Attinkom
We verify your trust

General Data Protection Regulation (GDPR)

Attinkom
We verify your trust

This publication contains general information only and Attinkom is not, by means of this publication, rendering any professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Attinkom shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, “Attinkom" means Attinkom LLC. Please see https://attinkom.com and email us at info@attinkom.com for any specific services that you may be looking for.

Attinkom
We verify your trust

Table of Contents

Attinkom
We verify your trust

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

Scope, Penalties, and Important Terms

First, if you process the personal data of EU citizens or residents, or you offer goods or services to such people, then **the GDPR applies to you even if you're not in the EU**.

Second, the **fines for violating the GDPR are very high.** There are two tiers of penalties, which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages.

The GDPR defines an array of legal terms at length. Below are some of the most important ones that we refer to in this article:

Attinkom
We verify your trust

Personal data

Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it's relatively easy to ID someone from it.

Data processing

Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing… so basically anything.

Data subject

The person whose data is processed. These are your customers or site visitors.

Data controller

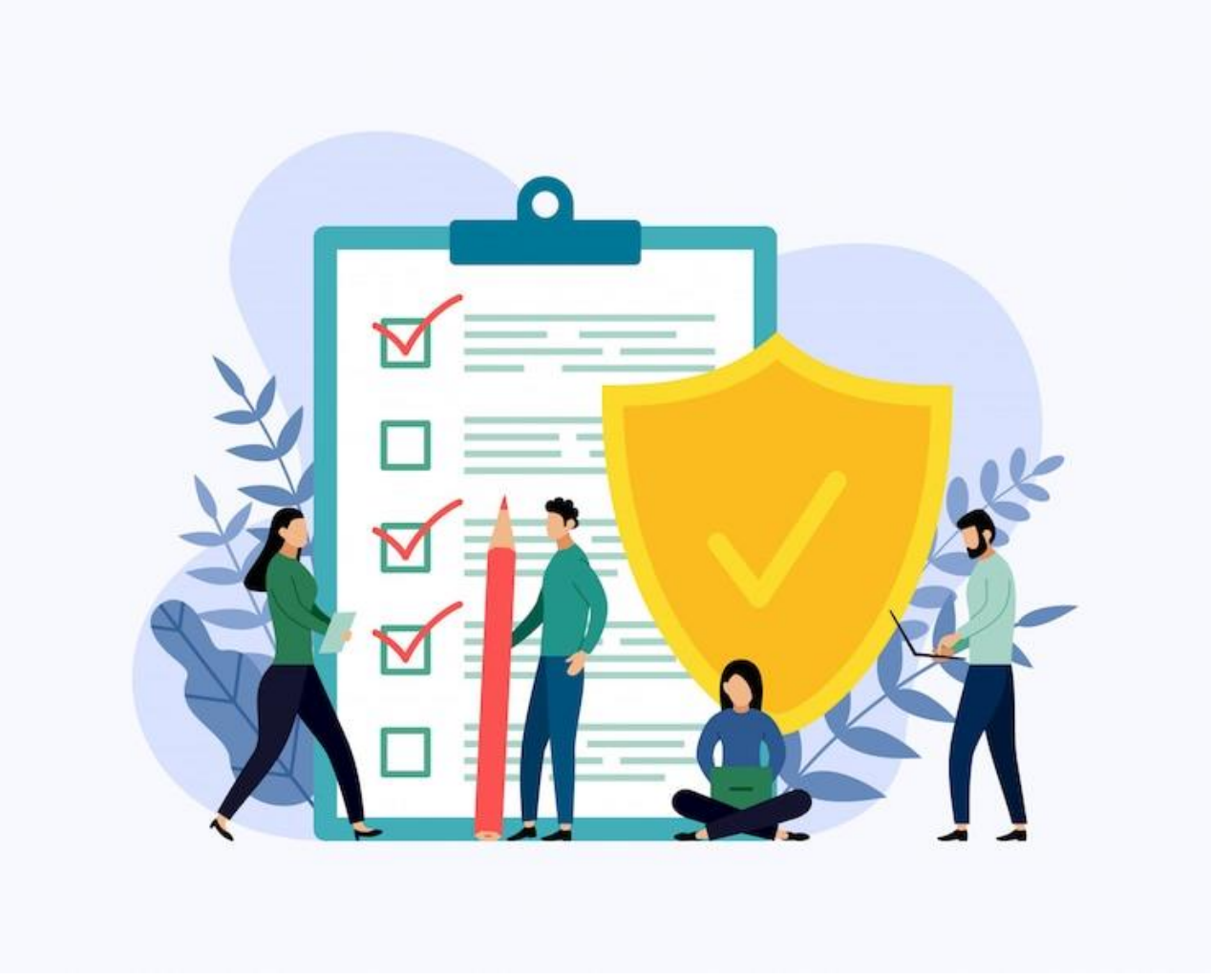
The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.

Data processor

A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations.

Types of Privacy Data Protected by GDPR

GDPR ensures the protection of personal data such as name, address, email address, photo ID of individuals, along with biometric data, racial or ethnic data, political and sexual orientation among others. Similarly, web data including IP address, profiling and analytics data, cookie data, location, and RFID tags are also protected.



People's privacy rights

You are a data controller and/or a data processor. But as a person who uses the Internet, you're also a data subject. The GDPR recognizes a litany of new privacy rights for data subjects, which aim to give individuals more control over the data they loan to organizations. As an organization, it's important to understand these rights to ensure you are GDPR compliant.

Attinkom
We verify your trust

Individuals can exercise the following rights under GDPR:

- ✓ The right to be informed – Companies must inform individuals and take their consent before gathering their personal data.
- ✓ The right of access – Individuals can request companies for access to their personal data that will be provided to them free of charge.
- ✓ The right to rectification - If individuals find their data to be incorrect or incomplete in the Company records, they get can get it updated
- ✓ The right to erasure – Individuals have the right to have their data deleted by withdrawing their consent to a Company's usage of their personal data.
- ✓ The right to restrict processing – Individuals have right to stop their data from being processed and used.
- ✓ The right to data portability - Individuals have the right to transfer their data to another service
- ✓ The right to object – This right, which ensures that data processing for direct marketing is stopped immediately upon request, must be informed by Companies to individuals at the very beginning of any communication.
- ✓ Rights in relation to automated decision making and profiling – Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Attinkom
We verify your trust

Accountability

The GDPR says data controllers have to be able to demonstrate they are GDPR compliant. And this isn't something you can do after the fact: If you think you are compliant with the GDPR but can't show how, then you're not GDPR compliant. Among the ways you can do this:

- ✓ Designate data protection responsibilities to your team.
- ✓ Maintain detailed documentation of the data you're collecting, how it's used, where it's stored, which employee is responsible for it, etc.
- ✓ Train your staff and implement technical and organizational security measures.
- ✓ Have Data Processing Agreement contracts in place with third parties you contract to process data for you.
- ✓ Appoint a Data Protection Officer (though not all organizations need one)

Attinkom
We verify your trust

Data Security

You're required to handle data securely by implementing "appropriate technical and organizational measures."

Technical measures mean anything from requiring your employees to use two-factor authentication on accounts where personal data are stored to contracting with cloud providers that use end-to-end encryption.

Organizational measures are things like staff trainings, adding a data privacy policy to your employee handbook, or limiting access to personal data to only those employees in your organization who need it.

If you have a data breach, you have 72 hours to tell the data subjects or face penalties. (This notification requirement may be waived if you use technological safeguards, such as encryption, to render data useless to an attacker.)

Data protection by design and by default

From now on, everything you do in your organization must, “by design and by default,” consider data protection. Practically speaking, this means you must consider the data protection principles in the design of any new product or activity. The GDPR covers this principle in Article 25.

Suppose, for example, you’re launching a new app for your company. You have to think about what personal data the app could possibly collect from users, then consider ways to minimize the amount of data and how you will secure it with the latest technology.

Consent

There are strict new rules about what constitutes consent from a data subject to process their information.

- Consent must be “freely given, specific, informed and unambiguous.”
- Requests for consent must be “clearly distinguishable from the other matters” and presented in “clear and plain language.”
- Data subjects can withdraw previously given consent whenever they want, and you have to honor their decision. You can’t simply change the legal basis of the processing to one of the other justifications.
- Children under 13 can only give consent with permission from their parent.
- You need to keep documentary evidence of consent.

Data protection principles

If you process data, you have to do so according to seven protection and accountability principles outlined in Article 5.1-2:

1. **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes specified.
4. **Accuracy** — You must keep personal data accurate and up to date.
5. **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose.
6. **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

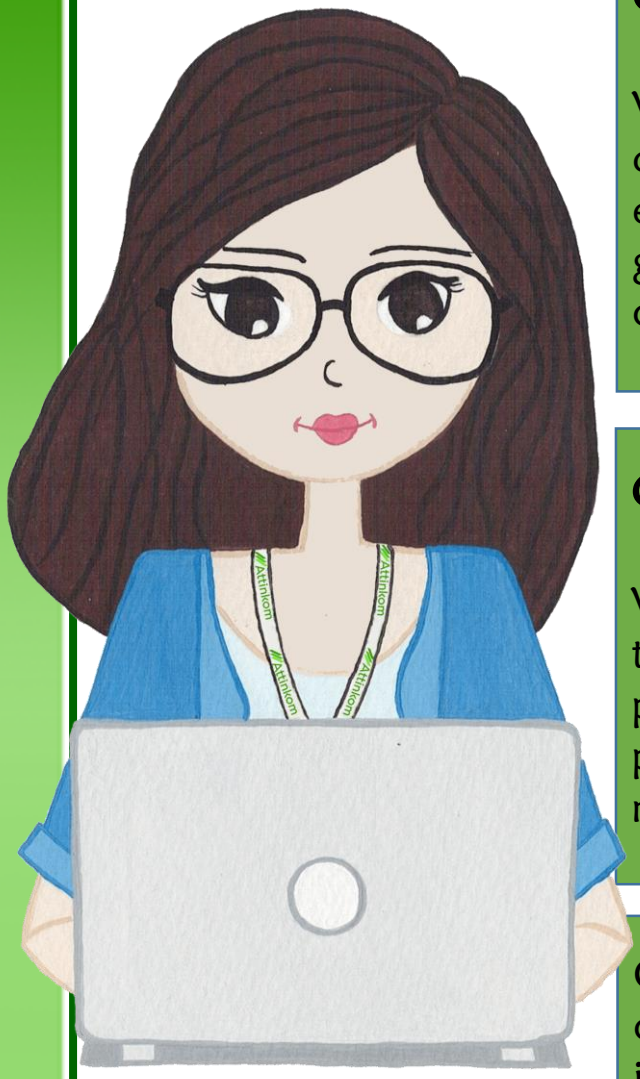
Benefits of Embracing GDPR Compliance

Organizations need to understand that the GDPR is not just a regulatory obligation, but also a means for achieving business and technology alignment. Data has always been a growing concern for all trades and managing it can be stressful for those without the correct systems in place. Here are a few ways your business can experience both immediate and long term benefits from GDPR compliance.

- Increased Cybersecurity
- More Accurate, Secure and Organized Data
- Gaining Better Customer Relationships thereby enhancing Business Reputation
- Better alignment with evolving technology

Attinkom
We verify your trust

How Attinkom can assist



GDPR Gap Assessment

Wecurrent review your organization's data protection and privacy environment and provide a detailed gap assessment to help your organization achieve compliance.

GDPR Assessment

We determine your compliance against the GDPR standard by reviewing the policies, procedures and processes in place to ensure that your organization meets the GDPR requirements.

Our assessors are available to assist your organization in understanding the impact of GDPR on your organization, as well as any gaps that your organization may have that affect GDPR compliance.