GDPR checklist for data controllers

Are you ready for the GDPR? Our GDPR checklist can help you secure your organization, protect your customers' data, and avoid costly fines for non-compliance.

To understand the GDPR checklist, it is also useful to know some of the terminology and the basic structure of the law. You can find this information on our What is GDPR? page. Please keep in mind that nothing on this page constitutes legal advice. We recommend you speak with an attorney specialized in GDPR compliance who can apply the law to your specific circumstances.

Lawful basis and transparency

- [ ] Conduct an information audit to determine what information you process and who has access to it.
- [ ] Have a legal justification for your data processing activities.
- [ ] Provide clear information about your data processing and legal justification in your privacy policy.

Organizations that have at least 250 employees or conduct higher-risk data processing are required to keep an up-to-date and detailed **list of their processing activities** and be prepared to show that list to regulators upon request. The best way to demonstrate GDPR compliance is using a **data protection impact assessment** Organizations with fewer than 250 employees should also conduct an assessment because it will make complying

with the GDPR's other requirements easier. In your list, you should include: the purposes of the processing, what kind of data you process, who has access to it in your organization, any third parties (and where they are located) that have access, what you're doing to protect the data (e.g. encryption), and when you plan to erase it (if possible).

Data security

- [ ] Take data protection into account at all times, from the moment you begin developing a product to each time you process data.
- [ ] Encrypt, pseudonymize, or anonymize personal data wherever possible.
- [ ] Create an internal security policy for your team members, and build awareness about data protection.
- [ ] Know when to conduct a data protection impact assessment, and have a process in place to carry it out.
- [ ] Have a process in place to notify the authorities and your data subjects in the event of a data breach.

You must follow the principles of "**data protection by design and by default**," including implementing "appropriate technical and organizational measures" to protect data. In other words, data protection is something you now have to consider whenever you do anything with other people's personal data. You also need to make sure any processing of personal data adheres to the data protection principles outlined in **Article 5**. Technical measures include encryption, and organizational measures are things like limiting the amount of personal data you collect or deleting data you no longer need. The point is that it needs to be something you and your employees are always aware of.

Accountability and governance

- [ ] Designate someone responsible for ensuring GDPR compliance across your organization.
- [ ] Sign a data processing agreement between your organization and any third parties that process personal data on your behalf.
- [ ] If your organization is outside the EU, appoint a representative within one of the EU member states.
- [ ] Appoint a Data Protection Officer (if necessary)

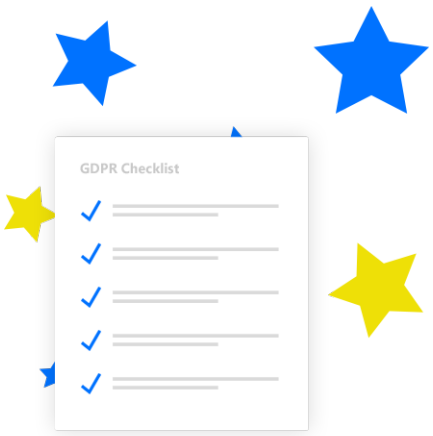
Another part of "**data protection by design and by default**" is making sure someone in your organization is accountable for GDPR compliance. This person should be empowered to evaluate data protection policies and the implementation of those policies.

Privacy rights

- [ ] It's easy for your customers to request and receive all the information you have about them.
- [ ] It's easy for your customers to correct or update inaccurate or incomplete information.
- [ ] It's easy for your customers to request to have their personal data deleted.
- [ ] It's easy for your customers to ask you to stop processing their data.
- [ ] It's easy for your customers to receive a copy of their personal data in a format that can be easily transferred to another company.
- [ ] It's easy for your customers to object to you processing their data.
- [ ] If you make decisions about people based on automated processes, you have a procedure to protect their rights.

People have the **right to see what personal data you have about them** and how you're using it. They also have a right to know how long you plan to store their information and the reason for keeping it that length of time. You have to send them the first copy of this information for free but can charge a reasonable fee for subsequent copies. Make sure you can verify the identity of the person requesting the data. You should be able to comply with such requests within a month.

Success!



Congratulations! If you've dutifully worked to the bottom of the GDPR checklist then you've significantly limited your exposure to regulatory penalties.

Finally, we want to remind you once more that this checklist is not in any way legal advice. There are dozens of provisions in the GDPR that apply only in rare instances, which would be counterproductive to cover here. You should check with a lawyer to make sure your organization fully complies with the GDPR.

Getting Started

[What is GDPR?]

[What are the GDPR Fines?]

[GDPR Compliance Checklist]

Templates

[Data Processing Agreement]

[Right to Erasure Request Form]

[Writing a GDPR-compliant privacy notice]

Technical Review

[Data Protection Office Guide]

[GDPR and Email]

[Does GDPR apply outside of the EU]

About Us

GDPR.eu is co-funded by the Horizon 2020 Framework Programme of the European Union **and operated by Proton AG**.

GDPR Forms and Templates

Data Processing Agreement > **Right to Erasure Request Form >** **Privacy Policy >**

Terms and Conditions Privacy Policy