

## GDPR Compliance for Startups: Beyond the Basics

The General Data Protection Regulation (GDPR) is a major EU law whose main goal is to give people more control over their personal data, especially as digital activities expand. It applies to any startup established in the EU, as well as to companies located in other countries, if they process personal data from individuals located in the EU, during i.e. the offer of goods and services. This means that, in all likelihood, the GDPR will apply to your startup from an early stage.

With that in mind, here we will give you an overview of the first steps to focus on, to foster a compliance by design mentality.

### Map your data flows

Start by understanding the personal data your startup collects, stores, and uses. Think of your website, CRM, email platforms, payment systems, and analytics tools. To make this task easier, involve the different leadership roles and teams within the organization and assess what data they handle and what information flows they rely on.

It is also important to not limit yourself to just “what” personal data is collected. Note the source (individuals, or a third-party), why you collect it, where it is stored and with whom it is shared with. Make sure to also note how long you keep it and whether it is transferred outside the EU/EEA.

For most startups, a spreadsheet or equivalent software is sufficient at the start, but consider automated tools if your processing activities grow. It is also important to review and update your map at least quarterly to cover any system or process changes.

### Identify your legal basis

Besides understanding what personal data it processes, your startup must also identify at least one lawful basis that justifies that processing. The most used ones are:

- **Consent:** it requires a clear, active opt-in by the individual and must be easy to withdraw.
- **Contract:** for the processing that is necessary either to take steps to enter a contract with an individual at their request, or to execute a contract.
- **Legitimate interest:** it is the most versatile, but it requires that you: (1) have an interest that is legitimate, (2) demonstrate that the processing is necessary for that purpose, and (3) verify your interests do not override individuals’ rights.

Bear in mind that different activities may require different legal bases, so it is important to document the applicable one(s) to each of your processing activities. It is also important to note that particularly sensitive information cannot, in general, be processed, unless specific exceptions apply, such as explicit consent, medical diagnosis, and treatment. This includes

the processing of health data, biometric data, and information that reveals political and philosophical opinions, as well as sexual orientation.

### **Draft your privacy policy(ies)**

Transparency is also a key element of the GDPR, and having clear, simple and tailored privacy policies goes a long way in that direction. To that end, a good starting point is targeting a specific audience per policy - think website users, clients, employees, etc - and drafting it in accordance with the specific processing activities that affect that audience.

When doing so, make sure to include, i.e. your company name, contact details, what categories of personal data you collect, why you collect it, and how long you keep it. It is also important to list your legal bases and users' rights, such as withdrawal of consent, access, objection, and deletion.

Draft these documents with plain, simple language and avoid legal jargon. Make them easy to find, for example, by adding links to your website footer and at every data collection point.

### **Manage your service providers and applicable agreements**

When dealing with third-parties that you work with, start by listing the ones that handle personal data for your startup. This includes cloud providers, SaaS platforms, email and analytics tools, CRM, payment solutions, and communication services.

For each identified processor, you must sign a Data Processing Agreement (DPA), specifying, for example, the purpose, duration, and type of data processed, your rights, along with required security measures, namely in case of data breaches. Many large vendors offer a standardized DPA as an annex to their terms and conditions but read it closely as this agreement should clarify i.e. that your service provider only acts on your instructions and maintains high security standards.

It is also important to check if and how your processors use their own subprocessors (other vendors that process your data). You should ask your service providers for a full subprocessor list (generally as an annex to the DPA) so that you may review and approve them, as appropriate.

Your job does not end once you sign. For example, you should review your vendors' practices and subprocessors periodically, at least the most critical. This active oversight helps protect against breaches and shows to your stakeholders that your startup is organised and takes vendor management seriously.

### **Implement security measures**

Lastly, you must implement security measures that match the type and volume of personal data you handle. This does not mean high-cost solutions are mandatory, especially given that most startups work with cloud hosting services that already have these measures in place. However, it is still important to assess whether your specific use-case requires additional measures to mitigate confidentiality and integrity risks. This can be the case if you

have a remote team, mobile devices, bring-your-own-device (BYOD) policies, or work in particularly sensitive sectors, such as healthcare.

Besides this, you can focus on other practical solutions. For example:

- Adopt role-based access control to restrict data access only to team members that actually need it.
- Automate your data retention policies, ensuring data is deleted or anonymized when it is no longer needed.
- Adopt multi-factor authentication on mobile devices, especially if you allow remote work or if your devices leave the office.
- Assign security to one of your team members and organize periodic reviews of your security measures.

Complying with the GDPR is no easy feat, but there are steps your startup can take from its early stages to foster compliance and avoid fixing problems later. These are also good steps in information management, meaning that, besides compliance, you are also focusing on having clean and organized internal processes that ultimately help your startup be more efficient, secure, and resilient.

**Francisco Arga e Lima**

**Paxlegal**

✉ [paxlegal@paxlegal.pt](mailto:paxlegal@paxlegal.pt)

🌐 [www.paxlegal.pt](http://www.paxlegal.pt)

📍 Av. Eng. Duarte Pacheco, Torre 1  
14.º andar – Sala 1  
1070-101 Lisboa, Portugal