include specific provisions on data protection and GDPR compliance. These service providers could be hosting providers, cloud storage services, marketing agencies, or any other companies with access to your EU customers' data. Make sure your contracts clearly define the roles and responsibilities of both parties in relation to GDPR compliance, including requirements for data security and the deletion of personal data when it is no longer needed.

How managed IT services providers can streamline GDPR compliance

Managed IT services providers (MSPs) offer a wide range of technologies and services that can help organizations achieve GDPR compliance. From encryption to access controls to cloud backups, they ensure personal data remains under virtual lock and key. MSPs evaluate the GDPR readiness of third-party providers, scrutinize contracts with hawk-like precision, and ensure the necessary data protection agreements are in place.

But that's not all — top-class MSPs can serve as your GDPR consultant. They can provide detailed GDPR gap analyses, pinpoint vulnerabilities in your operations, and recommend best practices to fill the gaps. They can even help you build transparent and lawful practices for collecting, processing, and storing data while training your teams in data privacy and security.

If you want to achieve GDPR compliance, we can show you the way. Contact us now to get started.

Phone: **(206) 725-7728** Email: **sales@fidelisnw.com**