# Privacy Compliance: Getting Started Guide

LegalSite

# Table of contents

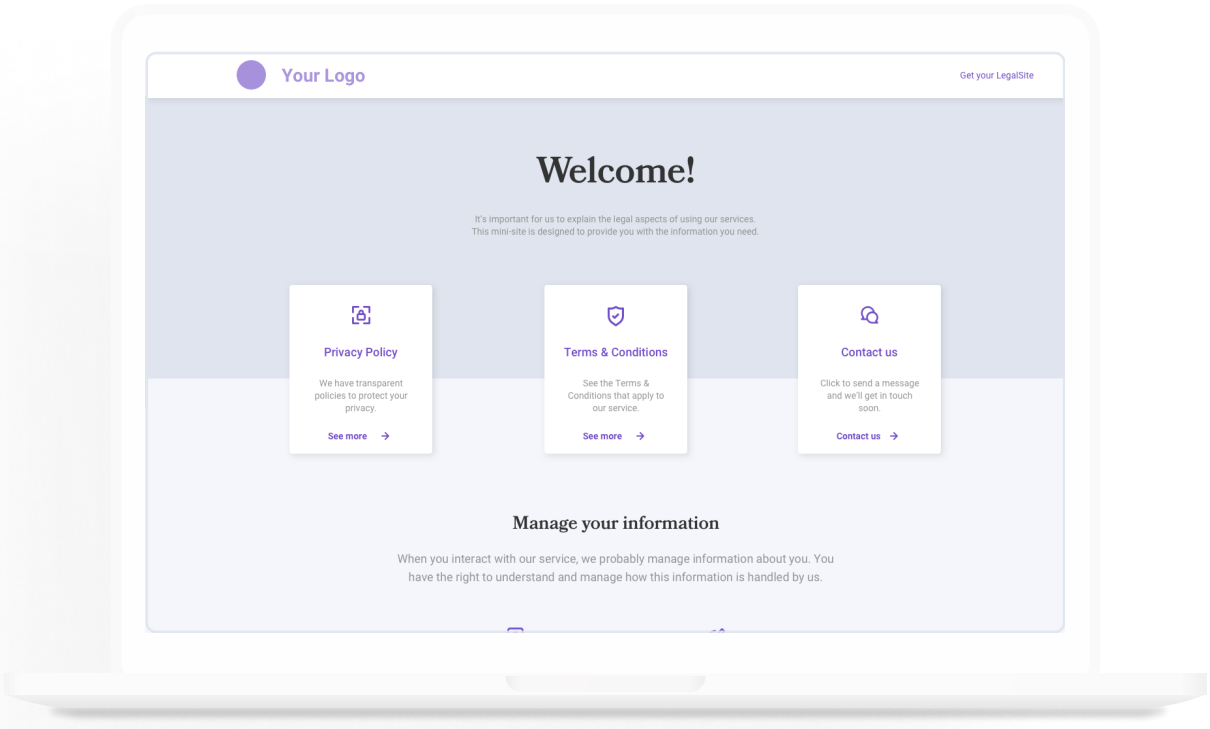
# What are Privacy Regulations

Laws like the GDPR are regulations to strengthen data protection for all individuals. This means that **if you have a website that processes personal data, you need to follow laws** and procedures to become compliant and avoid fines. Such personal data can include names, addresses, birth dates, contact information, or driver's licenses.

Besides the GDPR, most regions around the globe are putting in place privacy laws that businesses are expected to comply with. Privacy management should be part of your organization today.

With **LegalSite** your company becomes protected against legal risks, privacy compliant and always up to date with the latest regulatory developments.

Up and running in minutes so you can focus on your business.

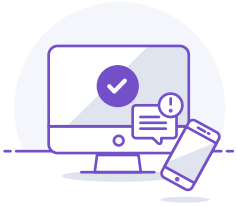


# Who needs to comply

**All websites that process data related to people should follow privacy compliance requirements**. Even if you run a simple blog or non-commercial website, you still need to comply.

The EU General Data Protection Regulations (GDPR) sets rules for collecting and processing personal information from users who live in the European Union. It's important to remember that it doesn't matter where websites are based, the law must be obeyed by **all sites worldwide that have visitors on the EU**.

This is also the issue with the California Online Privacy Protection Act of 2003 (CalOPPA) - The scope for this law is quite broad, as it does not only apply to businesses within California but all websites that are accessible by California residents.



Small website owners

Business

Enterprises

# What are the risks if I don't comply

Privacy regulations can have multiple penalties against those who violate privacy and security standards, regardless of your location globally, with fines reaching into hundreds of millions.

## Financial penalties

Art. 83 of GDPR addresses that non-compliance with the requirements can carry **fines up to EUR 20 million**, or in the case of a corporation, up to 4% of annual worldwide turnover, whichever is higher.

## Disciplinary measures

Several corrective measures can be taken such as warnings, reprimands, imposing temporary or **permanent bans on the processing of data**, demanding the rectification and/or deletion of data, and suspending the transfer of data for some time.

## Compensation for damages

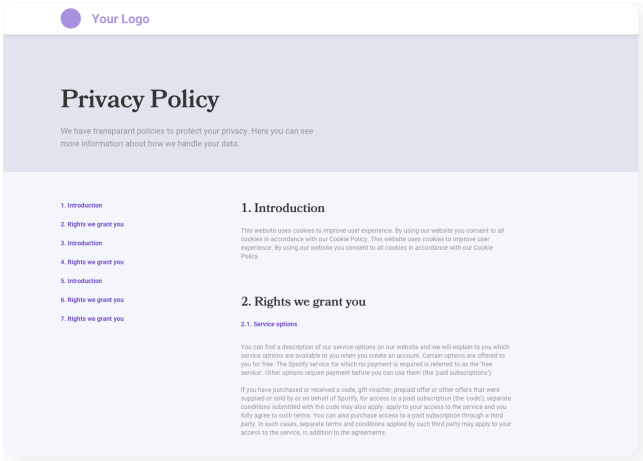
Any user who has suffered damage has the right to **receive compensation** from the controller or processor who has not complied with the obligations. A third-party can also take **legal action** against you, terminate service or permanently ban your company.

## Damaged reputation

How you handle your user's data can become a competitive advantage or break your reputation forever. In the long term, this can be the **biggest problem to recover from.**

# Requirements

Privacy compliance is so much more than merely setting up required pages such as a Privacy Policy page. It includes DPAs, handling data, solving requests, etc. You'll need to examine exactly how you're using user data in the first place to see if you're adhering to the GDPR or not. Having a consent page just simply isn't enough.




The legal system and privacy regulations are getting more and more complex. Even publishing a simple site, or a blog with visitor tracking requires you to put in place legal documents and procedures to comply. LegalSite helps your company to get protected against legal and financial risks.

The main requirements for adhering to the GDPR include:

## Terms & Conditions

Terms and Conditions are required for any business. They protect you from many potential liabilities.

## Privacy Policy

A Privacy Policy is required by law if you collect any kind of personal user information. That also includes any third-party service providers you're using like Google Analytics.

## Cookies consent pop-up

It is a requirement to display a cookie consent pop-up. You need consent for placing a cookie and also need to keep information such as when the user consent was given and to which Cookie policy agreed on.

## Access and Portability

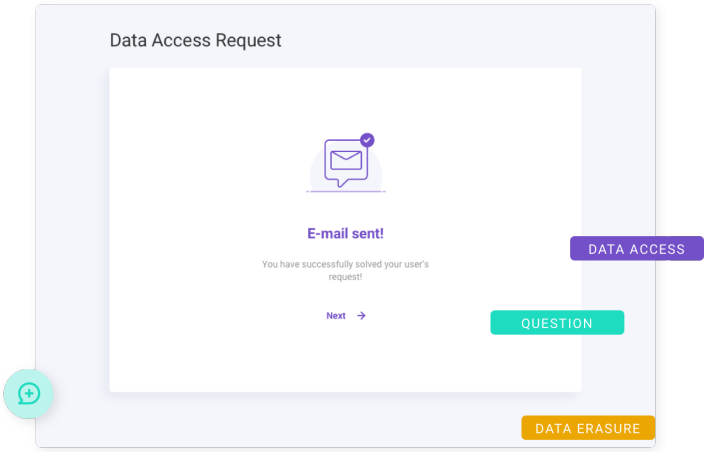
It allows your users to get access to their data and/or transfer it.  You also must provide visitors with information on the type of processing that is taking place, why and who is carrying it out.

## Accountability

Organizations need to be able to demonstrate what they did and its effectiveness when requested. This includes policies, procedures and incident management.

## Lawful processing

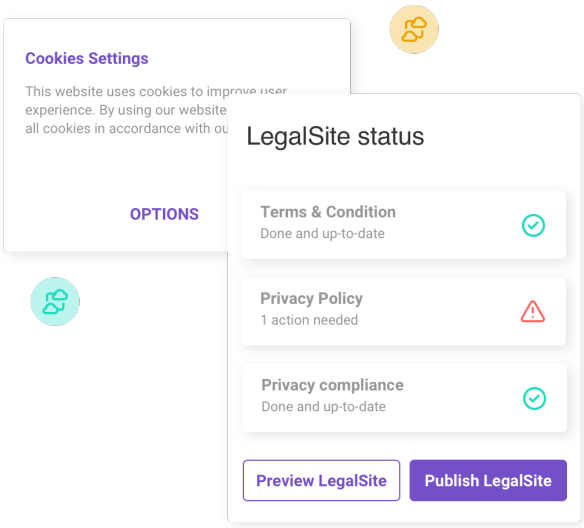
To process personal data you need consent, data processing agreements, and end-to-end data management policies in place. Including being able to process data requests.



# How it works

## Legal Pages

Do I need legal pages? The short answer: yes. Even operating a single-page website requires legal terms and privacy policies to be applied. Today you are taking a legal and financial risk if you do not put these in place. But don't worry, we do all the heavy lifting for you.




## Data Processing Agreements

A Data Processing Agreement (DPA) is a written contract required by the GDPR when one business processes personal data on behalf of another business. It's a way to give the controller an assurance that their data processors also protect the data and act in a GDPR compliant manner. With LegalSite you can track all your data processing agreements. We also provide a DPA template so you can send it to your clients using your LegalSite, including capturing online signatures.

## Privacy Impact Assessment

You are legally required to go through the procedure of assessing your privacy risks with a Privacy Impact Assessment (PIA). It's a questionary so you can document how your Data Subjects's data is maintained, how it will be protected and how it will be shared. It's important to know if the information being collected complies with privacy-related legal and regulatory compliance requirements. With a simple step by step form, we help you streamline this process and keep records of your assessments.

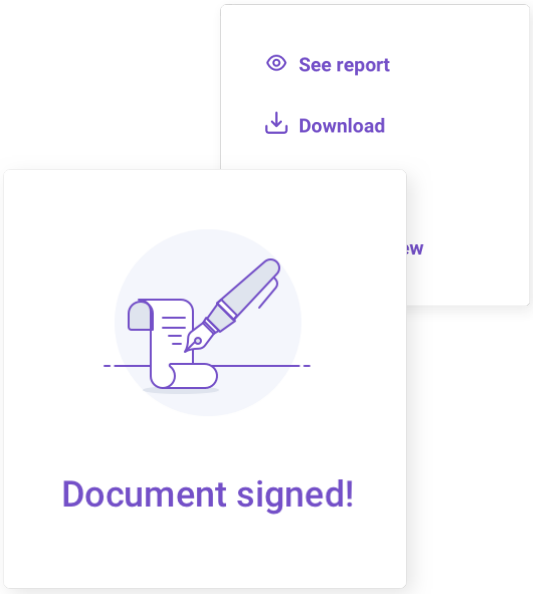
All commercial websites should invest in a Privacy Impact Assessment not just for the overall efficiency of their business, but also to make sure their bases are covered legally. If a loophole in a new project violates users' data right, you'll need to adjust it accordingly.

## Dealing with User requests

Privacy regulations allow your users to make multiple requests regarding their data and websites must respond to these requests within one month. With LegalSite you can centralize all incoming requests from your users such as data access and data erasure and see important deadlines. You can handle requests fast and easy, and still, ask for a lawyer to review it.

## Naming a Data Protection Officer

Your company is required to appoint a Data Protection Officer that will be responsible to ensure your company's compliance with GDPR and other data protection laws requirements. A DPO can be an existing employee or externally appointed and will act as the contact point for the supervisory authority, train the organization employees on compliance requirements and conduct regular assessments and audits.



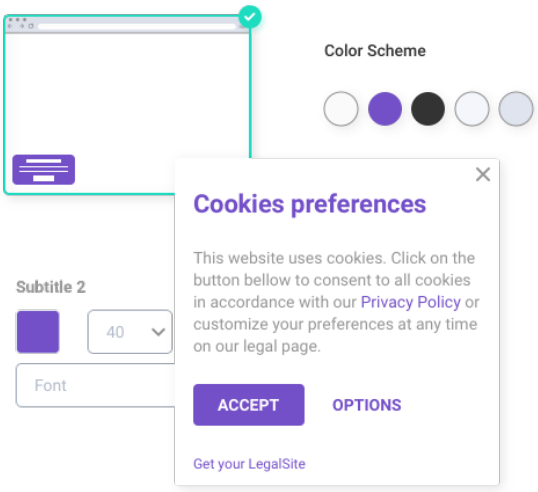

Under the GDPR, one must appoint a data protection officer if one is: a public authority, a website that requires very large scale and systematic monitoring of individual viewers or a website with core activities that involve large scale processing of special data categories, especially data related to criminal convictions and cases.

Regardless, if data protection is going to be a major aspect of your business, it may be wise to appoint a data protection officer anyway. Such an officer is responsible for overseeing an organization's overall data protection strategy and its implementation to adhere to GDPR guidelines.

Even if you aren't based in Europe, it is worth considering the employment of a data protection officer if you're in a business that deals with a significant amount of private data or is particularly large. A data protection officer can make sure that your privacy and security measures are playing out as planning and can also pinpoint vulnerabilities that could lead to a data breach.

## Data Breach Incidents

In the event of a data breach incident, it is imperative that you contact the affected users and/ or companies to notify them. You are also required to report personal data breaches to the relevant supervisory authority within 72 hours after becoming aware of the breach. We guide you through this process so it can be done easily and with transparency.




## Cookies and consent logs

The GDPR requires that websites keep a log of all consent given by users on Cookies and other Policies. Cookies are used by a majority of websites to track the number of visits, activity and more. They are fantastic tools for analytics and for looking into what your users are doing on your site, but privacy regulations have many requirements about how them, such as:

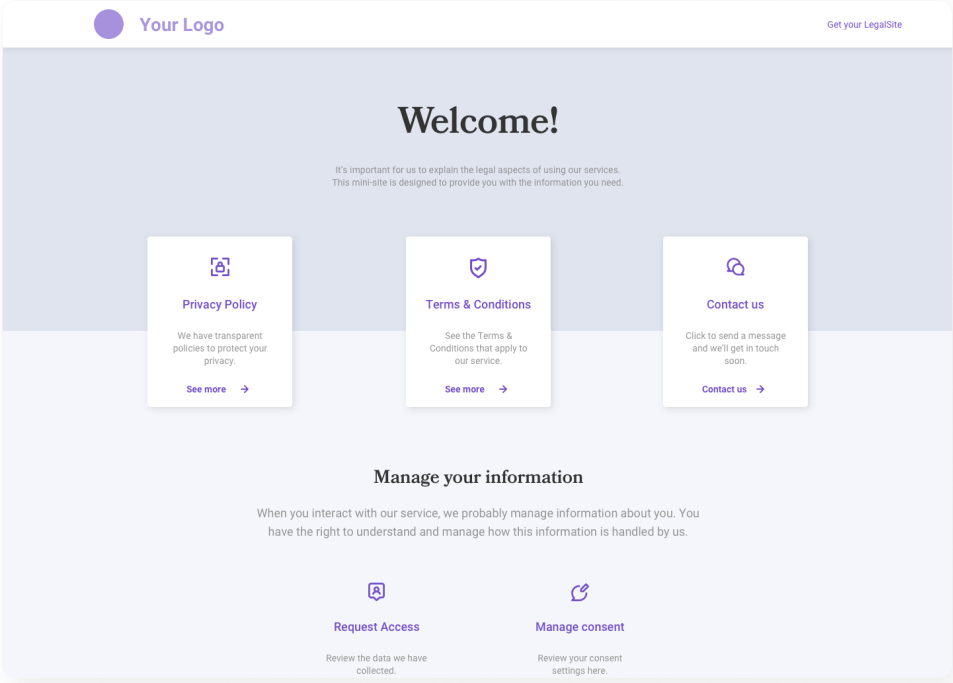
Any terms must be explained; Consent must be extremely unambiguous and requires a clear affirmative action or statement; For those under 16 years of age, additional consent and authorization are required from a parental figure.

Easily customize your agreement consent pop-ups with LegalSite. Adapt the privacy regulations ready cookie to your website visuals by changing the colors, fonts, and placing.

## LegalSite management

Managing all of these legal docs, consent forms, consent pop-ups, and legal jargon may seem like a lot. However, with LegalSite, managing and crafting all of these necessary legal documents is incredibly easy.

Go to www.legalsite.co and create an account to get protected against legal risks, privacy compliant and always up to date with the latest regulatory developments. Up and running in minutes so you can focus on your business.




LegalSite