The Small Business Guide To Privacy

Created by :

Termageddon

Table of Contents

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 out and we're tracking approximately 30 privacy bills at any given time. 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 at growing rates.

WHY TERMAGEDDON?

Termageddon, LLC is a generator of Privacy Policies, Terms of Service and more for websites and applications. We're founded by a privacy attorney and update our clients' policies whenever the laws change, ensuring that the policies stay up to date. Termageddon is not a law firm and this Guide is not intended to provide legal advice.

Many small business owners have not received a formal introduction to privacy requirements. As such, the best place to start is with a description of the most important concepts.

PRIVACY

"Privacy" is defined as the state or condition of being free from being observed or disturbed by other people. Privacy has also been defined as the right to be left alone.

PERSONALLY IDENTFIABLE 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.

PRIVACY POLICY

A Privacy Policy is a document that describes your privacy practices to anyone that visits your website. It includes the disclosures required by the privacy laws that apply to you. The three primary disclosures all laws share are:

- What PII you collect
- What you do with that PII
- Who you share the PII with

It's important to note that some privacy laws can require **20 or more disclosures** to be included in your Privacy Policy!

COOKIES

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

COOKIE POLICY

A Cookie Policy is a document that explains to website visitors what cookies you use on your website, including their purpose, provenance, and duration. The purpose of the Cookie Policy is to give users all of the information they might need in regard to how their personal data is processed and used by the website in relation to cookies, as well as inform them of their choices regarding cookies.

COOKIE CONSENT BANNER

A cookie consent banner is a popup that goes onto your website that stops certain cookies and trackers from firing (e.g. it stops Google Analytics from tracking the website visitor) until the user consents to those cookies. The cookie consent banner works to comply with applicable privacy laws that require website visitors to consent prior to them being tracked.

How Is PII Collected?

Most modern websites collect PII. Frankly, it's hard for any business -- especially small businesses -- to operate and grow efficiently without collecting PII. Below are some of the most common ways in which PII is collected by small businesses:

FORMS

'Contact Us' forms, registration forms, lead generation forms, and even payment forms are all very common ways in which websites collect PII like names, phone numbers, and email addresses. Since forms require users to submit their information, they're one of the more well-known methods for collecting PII.

NOTE: Collecting PII isn't a bad thing. Website owners just need to be aware of what data is being collected so that they can inform visitors via their website policies.

ANALYTICS TOOLS

Many small business websites use an analytics service such as Google Analytics, which can tell you how many people visited your website per month and how they found your website. In order to work properly, these tools gather IP addresses and keep track of how users interact with a certain website.

DIGITAL ADS

Similar to analytics tools, digital ads that use pixels (e.g. Facebook Pixels) will keep track of user IP addresses and activity to help you measure the performance of your ads.

HOW SMALL BUSINESSES TYPICALLY USE DATA

While there are countless reasons a business could want to collect data, some of the more common reasons are:

- To contact potential customers (phone, email, etc.)
- Newsletter subscriptions (name, email)
- To provide customer support (phone, email, etc.)
- To learn more about customers (IP address)
- To collect payments (name, phone, address, etc.)
- To ship products (name, address)
- To send direct ads/deals (IP address)

NOTE: Sharing Data and Selling Data are not the same thing. While Sharing data is a very common, selling data is rare -- especially for small businesses.

HOW SMALL BUSINESSES TYPICALLY SHARE DATA

Sharing PII is extremely common for small businesses, but many think they don't do it. For example, it's common for businesses to share data with:

- Email marketing vendors (MailChimp, HubSpot, etc,)
- Customer management systems (HubSpot, Salesforce, etc.)
- Content management systems (WordPress, Wix, etc.)
- Parties that need to operate your website (Web developer or designer)
- Shipping services (FedEx, USPS, UPS, etc.)
- Social media/video embeds (YouTube, Facebook, etc.)

WHY ARE COOKIES COLLECTED?

Cookies are commonly placed on user devices as they can be an integral part of surfing the web. For example, websites may use cookies for any of the following purposes:

- Remembering account login information;
- Remembering language preferences;
- Ensuring the security of a website or of sensitive information (e.g. credit card details);
- Remembering what a user added to their cart; and
- Tracking users for analytics and digital ad purposes.

DOES YOUR SITE COLLECT COOKIES?

The easiest way to know if your website uses cookies is to use a scanner. There are several free scanners (we recommend Usercentrics) that will let you know if your website uses cookies.

For small businesses, it's pretty common for websites that use any of the following features to also have cookies:

- Analytics tools like Google Analytics
- Google AdSense
- Digital Ads (Facebook Pixel, Twitter Ads, LinkedIn Insights, Reddit Pixels, etc.)
- eCommerce features (Cart reminders, targeted ads, etc.)
- Account logins

If you look back ten years, the privacy of PII online was of interest only to lawyers, conspiracy theorists, and those in healthcare and banking. So what has changed? Why do small businesses need to start thinking about privacy law compliance?

In 2018, Facebook experienced a leak in which **millions of its users had their PII harvested** by Cambridge Analytica without consent. This changed how consumers think about privacy and kicked off a slew of requirements.

CONSUMERS CARE

In just a few years, online privacy has gone from being something very few people thought about, to almost a competitive advantage for businesses that have good privacy practices.

A study done in 2020 by Transcend called “The Data Privacy Feedback Loop” found that:

- 93% of Americans would switch to a company that prioritizes privacy;
- 91% of Americans would prefer to buy from companies that always guarantee them access to their PII;
- 84% of respondents said that they are open to new state privacy laws;
- 91% of respondents said that the right to delete PII and to know how their PII is used should extend to all U.S. citizens;
- 52% of Americans will not use products or services that they believe have privacy issues.

IT'S THE LAW

The collection of PII also matters because such collection is governed by privacy laws that can start applying as soon as you collect PII. This means that you do not need to share, sell, or even use the PII for certain privacy law requirements to apply to your website. Many laws also can apply to a business regardless of revenue size, employee size, or amount of data collected.

THE LAWS PROTECT CONSUMERS, NOT BUSINESSES

Privacy laws are unique in the sense that they protect consumers, and not businesses. Due to the nature of the Internet, consumers from anywhere can submit their PII to your website, meaning that you may need to comply with the privacy laws of multiple states and countries, even if you are not physically located there.

FINDING WHICH LAWS APPLY TO YOU

There are numerous privacy laws out there with dozens of more bills currently in the works. Therefore, when determining what privacy laws apply to you, the most important factors to consider are:

- Whose PII you are collecting
- Where you do business
- To whom you offer goods or services
- Who you track via cookies, pixels, analytics services, or other tracking technologies
- Many laws apply to businesses regardless of size, employee size, and amount of data collected

CREATING YOUR POLICIES

Most privacy laws have very specific requirements for a website's Privacy Policy and (sometimes) Cookie Consent Banners. Once you determine what laws apply to you, updating your policies accordingly comes next.

CALOPPA HISTORY

CalOPPA was originally enacted in 2003 and was amended in 2013 to address online tracking by requiring Privacy Policies to disclose how that website responds to Do Not Track signals and similar technologies (in addition to numerous other disclosures listed on next page).

According to the California Attorney General, “meaningful Privacy Policy statements safeguard consumers by helping them make informed decisions about which companies they will trust with their personal information”. CalOPPA was enacted to help “foster the continued growth of the Internet economy…by allowing individuals to rely on a Privacy Policy posted online.” The law is meant to reassure consumers who are unsure of doing business online.

WHO NEEDS TO COMPLY WITH CALOPPA?

CalOPPA has an extremely broad reach, potentially applying to any modern website with something as simple as a contact form. CalOPPA applies to an "operator" of a commercial website that collects the PII of consumers residing in California.

The law defines "operator" as any person or entity that owns a website that collects the PII of residents of California where the website is operated for commercial purposes. Even if the operator is located outside of California, the law could still apply to them.

CALOPPA REQUIREMENTS

A CalOPPA-compliant Privacy Policy needs to make the following disclosures:

- Identify the categories of PII that you collect and the categories of third parties with whom you may share the PII;
- Describe the process by which you notify consumers of material changes to your website's Privacy Policy;
- Identify its effective date;
- Disclose how you respond to web browser "do not track" signals or other mechanisms tharp provide consumers the ability to exercise choice regarding the collection of PII about the consumer's online activities over time and across third-party websites, if you engage in such collection;
- Disclose whether other parties may collect PII about consumer's online activities over time and across different websites when a consumer uses your website.

CALOPPA ENFORCEMENT

CalOPPA is enforced by the California Attorney General, who can impose a penalty of **$2,500 per violation** for failure to comply. In this case, "per violation" means per website visitor from California. Even if you have a few dozen California residents visit your website per month, you can see how these fines can add up to a really large amount.

HISTORY OF NEVADA REVISED STATUTES CHAPTER 603A

Nevada Revised Statutes Chapter 603A originally went into effect in 2017, it was amended by SB220, which went into effect on October 1st, 2019 and added additional requirements for Privacy Policy disclosures. The law was again amended by SB260 in June of 2021.

WHO DOES THE NEVADA REVISED STATUTES CHAPTER 603A APPLY TO?

The Nevada privacy law applies to "operators", which are defined as any person who:

- Owns and operates a website for business purposes;
- Collects and maintains the personal information from consumers who reside in Nevada and use or visit the website; and
- Purposefully directs its activities towards Nevada, consummates a transaction with the State of Nevada or a resident of Nevada, purposefully avails itself of the privilege of conducting activities in Nevada or otherwise engages in any activity that constitutes sufficient nexus with Nevada to satisfy the requirements of the U.S. Constitution.

While sufficient nexus can be difficult to define, if you have a website that collects the PII of Nevada consumers and you have customers in Nevada, you need to comply with this privacy law by having a compliant Privacy Policy. Note that your business does not have to be located in Nevada for this law's requirements to apply to you.

NEVADA REVISED STATUTES CHAPTER 603A PRIVACY POLICY REQUIREMENTS

Nevada Revised Statutes Chapter 603A requires you to have a Privacy Policy that makes the following disclosures:

- The categories of PII collected;
- The categories of third parties with whom that PII is shared;
- Whether or not you sell the PII of Nevada consumers;
- A designated request address at which Nevada consumers can submit a request asking you not to sell their PII;
- A description of the process by which you will let users to know of any changes to your Privacy Policy;
- If a third party collects information about the user throughout different websites (cookies); and
- The effective date of your Privacy Policy.

Remember that your Privacy Policy needs to include all of the above disclosures to be compliant or you can face fines.

NEVADA REVISED STATUTES CHAPTER 603A ENFORCEMENT

The Nevada Attorney General enforces this privacy law and can impose penalties of up to **$5,000 per violation**. In this case, “per violation” can mean per website visitor whose privacy rights you infringed upon, meaning that the fines can add up quickly, even if you have only a few website visitors from Nevada per month.

HISTORY OF DOPPA

The Delaware Online Privacy and Protection Act (DOPPA) is a comprehensive law focusing on online and personal privacy. It went into effect in 2016 and actually shares many of the same provisions listed in CalOPPA.

WHO DOES DOPPA APPLY TO?

DOPPA has an extremely broad reach, potentially applying to any modern website with something as simple as a contact form. DOPPA applies to an "operator" of a commercial website that collects the PII of consumers residing in Delaware.

The law defines "operator" as any person or entity that owns a website that collects the PII of residents of Delaware and the website is operated for commercial purposes.

Note: Like many other privacy laws, DOPPA does not discuss where the operator of the website is located. This means that the law can apply to small businesses located outside of Delaware.

DOPPA REQUIREMENTS

A DOPPA-compliant Privacy Policy needs to make the following disclosures:

- Identify the categories of PII that you collect and the categories of third parties with whom you may share the PII;
- Describe the process by which you notify consumers of material changes to your website's Privacy Policy;
- Identify its effective date;
- Disclose how you respond to web browser "do not track" signals or other mechanisms tharp provide consumers the ability to exercise choice regarding the collection of PII about the consumer's online activities over time and across third-party websites, if you engage in such collection;
- Disclose whether other parties may collect PII about consumers' online activities over time and across different websites when a consumer uses your website.

DOPPA ENFORCEMENT

DOPPA is enforced by the Delaware Attorney General, who can impose a penalty of **$2,500 per violation** for failure to comply with this law. In this case, "per violation" means per website visitor from Delaware. Even if you have only a few dozen Delaware residents visit your website per month, you can see how these fines can add up to a really large amount.

HISTORY OF GDPR

The General Data Protection Regulation (GDPR) is a privacy law that went into effect on May 25, 2018, with the goal of protecting the PII of residents of the European Union. It has become arguably the most comprehensive and most frequently enforced privacy law in the world.

WHO DOES GDPR APPLY TO?

You need to comply with GDPR if you:

- Are located in the European Union;
- Offer goods or services, regardless of payment, to European Union residents, regardless of where you are actually located; or
- Monitor the behavior of European Union residents through tracking technologies such as cookies or pixels (i.e. you use an analytics service on your website such as Google Analytics), regardless of where you're located.

GDPR is unique in that it prohibits the processing of PII unless a specific exception (i.e. legal basis) applies. This means that by default, the collection, use, and disclosure of PII of residents of the European Union is not allowed.

There are some exceptions that allow for the collection of PII. For small businesses, the three most common exceptions are:

- The individual has given consent;
- The processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which you are subject.

A GDPR PRIVACY POLICY MUST DISCLOSE:

- List of personal data that is processed;
- The identity and contact details of the controller and, where applicable, of the controller's representative;
- The contact details of the Data Protection Officer, where applicable;
- The purposes of the process for which the personal data is intended;
- The legal basis for the processing;
- Where processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, the legitimate interests pursued;
- The recipients or categories of recipients of the personal data, if any;
- Where applicable, the fact that the controller intends to transfer personal data to a third country or an international organization;
- The period for which the personal data will be stored, or if that is not possible, the criteria used for determining that period;
- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- Where processing is based on consent, the existence of the right to withdraw consent at any time;
- The right to lodge a complaint with a supervisory authority;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary for entering into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such personal data;
- The existence of automated decision-making, including profiling and, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

GDPR ENFORCEMENT

Less severe violations can see fines up to **€10,000,000 or up to 2% of total global annual turnover** for the preceding fiscal year, whichever is higher. Severe violations can see fines up to **€20,000,000 or up to 4% of global annual turnover** for the preceding fiscal year.

HISTORY OF UK DPA

The United Kingdom Data Protection Act (UK DPA) is a key piece of legislation that governs the protection of personal data within the UK. It sets out the framework for data protection law, ensuring that personal information is used fairly, lawfully, and transparently. The Act establishes the rights of individuals regarding their personal data, including access, correction, and the right to be forgotten. It also outlines the obligations of businesses and organizations in handling personal data, such as obtaining valid consent for its use and implementing adequate security measures.

WHO DOES PIPEDA APPLY TO?

While technically not part of the European Union anymore, the United Kingdom has a privacy law, the United Kingdom Data Protection Act 2018. This law is essentially a copy of the GDPR, with the words "European Union" being replaced with "United Kingdom."

UK DPA PRIVACY POLICY REQUIREMENTS

To comply with the UK DPA, you must meet all the Privacy Policy requirements previously listed for GDPR (see page 17).

UK DPA ENFORCEMENT

Less severe violations can see fines **up to £10,000,000 or up to 2% of total global annual turnover** for the preceding fiscal year, whichever is higher. Severe violations can see fines up to **£20,000,000 or up to 4% of global annual turnover** for the preceding fiscal year, whichever is higher.

HISTORY OF PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a privacy law that was enacted to protect the privacy rights of Canadians. PIPEDA achieves this goal by providing Canadians with rights with regard to their personal information, requiring certain websites to have a Privacy Policy and imposing heavy fines for failure to comply.

WHO DOES PIPEDA APPLY TO?

PIPEDA applies to private companies across Canada that collect, use or disclose personal information in the course of a commercial activity. In this case, commercial activity means any transaction, act, or conduct, or any regular course of conduct that is of a commercial character. PIPEDA also applies to all businesses that operate in Canada and handle personal information that crosses provincial or national borders, regardless of the territory in which the business is actually based.

PIPEDA can also apply to businesses that are not based in Canada if there is a real and substantial connection either between the subject matter, the parties, or the territory of Canada. Companies that are located outside of Canada but have clients in Canada or that hold the personal information of Canadians may also need to comply with PIPEDA.

PIPEDA REQUIREMENTS

PIPEDA requires certain websites to have a Privacy Policy. A PIPEDA-compliant Privacy Policy must include the following disclosures:

- The name or title, and the address of the person who is accountable for your privacy policies and practices and to whom complaints or inquiries can be forwarded;
- The means of gaining access to the personal information you hold about Canadians;
- A description of the personal information that you hold and the purposes for which you will use it;
- A copy of any brochures or other information that explain your policies, standards or codes;
- What personal information you share with others, if any;
- Categories of third parties with whom you share the personal information;
- Where you obtain the personal information from;
- How you protect the personal information; and
- Whether you intend to transfer personal information outside of Canada.

PIPEDA ENFORCEMENT

Failure to comply with PIPEDA can lead to **fines of up to $100,000 for each violation**. This means that fines can add up very quickly, even if you have only a few dozen website visitors from Canada per month.

HISTORY OF QUEBEC LAW 25

After much debate regarding whether Canada's federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), offers sufficient privacy protections for consumers, Quebec passed a new privacy law, Quebec Law 25 (previously Quebec Bill 64).

WHO DOES QUEBEC LAW 25 APPLY TO?

Quebec's Law 25 applies to persons who collect, hold, use or share the personal information of residents of Quebec in the course of carrying on an enterprise within the meaning of Article 1525 of the Civil Code. Article 1525 of the Civil Code defines "enterprise" as "the carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service."

This law applies to anyone participating in an economic activity, even if that activity is not commercial, meaning that nonprofit organizations will need to comply with this law, as well as for-profit organizations.

The fact that nonprofit organizations will need to comply with Quebec's new privacy law is an important difference to PIPEDA, which generally applies to organizations that engage in commercial activity. While this means that nonprofit organizations are generally exempt from PIPEDA, they could be subject to PIPEDA if they engage in commercial activities such as the selling, bartering, or leasing of donor lists.

QUEBEC LAW 25 REQUIREMENTS

Quebec's Law 25 also diverges from PIPEDA by requiring the following disclosures to be made in Privacy Policies:

- What PII is collected;
- The purposes for which personal information is being collected;
- The means through which the personal information is being collected;
- The right of access, portability, and rectification of personal information;
- The person's right to withdraw consent to the communication or use of the personal information collected;
- How privacy rights requests can be sent to the organization;
- If personal information is collected using technology that allows the person to be identified, located and profiled, the Privacy Policy must inform the person of the use of such technology and of the means available, if any, to deactivate the functions that allow the person to be identified, located, or profiled;
- If personal information will be used for automated decision making, that fact must be disclosed;
- The possibility that the personal information may be communicated outside of Quebec;
- The title and contact information of the person in charge of the personal information.

QUEBEC LAW 25 ENFORCEMENT

Perhaps the biggest and most important difference between PIPEDA and Quebec's Law 25 is enforcement. Under Quebec's new privacy law, individuals can make a complaint to Quebec's Commission d'acces a l'information. If the individual is not happy with the resolution of the complaint, they can appeal to the Court of Quebec. The penalties for failure to comply are also steep – a maximum of CAD $50,000 in case of an individual violating the law or a maximum of CAD $10,000,000 or, if greater, 2% of the worldwide turnover for the preceding fiscal year in case of an organization violating the law. Lastly, Quebec's Law 25 even allows the prosecutor to institute penal proceedings for violations of the law.

WHO DOES AUSTRALIA PRIVACY ACT 1988 APPLY TO?

This privacy law applies to Australian organizations with an annual turnover of more than AUD $3,000,000. The law defines "organization" as an individual, including a sole trader, a body corporate, a partnership, any other unincorporated association, or a trust.

While this privacy law primarily applies to medium and large businesses due to the revenue requirement, it is important to note that there are a few exceptions which would require small businesses to comply as well. The following Australian small businesses with an annual turnover of AUD $3,000,000 need to comply with this privacy law:

- A private-sector health care provider – an organization that provides a health service and includes:
  - A traditional health care provider (hospital, medical practitioner, or pharmacy);
  - A complimentary therapist, such as a naturopath or a chiropractor;
  - A gym or weight loss clinic;
  - A childcare center, a private school, and a tertiary educational institution.
- A business that sells or purchases personal information;
- A credit reporting body;
- A contracted service provider for an Australian Government contract;
- An employee association registered or recognized under the Fair Work (Registered Organisations) Act 2009;
- A business that has opted-in to the Privacy Act 1988;
- A business that is related to a business that is covered by this privacy law;
- A business prescribed by the Privacy Regulation 2013.

In addition, organizations formed outside of Australia may need to comply with this law, regardless of revenue, if they have an Australian link. Your organization has an Australian link if it carries on business in Australia and collects and holds personal information in Australia.

AUSTRALIA PRIVACY ACT 1988 PRIVACY POLICY REQUIREMENTS

The Australia Privacy Act 1988 requires that an organization's Privacy Policy include the following disclosures:

- Your name and details;
- What kinds of personal information you collect and store;
- How you collect the personal information and where it is stored;
- The reasons why you need to collect the personal information;
- How you will use and disclose the personal information;
- How a consumer can access their personal information or ask for a correction;
- How to lodge a complaint if a consumer believes that their personal information has been mishandled and how you will handle that complaint;
- If you are likely to disclose the consumer's personal information outside of Australia and, if practical, which countries you are likely to disclose it to.

You also need to periodically review your Privacy Policy to ensure that it is accurate and update your Privacy Policy when your practices change.

AUSTRALIA PRIVACY ACT 1988 ENFORCEMENT

The Australia Privacy Act 1988 can impose penalties of **up to AUD $2,100,000** for serious or repeated breaches of privacy.

NOT AN EXTENSIVE LIST

The laws listed on the previous pages are typically the ones that apply to smaller businesses.

That being said even the following laws (that typically only affect big businesses), can apply to small businesses as well in certain circumstances:

- California Privacy Rights Act (CPRA)
- Virginia Consumer Data Protection Act (VCDPA)
- Colorado Privacy Act
- Utah Consumer Privacy Act
- Connecticut SB6

If you do not meet the thresholds of these particular laws (most small businesses do not), it is important to note that the these laws requires controllers to ensure that processors of personal data adhere to the requirements of the law.

So, if you are processing data on behalf of a client that is subject to these laws, you may be required, **via contract**, to meet the obligations of these laws even if they don't apply to you via statute.

ABOUT THE ePRIVACY DIRECTIVE

Also called the "Cookie Law," the ePrivacy Directive 2002 requires European Union Countries to create laws that state that websites need to provide information about cookies and tracking technologies and obtain the consent of users before putting such cookies or technologies on their devices. The laws passed by EU countries under this Directive protect the privacy of residents of the European Union so they can apply to websites of businesses outside of the EU.

NOTE: The ePrivacy Directive will soon be replaced by the ePrivacy Regulation 2021, which, when finalized, will update these rules.

ABOUT GDPR

The General Data Protection Regulation (GDPR) is a privacy law that went into effect on May 25, 2018, with the goal of protecting the PII of residents of the European Union. It has become arguably the most comprehensive and most frequently enforced privacy law in the world.

GDPR'S COOKIE REQUIREMENTS

General Data Protection Regulation (GDPR): requires the consent of website users for the collection of personal data, which includes the data collected by certain types of cookies. GDPR applies to you if you:

- Have an establishment in the European Union;
- Offer goods or services to European Union residents, regardless of your location;
- Monitor the behavior of European Union residents, regardless of your location.

ABOUT THE UK DPA

The United Kingdom Data Protection Act (UK DPA) is a key piece of legislation that governs the protection of personal data within the UK. It sets out the framework for data protection law, ensuring that personal information is used fairly, lawfully, and transparently. The Act establishes the rights of individuals regarding their personal data, including access, correction, and the right to be forgotten. It also outlines the obligations of businesses and organizations in handling personal data, such as obtaining valid consent for its use and implementing adequate security measures.

UK DPA'S COOKIE REQUIREMENTS

United Kingdom's Data Protection Act 2018 (UK DPA): requires the consent of website users for the collection of personal data, which includes the data collected by certain types of cookies. UK DPA applies to you if you:

- Have an establishment in the United Kingdom;
- Offer goods or services to United Kingdom residents, regardless your location;
- Monitor the behavior of United Kingdom residents, regardless of your location.

ABOUT CPRA

The California Privacy Rights Act (CPRA) was approved in 2020 and replaced the California Consumer Rights Act (CCPA).

CPRA'S COOKIE REQUIREMENTS

CPRA requires websites that sell personal information to provide users with a means to opt out of such sales. This is usually done through the cookie consent banner that asks users whether they would like to opt out of sales of their personal information. CPRA applies to for-profit entities that collect and process the personal information of California consumers, that do business in California and that meet one of the following thresholds:

- Has annual gross revenues in excess of $25,000,000;
- Annually buys, receives, sells or shares the personal information of 50,000 or more California consumers, households or devices;
- Derives 50% or more of its annual revenue from selling the personal information of California consumers.

ABOUT PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a privacy law that was enacted to protect the privacy rights of Canadians. PIPEDA achieves this goal by providing Canadians with rights with regard to their personal information, requiring certain websites to have a Privacy Policy and imposing heavy fines for failure to comply. In this Compliance Guide, we will discuss the following as it relates to PIPEDA:

PIPEDA'S COOKIE REQUIREMENTS

PIPEDA requires website users to consent prior to the collection of personal data, which can be defined as the data that is collected through cookies and other tracking technologies. PIPEDA applies to private companies across Canada that collect, use or disclose personal information in the course of a commercial activity. In addition, PIPEDA can also apply to businesses outside of Canada if they collect the personal information of Canadians in the course of a commercial activity.

ABOUT QUEBEC LAW 25

After much debate regarding whether Canada's federal privacy bill, the Personal Information Protection and Electronic Documents Act (PIPEDA), offers sufficient privacy protections for consumers, Quebec passed a new privacy law, Quebec Law 25 (previously Quebec Bill 64). While the text of Quebec's Law 25 has not been officially made available, we were able to obtain a copy and, in this article, we will discuss who this new law applies to and how it will affect your business.

QUEBEC LAW 25'S COOKIE REQUIREMENTS

Quebec's Law 25 applies to persons who collect, hold, use or share personal information in the course of carrying on an enterprise within the meaning of Article 1525 of the Civil Code. Article 1525 of the Civil Code defines "enterprise" as "the carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service." This new law will apply to anyone participating in an economic activity, even if that activity is not commercial, meaning that nonprofit organizations will need to comply with this law, as well as for-profit organizations.

MORE LAWS INCOMING

Since the U.S. federal government has not passed a privacy law and it is unlikely that it will do so in the future, states have taken it upon themselves to protect the privacy of individuals online. As such, there are now over a dozen proposed privacy bills in the U.S. as well as globally.

NOTE: Six new laws went into effect in 2023, with another three scheduled to go live in 2024.

While each of these bills are different, there are some important clauses that you should be aware of:

- The bills would apply outside of the state/country in which they are passed;
- Most of the bills would apply to small businesses, while some would apply to large businesses only;
- All of the bills would require websites to have a Privacy Policy that contains specific disclosures; and
- Some of the bills would allow consumers to sue businesses directly for violations.

Regulations, guidance, and enforcement actions can also affect Privacy Policy requirements.

Due to these proposed bills, you don't just need a Privacy Policy that complies with privacy laws of today, you also need a Privacy Policy that keeps up to date with the privacy laws of tomorrow.

NOTE: For a full list of the bills we're tracking, visit https://termageddon.com/global-privacy-bill-tracker/

WHERE SHOULD A PRIVACY POLICY BE LOCATED?

First and foremost, a Privacy Policy should be easy to find on your website. It shouldn't be hidden behind any 'legal' or 'policies' links in the footer. It's best practice (and required by some laws) to clearly write out the name of the policy and link directly to it (like the example below):

> **NOTE:** Some privacy laws require upwards of **20 different disclosures** in order for your Privacy Policy to be compliant with that law.

WHAT SHOULD A PRIVACY POLICY INCLUDE?

There are three main disclosures every Privacy Policy must make:

- What PII is collected;
- How that PII is used; and
- Who it is shared with.

Unfortunately for those who write Privacy Policies, the above three disclosures are not sufficient to have a compliant Privacy Policy under most laws, and the disclosures can become very lengthy, depending on what privacy laws apply to your website. The process requires a website owner to:

Step 1: Understand what PII your website collects.
Step 2: Determine which privacy laws apply to your website.
Step 3: Include the necessary disclosures from each privacy law.
Step 4: Come up with a strategy to keep the Privacy Policy up-to-date as privacy laws change.

WHAT SHOULD A COOKIE BANNER INCLUDE?

A Cookie Banner should be easily seen as soon as someone enters your website for the first time. It should also:

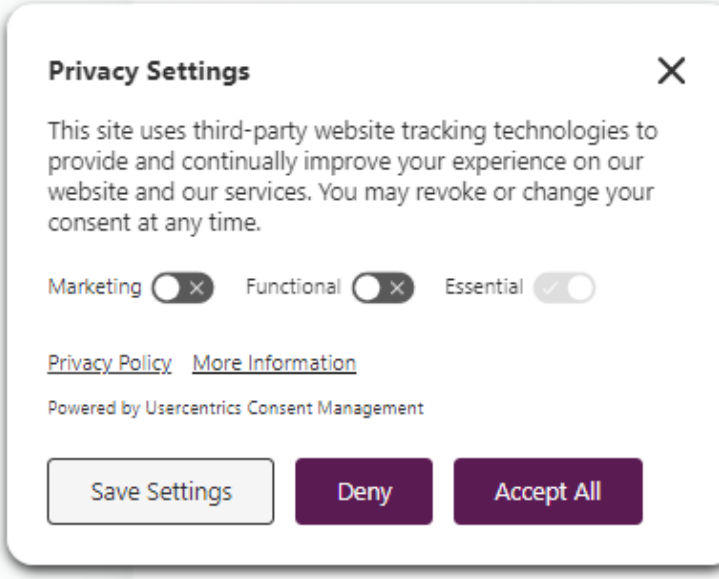
- Clearly state what cookies are used;
- Provide both 'Accept' and 'Decline' buttons on the banner to give users a choice (meaning you can't just have an 'okay' button);
- Allow the user to close or dismiss the banner and continue browsing;
- Include a way for users to manage their cookie preferences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

NOTE: CPRA requires a different cookie consent banner layout that allows individuals to opt out of the sale of their personal information.

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. Here's a good example of a Cookie Consent Banner:



- [ ] 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 either creating a privacy rights portal or providing your contact information in your Privacy Policy.

THANK YOU!

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. 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