techahead

DEMYSTIFYING GDPR

ULTIMATE CRASH COURSE TO COMPLIANCE

ANYONE CAN BE GDPR READY
NO APHORISM TRUE ADVICE

EXECUTIVE SUMMARY

01 | What is GDPR? 1

02 | To whom does GDPR apply? 2

03 | What are the key objectives Of GDPR? 3

04 | Organization’s Data Security under GDPR 5

4.1 Infrastructure 6

4.2 Company and Data 8

4.3 Product/Application 10

4.4 Employees 12

4.5 Users/Customers 13

4.6 Source Code 15

05 | What makes GDPR different? 16

06 | Fine for Non-compliance 17

07 | Conclusion 18

WHAT IS GDPR?

The General Data Protection Regulation (GDPR) is an EU regulation on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).

GDPR demands greater accountability and transparency from organizations in aspects regarding data storage and processing.

It also addresses the export of citizens personal data outside the EU and EEA. The GDPR regulation aims primarily to give control to citizens and residents over their data. Any operating body that processes personal data should ensure that they abide by the law and its required procedures.

General Data Protection Regulation became enforceable throughout the EU on 25 May 2018. It replaces the 1995 Directive. In the UK, GDPR replaces the Data Protection Act and will be enforced by the Information Commissioner’s Office (ICO), which has the power to prosecute companies that have not taken measures to combat potential vulnerabilities of sensitive data.

Under the terms of GDPR, organizations need to ensure not only that personal data is gathered legally and under strict conditions, but also that those who collect and manage it are obliged to protect it from misuse and exploitation, as well as respect the rights of data owners and face penalties for not doing so.

TO WHOM DOES GDPR APPLY?

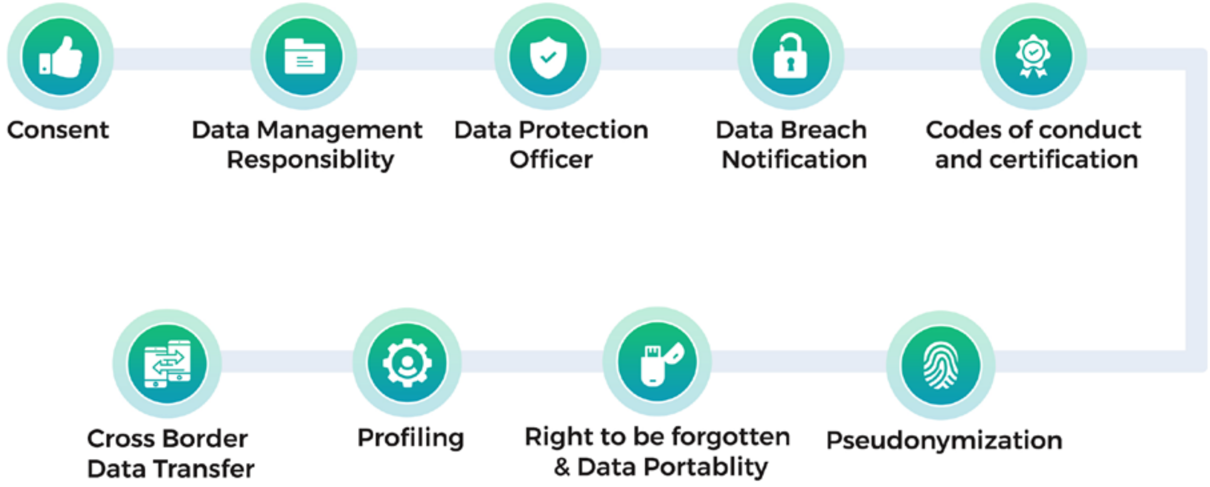
Complying with GDPR is not optional. GDPR enforces data controllers to use both organizational and technical safeguards to make sure there is no alteration of the data. Being non-compliant with GDPR can have expensive consequences.

GDPR not only applies to organizations located within the EU but also to organizations located outside of the EU if they offer goods or services, or monitor the behavior of EU data subjects. It applies to all companies processing and holding personal data of subjects residing in the European Union, regardless of the company's location.

The GDPR law applies to:

1. A company or entity which processes personal data as a part of the activities of one of its branches established in the EU, regardless of where the data is processed; or
2. A company established outside the EU offering goods/services (paid or for free) or monitoring the behavior of individuals in the EU.

If your company processes personal data as described above, you need to comply with the GDPR.


Consent
Data Management Responsiblity
Data Protection Officer
Data Breach Notification
Codes of conduct and certification
Cross Border Data Transfer
Profiling
Right to be forgotten & Data Portablity
Pseudonymization

KEY ASPECTS OF GDPR

The following are the most important aspects of the law:

1 Easier access to one's data: Individuals will have more information on how their data is processed, and this information will be available in a clear and understandable way.

2 Right to data portability: It will be easier to transfer personal data between service providers.

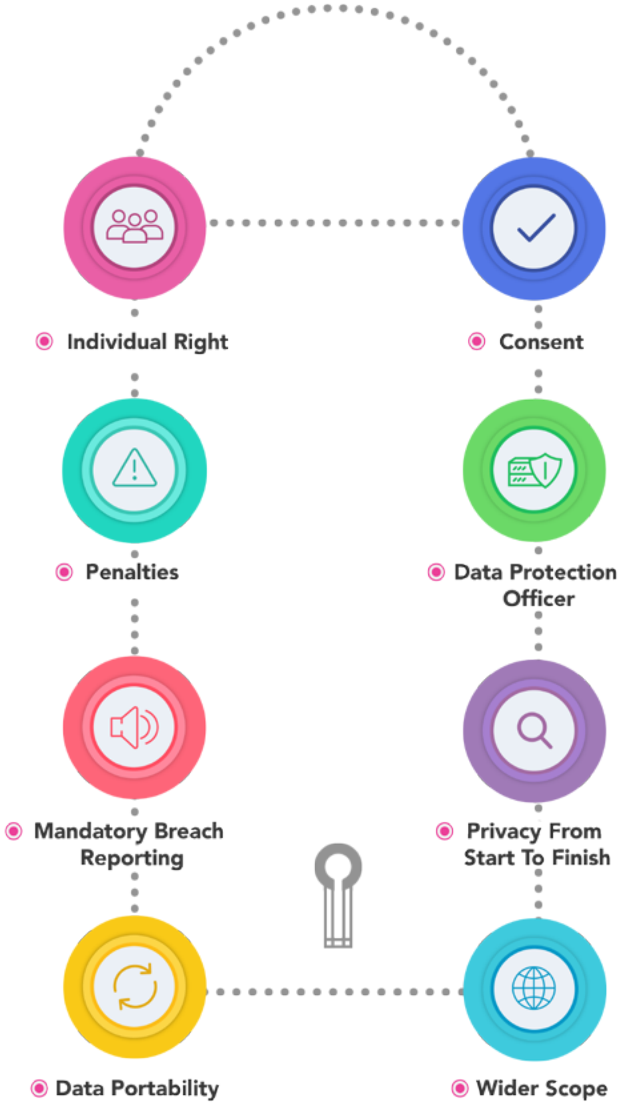
3 Right to be forgotten: When a user no longer wants data to be processed, provided that there are no legitimate grounds for retaining it, the data will be deleted.

4 Clarity of data usage: Data collectors should clarify 'How, Who, Why and Where and for how long' the data will be used.

The right to know when their data has been hacked: For example, companies and organizations must notify the national supervisory authority of serious data breaches as soon as possible so that users can take appropriate measures.

THE REGULATION PROVIDES SPECIFIC SUGGESTIONS ON WHAT KIND OF SECURITY MEASURES MUST BE FOLLOWED

- Encryption of personal data
- Ability to ensure confidentiality, integrity and resilience of services when processing the data.
- The ability to restore the availability and access to data in a timely manner in the event of physical and technical assistance.



DATA SECURITY

Organization’s Data Security Under GDPR

We have categorized the data aspects of six different parts of the organization and product layers. Let us look at the actions and checks for these layers in the following pages.

INFRASTRUCTURE

INFRASTRUCTURE

GDPR Compliance Checklist for Infrastructure (✓)

- □ **Use SSL certificates to secure people using your website**
  Encrypting communications is not only about privacy but also about your users' safety, since it will prevent most attempts at tampering with what they receive.

- □ **Check your website's basic security**
  Websites are vulnerable to many different classes of vulnerabilities, some may be prevented by the appropriate configuration on the server. Static websites may expose your users to fewer risks.

- □ **Isolate assets at the network level**
  Only your public API's should be exposed to the Internet. You should isolate your networks to prevent any unauthorized accesses to your database which will prevent attackers from connecting to it and attempting to crack the password or exploit vulnerabilities.

- □ **Keep your OS up to date**
  You should download all your OS's security updates and regularly update your machines. For servers, you can delegate it to a PaaS provider (Heroku, AWS Beanstalk, etc.)

- □ **Backup, then backup again**
  Backup all your critical assets. Ensure that you attempt to restore your backups frequently, so you can guarantee that they're working as intended.

- □ **Restrict internal services by IP address**
  Everything non-public should only be accessible through a bounce host (e.g. no direct access to databases).

- □ **Centralize and archive your logs and make them meaningful**
  Logs are necessary to trace what happened after an incident, find where the attacker came from, and possibly even who they are. Many solutions exist to gather your logs. You need to take care that the system time configured on each of your machines is in sync so that you can easily cross-correlate logs.

- □ **Protect your application from DDoS attacks**
  A Distributed Denial-of-Service Attack (DDoS) can have devastating consequences on businesses.

INFRASTRUCTURE

□ **Keep a list of your servers**
If you are using a cloud service and all your machines are registered or spawned through cloud service provider- it is already built in within your service. In case you have your own server setup- you will need to create and maintain a list of your assets (servers, network devices, etc.), and review it regularly to determine if you still need them, keep them up to date, and ensure that they benefit from your latest deployments.

□ **Keep a list of your data processors**
It is essential to have a list of all data processors, and a contract must be signed between both parties to ensure data security.

□ **Watch for unusual patterns in your metrics**
Takeovers will often be used to steal your data or setup your servers to be used as bouncers. These can be detected by watching for unusual patterns in metrics such as network bandwidth, CPU and memory consumption, and disk usage.

□ **Know how to redeploy infrastructure from scratch**
This allows you to spawn new infrastructure quickly and populate it with data from your backups. It is the perfect use case for disaster recovery.

COMPANY AND DATA

COMPANY AND DATA

GDPR Compliance Checklist for Company and Data (✓)

□ **Ensure your domain names are secured**
Domain names should regularly be renewed. If you have bought one from a third party, you should also make sure that the authoritative configured name server is your own.

□ **Be honest and transparent about any data you collect and who you share it with:** In the case of a breach, the attackers may disclose any data they gather. Your customers need to be aware of what data you're storing, who you share it with, what you do with it and how long you will keep it. Have a contract with any third-party data processor.

□ **Make sure all your critical services are secured tool**
Companies rely on Google Apps, Slack, WordPress etc. These services have default settings, which should be changed to comply with the required security level. All of these services should be kept up to date.

□ **Make sure your email is secured**
Email is the first point of call for cyber attacks. Research indicates that 91% of attacks start via email. Deploy industry-standard protocols that help companies to secure their email and domains against phishing attacks.

□ **Cross-border data flows in your privacy policy**
If you are disclosing users data outside EU, it should be clearly mentioned in your privacy policy about how that data is being processed.

□ **Do not share Wi-Fi**
Sharing Wi-Fi networks with guests or neighbors may give them the opportunity to gather information on your network and allow them to access resources protected by source IP.

□ **Take special care of your non-tech employees**
Non-tech employees are less used to technical trickery and can be deceived more easily than others, opening the door to ransomware or confidentiality issues. They should be trained and empowered to be distrustful and to preserve the company's assets.

□ **Have a public security policy for data accessibility**
This page should be on your corporate website describing how you plan to respond to external bug reports and threats.

□ **Have an internal security policy**
This is a short document stating the security requirements in your company and defining who is responsible and/or concerned with all aspects of security. Also, explain why the company needs personal information. It should contain a reason for data processing, e.g., the fulfillment of a contract.

COMPANY AND DATA

□ **Set up a bug bounty program**
A bug bounty program will allow external hackers to report vulnerabilities. Most of the bug bounty programs offer rewards for bugs found. You need security-aware people inside your development teams to evaluate any reports you receive.

□ **Make an inventory of your company's assets**
An awareness of your company's assets enables you to monitor the points that need the most attention and vulnerabilities that need to be hardened.

□ **Have a security incident response plan**
A plan must be ready to tackle any security breach or any suspicious activity.

□ **Notify Users about the security incident**
This will allow whoever is in charge at the time of a breach to communicate accordingly about an incident and will allow the fastest response in technical / communication terms.

□ **Cross-border data flows in your privacy policy**
If you are disclosing users data outside EU, it should be clearly mentioned in your privacy policy about how that data is being processed.

□ **Data Protection Officer**
This person should have knowledge of GDPR guidelines as well as knowledge about the internal processes that involve personal information.

□ **For Business outside EU, Have a representative In any of the EU states**
If you have a business outside of the EU and you collect data on EU citizens, you should assign a representative in one of the member states for your business. This person should handle all issues related to processing. Particularly, a local authority should be able to contact this person.

□ **Data Breach Notification within 72 Hours**
Personal data breaches should be reported within 72 hours to the local authority. You should report what data has been lost, what the consequences are, and what countermeasures you have taken. Unless the data leaked was encrypted, you should also report the breach to the person (data subject) whose data you lost.

PRODUCT/APPLICATION

PRODUCT / APPLICATION

GDPR Compliance Checklist for Product/Application (✓)

□ **Set User Specific access privileges**
In case an attacker successfully attacks your application, and get access as a user, the attacker will not automatically have access to host services, so it is a prudent strategy to set user-specific privileges.

□ **Monitor your Third party dependencies**
Applications are built using dozens of third-party libraries. A single flaw in any of these libraries may put your entire application at risk.

□ **Use a real-time protection service**
These tools protect web applications from attacks at runtime. The protection logic is inserted into the applications. They protect against all major vulnerabilities (SQL injections, XSS attacks, account takeovers, code injections, etc.) without false positives.

□ **Hire an external penetration testing team**
They take an external and naive point of view of your infrastructure and products. Pentesters will take nothing for granted and will check even the most basic assumptions, as well as all your infrastructure. You can also ask them to start with a full, blind discovery of your infrastructure, which can help you remember about old assets.

□ **Checkbox for Terms and Conditions about the data collection**
If your website collects personal information in some way, you should have an easily visible link to your privacy policy and confirm that the user accepts your terms and conditions.

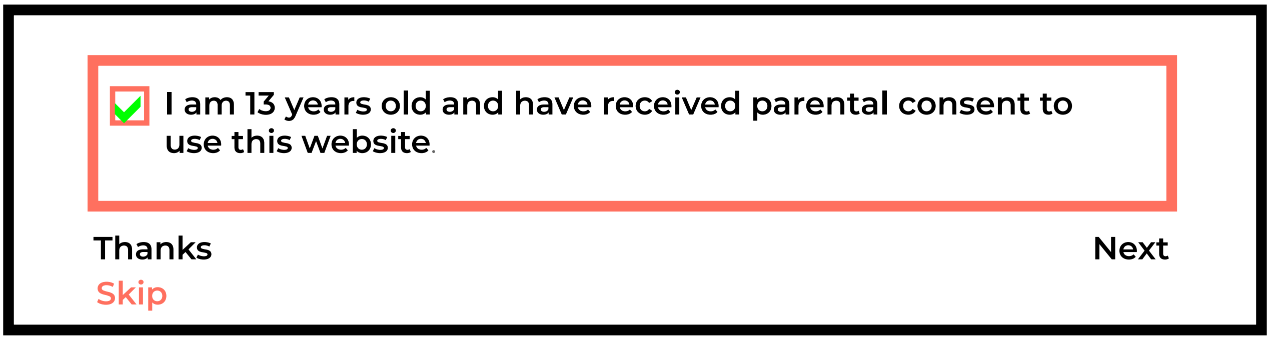
□ **Inform users on updation of your policies**
Email upcoming changes of your privacy policy. Your communication should explain in a simple way about what has changed.

□ **Clear Privacy Policy**
The policy should be written in clear and simple terms and should not conceal its intent in any way. Failing to do so could void the agreement entirely. When providing services to children, the privacy policy should be easy enough for them to understand.

PRODUCT / APPLICATION

□ **Easy consent withdraw**
Provide an easy way for users to withdraw the consent they have allowed.

□ **Child data processing policy**
For children younger than 16, you need to make sure a legal guardian has given consent for data processing. If consent is given via your website, you should try to make sure approval was actually given by the legal guardian.



☑ **I am 13 years old and have received parental consent to use this website.**

EMPLOYEES

EMPLOYEES

GDPR Compliance Checklist for Employees (✓)

□ **Accustom everyone to security practices**
Humans are often the weakest links in the chain of security. By explaining how an attacker could infiltrate your company, you will increase your employees' awareness and thus minimize the chance of them falling into such a trap.

□ **Require 2FA in your services**
Your employees should all use two-factor authentication on all services you use. If their password is stolen, the attacker cannot use it without the two-factor authentication.

□ **Encrypt all employee laptops & phones**
By encrypting all laptops, you protect both your company's assets and your employees' private files.

□ **Accustom your team to lock their machines while away**
Your office may be secured, but you will eventually have to receive external people for a party or a meeting. Locking all the machines is a great habit. If you get in the habit of locking your machine at the office, you'll be unlikely to forget to also do it in a Starbucks or at a meetup.s.

□ **Use a password manager to ensure you only use strong passwords**
Using a complex and unique password for every website is great advice, but it can be very difficult to remember all of them. Password managers are an excellent way to manage these since they will remember everything for you with a master password.

□ **Follow an onboarding/ offboarding checklist**
This checklist should contain a list of all the steps you need to enforce when an employee, contractor, intern, etc., join your company. A similar list should also be used when someone is leaving your team to ensure that they no longer have access to any of your company's resources

□ **Do not share accounts**
Sharing a user account makes it hard to understand who is using the service or to identify who has performed a given action.

□ **Use centralized account management**
A centralized place with all user authorizations is the best way not to forget anything once you need to update a user profile (e.g. if an internship has concluded). It is also a great place to define standard account creation you need for a given user.

USERS/CUSTOMERS

USERS / CUSTOMERS

GDPR Compliance Checklist for Users/Customers (✓)

□ **Enforce a password policy**
Your user accounts will be much harder to steal if you require them to use complex passwords: mixed case, special characters, minimum length, etc.

□ **Encourage your users to use 2FA**
As you get higher profile customers, you will be required to implement stronger security practices. This includes offering them two-factor authentication, role-based account management, etc.

□ **Monitor your users' suspicious activities tool**
Some users may behave suspiciously, trying to hack into your application, subvert your services, or bother your other customers. By monitoring such users, you will be able to block or flag the illegitimate ones.

□ **Right of personal information access / Update**
Provide easy online access or a way to provide them access and update to their personal information.

□ **Automate deletion of data you no longer need**
Setup a mechanism that deletes user's personal data once it is no longer needed.

□ **Delete data on Users request**
Provide easy online access or a way to delete their personal information

□ **Stop processing user data on request by user**
Setup a mechanism that stops processing users personal information on the individual's request.

□ **Easy delivery of users' data to themselves or third-party**
Setup a mechanism to deliver users' information to them or any 3rd party whenever requested.

USERS / CUSTOMERS

□ **Right to Object to data processed by automatic decision**
Users should have access to their data that involve automated decision making. On objection, the processor should stop using user's data and remove the same as per request.

□ **Notify your users about policy updates**
You should notify your users everytime you change your policies and terms of usage.

SOURCE CODE

SOURCE CODE

GDPR Compliance Checklist for Source Code (✔)

□ **Enforce a secure code review checklist**
Security should always be kept in mind while coding. In addition, keep in mind the typical security flaws.

□ **Use a static security code analysis tool**
Static code analysis tools can quickly overwhelm you with a lot of meaningless false-positives but switch on security-focused tools can help you discover vulnerabilities inside your code and most importantly increase the security awareness.

□ **Maintain a backlog of security concerns in your issue tracking tool**
The developer should contribute to maintaining a list of security issues to be fixed in the future.

□ **Never do cryptography yourself website**
Always rely on existing mechanisms, libraries, and tools. Cryptography needs expertise. Building your own implementations or using flags and options you don't fully understand will expose you to major risks.

□ **Keep secrets away from code**
Never commit secrets in your code. This allows a clear separation between your environments (typically development, staging, and production).

□ **Perform security-oriented test sessions**
Every once in a while, the team should spend time targeting all parts of the application, looking for vulnerabilities. Make sure to test for account isolation, token unicity, unauthenticated paths, etc.

□ **Use a secure development life cycle**
The secure development lifecycle is a process that helps tackle security issues at the beginning of a project. While rarely used, it provides good insights at all stages of the project, from the specification to the release.

WHAT MAKES GDPR DIFFERENT?

GDPR not only expands the scope of legislation about data privacy but also broadens the definition of the personal data that needs to be governed. It defines personal data as any information that can be used to identify an individual, directly or indirectly.

Any company that markets goods or services to EU residents can be subject to the GDPR. This is regardless of the physical location of the business itself. This provision in the GDPR essentially makes it a worldwide law.

GDPR will require that both controllers and processors that regularly collect or process personal data from EU citizens on a large scale to appoint a local representative in the EU states where they do their business.

Personal data identifiers include: Name, Identification numbers, location data and online identifiers. Also included are all factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a person.

GDPR applies wherever data is sent, processed or stored.

FINE FOR NON COMPLIANCE

There are several penalties that can be imposed for different infringements of the regulation. The new regulation has a set of serious penalties for organizations which fail to comply, especially those that suffer data breaches due to non-compliance. A written warning can be sent to organizations in cases of first and unintentional non-compliance. Easily the least-scary penalty of all, this warning should be taken very seriously as it will be the first and last caution – you won't want to get caught out again.

Depending on the violation, fines may range from €10 million or 2% of the annual revenue or €20 million or 4% of the worldwide annual revenue of the prior fiscal year, whichever is higher.

SUPERVISORY AUTHORITY WILL IMPOSE FINES BASED ON:

Nature of Infringement

Intention

Mitigation

Preventive Measures

History

Coooperation

Data Type

Notification

CONCLUSION

The General Data Protection Regulation (GDPR) may look like an imposing and costly exercise, but for business and economies it has the potential to add enormous value for those who get it right. Companies today collect vast amount of data. The GDPR compliance effort can be used to create opportunity by cleaning house, honing processes to collect the right information at the right time and developing a stronger bond with the customers from whom data is collected. In simple words, it is an opportunity to take stock and make improvements.

Non-compliance with GDPR can result in heavy fines and increased regulatory actions. More importantly, significant breaches can damage an organization's brand, value, and reputation. Protecting the brand requires that an organization that collects personal data must be able to prove consistently and reliably that it complies with the GDPR privacy and security principles.

The processing of personal data should be "adequate, relevant and limited to what is necessary for the purposes for which they are processed". A data protection officer should be designated who is responsible for monitoring compliance with GDPR and making sure that personal data is safe and secure.

All relevant people have the right to receive a copy of their data, the right to correct and restrict their data as well as the right to erase data.

The path towards GDPR compliance includes a coordinated strategy involving different organizational entities including legal, human resources, marketing, security, IT and others. Organizations should therefore have a clear strategy and action plan to address the GDPR requirements.

LOCATIONS

- Los Angeles
- New Jersey
- India

CONNECT WITH US

- in /techahead
- f /techahead
- /techahead

techahead

This document is purely for information purpose. The content of this document may change without any prior notice and can not be used for the legal purpose. This document under 'TechAhead Software' cannot be reproduced or transmitted by any organisation, by any organisation at any platform without legal permission. TechAhead doesn't hold any responsibility for any errors in the document, or any kind of libility on any platform at any level.