

The Small Business Guide To Privacy

Created by :
Termageddon





Table of Contents

Introduction	2
Privacy Policy and PII	3
Who privacy laws apply to	4
Privacy Policy laws and changes	5-7
Privacy Policy disclosures	8
Cookie Policy and consent solution	9
Cookie laws	10-11
What your cookie consent banner should look like	12
Compliance checklist	13



ABOUT THE GUIDE

Small business owners have a lot to worry about - salaries, business plans, clients, the actual product or service that you are offering, marketing and much more. One requirement that often slips through the cracks is privacy law compliance. In truth, privacy requirements can seem daunting and confusing.

One of the main reasons behind this confusion is that there are no resources that spell out privacy compliance requirements in plain language all in one place. That is our goal behind this Small Business Guide to Privacy - to tell you everything that you need to know, in one place.

WHY PRIVACY? WHY NOW?

Privacy is here to stay. Each year new privacy laws go into effect and more and more privacy bills are being proposed. This rise in regulations has also led to a rise in enforcement via fines and lawsuits. While the large corporations usually occupy the headlines, small businesses are also being fined and sued at growing rates.

WHY TERMAGEDDON?

Termageddon, LLC is a generator of Privacy Policies, Cookie Policies, Consent Tools, Terms of Service and more for websites. Termageddon can also automatically update policies to keep them up to date with changing legislation. Termageddon is not a law firm and this Guide is not intended to provide legal advice.



WHAT IS A PRIVACY POLICY?

A Privacy Policy is document that is displayed on your website that discloses what Personally Identifiable Information (PII) your website collects, what you do with that information, and who you share it with.

A Privacy Policy must include all of the disclosures that are required by the privacy laws that apply to you, must be up to date, and must accurately represent your privacy and business practices.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

PII (also referred to as 'personal data' or 'personal information') is any information that could identify someone or any information that relates to an identifiable person.

Examples of PII include:

- Name;
- Email address;
- Physical address;
- Phone number; or
- IP address.

Most modern websites collect this personal information through features such as:

- Contact forms;
- Email newsletter sign up forms;
- Account creation forms;
- Analytics;
- Blog commenting features;
- Analytics (e.g. Google Analytics); or
- Advertising (e.g. Meta Pixel).

This information is protected by privacy laws, which can require your website to have a Privacy Policy.



WHO DO PRIVACY LAWS APPLY TO?

Privacy laws apply to websites that collect Personally Identifiable Information. Privacy laws are created to protect individuals and not businesses, so the privacy laws of other states or countries can apply to you even if you are not located in that state or country.

To determine which privacy laws apply to you, you should ask:

- Where are your customers located?
- Who can submit their personal information on your website (e.g. submit a contact form)?
- Where do you offer goods or services?
- Who can access your website and be tracked (e.g. through analytics or advertising tools)?

Many privacy laws apply to small businesses, regardless of revenue amounts, number of employees, or the amount of personal information collected.

Privacy laws can start applying as soon as PII is collected, meaning that you do not need to share, sell, or even use the PII for privacy laws to apply to you.



PRIVACY LAWS THAT CAN REQUIRE A PRIVACY POLICY

The following privacy laws can apply to small businesses and require them to have a Privacy Policy:

1.CALIFORNIA ONLINE PRIVACY AND PROTECTION ACT (CALOPPA)

The California Online Privacy and Protection Act (CalOPPA) applies to any operator of a website that collects the PII of residents of California.

2.NEVADA REVISED STATUTES CHAPTER 603A

Nevada Revised Statutes Chapter 603A applies to any operator of a commercial website that collects the PII of residents of Nevada and does business in Nevada.

3.DELAWARE ONLINE PRIVACY AND PROTECTION ACT (DOPPA)

Delaware Online Privacy and Protection Act applies to any operator of a website that collects the PII or residents of Delaware.

4.RHODE ISLAND DATA TRANSPARENCY AND PRIVACY PROTECTION ACT (DTPPA)

The portion of the Rhode Island Data Transparency and Privacy Protection Act that includes the requirement to have a Privacy Policy applies to any commercial website that does business in Rhode Island or with customers in Rhode Island.



5.GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR applies to businesses that are:

- Located in the European Union;
- Offer goods or services to European Union residents (regardless of your location); or
- Monitor the behavior of European Union residents through features such as cookies, tracking pixels or analytics (regardless of your location).

6.UNITED KINGDOM DATA PROTECTION ACT (UK DPA)

UK DPA applies to businesses that are:

- Located in the United Kingdom;
- Offers goods or services to residents of the United Kingdom (regardless of your location); or
- Monitor the behavior of residents of the United Kingdom through features such as cookies, tracking pixels or analytics (regardless of your location).

7.PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

PIPEDA applies to any organization (regardless of location) that collects, uses, or discloses the PII of residents of Canada in the course of a commercial activity.

8.QUEBEC LAW 25

Quebec Law 25 applies to persons who collect, hold, user or share the personal information of residents of Quebec, Canada.

9.PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

POPIA applies to any business located in South Africa or businesses that are not located in South Africa but that are processing PII in South Africa.



10.AUSTRALIA PRIVACY ACT 1988

Australia Privacy Act 1988 applies to businesses outside of Australia if they do business in Australia and collect the PII of residents of Australia. It also applies to Australian businesses, regardless of their size, if they are:

- Private sector healthcare providers;
- Businesses that sell or purchase PII;
- Credit reporting bodies;
- Contracted service providers for Australian government contracts;
- Employee associations;
- Businesses that have opted in to comply with the law;
- Businesses that are related to a business covered by the law; and
- Business prescribed by Privacy Regulation 2013.

Please note that this not an exhaustive list - there are other privacy laws that may apply to larger businesses or you may be required to comply with other laws by contract.

CHANGES TO PRIVACY LAWS

As individuals are demanding to have a right to privacy, more states and countries are proposing and passing privacy laws. In addition, as technology evolves, existing privacy laws are being changed to keep up with the privacy risks introduced by these new technologies. You can learn more about proposed privacy bills here: <https://termageddon.com/global-privacy-bill-tracker/>.

All of these changes can affect the disclosures that need to be included in Privacy Policies. Therefore, it is important to not just have a Privacy Policy that is compliant with today's laws, but to also have a strategy to keep the Privacy Policy up to date with changing legislation.



WHAT DOES YOUR PRIVACY POLICY NEED TO STATE?

A lot of businesses assume that a Privacy Policy is just random disclosures or legalese. Unfortunately, this is simply not true. While Privacy Policies include general information such as what PII you collect, what you do with that PII, and who you share it with, most of the disclosures are based on the privacy laws that apply to you.

Privacy laws dictate that disclosures that must be included in your Privacy Policy. That is why it is so important to first determine which privacy laws apply to you - the privacy laws will state what disclosures your Privacy Policy needs to contain.

It is also important to note that the disclosures required by privacy laws do not always overlap. For example, a Privacy Policy that is compliant with GDPR will not include all of the disclosures required by CalOPPA or Nevada Revised Statutes Chapter 603A.

Lastly, you will need to ensure that your Privacy Policy accurately reflects your business and privacy practices. For example, if your Privacy Policy states that your website collects names and emails but you actually collect names, emails, and phone numbers, your Privacy Policy will not be compliant as it does not accurately reflect your practices.



WHAT IS A COOKIE POLICY?

A Cookie Policy is a document that is displayed on your website that lists what cookies your website sets, including their purpose, provenance and duration. It also informs website users of their choices regarding cookies (e.g. if they can opt in or out of certain cookies being placed on their device).

WHAT IS A COOKIE CONSENT SOLUTION?

A cookie consent solution is a banner that goes onto your website that provides individuals with information regarding the cookies that your website sets and asks them to either agree or decline the placement of cookies onto their device and/or browser. A cookie consent solution should prevent non-essential cookies from firing until the user has consented to such cookies and must include an “accept” and a “decline” option.

WHAT ARE COOKIES?

A cookie is a small piece of code that is created and stored on a website user’s browser and/or their device when visiting a website that sets cookies. Cookies are used to track information about the visitor for various reasons such as analytics, marketing, security, advertisements, and logging into accounts.

Many tools commonly used by websites such as Google Analytics, Shopify Analytics, Hotjar, Meta Pixel, LinkedIn Insights Tag, Google Maps, reCAPTCHA, YouTube Videos, and Vimeo Videos set cookies.



PRIVACY LAWS THAT CAN REQUIRE A COOKIE CONSENT BANNER

The following privacy laws can apply to small businesses and require them to have a cookie consent banner:

1.CALIFORNIA INVASION OF PRIVACY ACT

CIPA applies to any tracking of a website visitor from California through cookies, pixels, or similar tools and is enforced by the California Attorney General who can impose hefty fines for violations.

2.GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR applies to businesses that are:

- Located in the European Union;
- Offer goods or services to European Union residents (regardless of your location); or
- Monitor the behavior of European Union residents through features such as cookies, tracking pixels or analytics (regardless of your location).

3.UNITED KINGDOM DATA PROTECTION ACT (UK DPA)

UK DPA applies to businesses that are:

- Located in the United Kingdom;
- Offers goods or services to residents of the United Kingdom (regardless of your location); or
- Monitor the behavior of residents of the United Kingdom through features such as cookies, tracking pixels or analytics (regardless of your location).



3.PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

PIPEDA applies to any organization (regardless of location) that collects, uses, or discloses the PII of residents of Canada in the course of a commercial activity.

4.QUEBEC LAW 25

Quebec Law 25 applies to persons who collect, hold, user or share the personal information of residents of Quebec, Canada.

Please note that this not an exhaustive list - there are other privacy laws that may apply to larger businesses or you may be required to comply with other laws by contract.

WHAT SHOULD A COOKIE CONSENT BANNER INCLUDE?

A cookie consent banner should be easily seen as soon as someone enters your website for the first time. It should also:

- Clearly state what cookies are used;
- Provide both 'Accept' and 'Decline' buttons on the banner to give users a choice (meaning you can't just have an 'okay' button);
- Allow the user to close or dismiss the banner and continue browsing;
- Include a way for users to manage their cookie preferences (and withdraw consent) at any time.



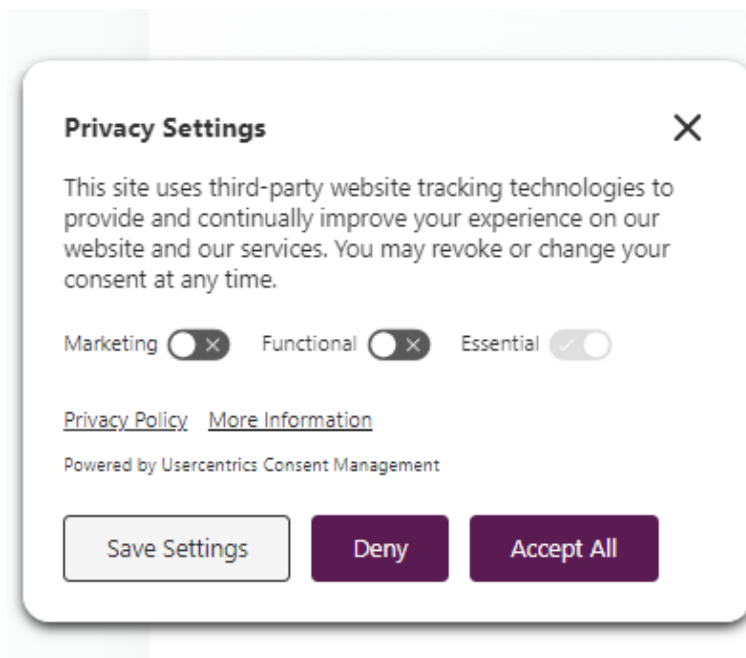
What Should Your Cookie Consent Banner Look Like?

12

WHAT SHOULD A COOKIE BANNER LOOK LIKE

Privacy laws typically are pretty open as to how a Cookie Banner looks in terms of color, shape, size, but the main takeaway is that everything should be easy to see, understand, exit out of, and manage.

This means keeping fonts large, and using contrasting colors so nothing blends in or is hard to see. You should also avoid dark patterns that can trick users into consenting (e.g. a large green “accept” button and a small red “deny” link). Here’s a good example of a cookie consent banner:





Compliance Checklist

13

- ☐ Determine who in your company will be primarily responsible for implementing privacy compliance.
- ☐ Determine what PII you collect by reviewing your website for forms and tracking tools.
- ☐ Determine how you use the PII that you collect. If you have no specific use for the PII or if that PII is not actually useful to you, then stop collecting it.
- ☐ Determine who you share PII with.
- ☐ Determine if you transfer the PII to anyone in other countries.
- ☐ Generate your Privacy Policy at Termageddon.com.
- ☐ Review your Privacy Policy and make sure that you follow it.
- ☐ Use Termageddon to implement a cookie consent banner & Cookie Policy if applicable to your site.
- ☐ Create procedures and train your staff on how to respond to requests from consumers to exercise their privacy rights.
- ☐ Implement security procedures and protocols to reduce the chance of a PII breach.
- ☐ Develop and implement a privacy audit procedure and conduct an annual audit of your privacy practices.
- ☐ Issue ongoing privacy reminders to your staff; Ensure that all of your staff members have signed Non-Disclosure or Confidentiality Agreements.
- ☐ Ensure that it is easy for your customers to exercise their privacy rights by training your staff on how to respond to privacy rights requests.



Thank you for taking the time to read through this Small Business Guide to Privacy! We hope that you found it informative and helpful on your journey towards privacy compliance.

If your business has a website that collects Personally Identifiable Information such as names, emails, or phone numbers, or IP addresses, you are probably already required to have a Privacy Policy by laws that are already in place. In addition, with more and more privacy laws being proposed every day, you also need to have a strategy for keeping your Privacy Policy up to date with these changes.

It is imperative that you comply with privacy requirements not just because failure to do so can mean high fines, and even lawsuits, but also because consumers are increasingly choosing companies that value and respect privacy.

NEED SOME HELP?

If you are in need of a Privacy Policy, Cookie Policy, or Cookie Consent Banner for your website, we hope that you consider [Termageddon.com](https://termageddon.com). We generate all the website policies a small business needs. We're popular among small businesses because we:

- Are founded by a privacy attorney
- Offer an affordable solution (no hidden fees)
- Automatically update all our customers' policies whenever laws change or go into effect
- Provide excellent customer service