THE SMALL BUSINESS GUIDE TO PRIVACY

CREATED BY:
TERMAGEDDON.COM

ABOUT THE **SMALL BUSINESS GUIDE TO PRIVACY**

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 so that you no longer have to sift through mountains of documents to figure out your obligations and responsibilities.

In this guide, we will discuss the privacy laws that can apply to small businesses, their requirements, the future of privacy obligations, consumer views towards privacy, and the penalties for violations of privacy laws. We will also provide a checklist that can help streamline your compliance efforts.

By the end of reading this guide, you will be able to determine what privacy laws apply to you and what your responsibilities are. This will allow you to focus your efforts on improving compliance and on bettering your business' privacy efforts.

This Small Business Guide to Privacy was written by Donata Stroink-Skillrud of Termageddon, LLC. Donata is a privacy and technology attorney and a Certified Information Privacy Professional. She is the President of Termageddon, responsible for the questionnaires and the text and variations of policies and for keeping policies up to date with changing laws.

Donata is the Vice-Chair of the American Bar Association's ePrivacy Committee and the Chair of the Chicago Chapter of the International Association of Privacy Professionals. Donata has taught classes at the Illinois State Bar Association on the General Data Protection Regulation (GDPR) to other attorneys.

Termageddon, LLC is a generator of Privacy Policies, Terms of Service and more for websites and applications. They update their 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. You should speak to your attorney prior to implementing any compliance solutions.

IMPORTANT TERMS

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.

First, the term "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. The individual's right to privacy has been spelled out in the constitutions of certain states and countries. Meanwhile, others regulate this privacy via laws that protect the privacy of consumers online.

Second, Personally Identifiable Information (PII) is any information that could identify someone or any information that relates to an identifiable person. Examples of PII include:

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

Note that PII may also be referred to as "personal information" or "personal data."

Small business websites usually collect PII through the following means:

- Contact us forms;
- Email newsletter sign up forms;
- Account creation portals; and
- Analytics programs.

If your website has any of the above features, you are collecting PII and thus may be required by law to have a Privacy Policy.

Lastly, a Privacy Policy is a document that describes your privacy practices to anyone that visits your website. While it can and may be required to make many other disclosures, the main portions of the Privacy Policy disclose the following information:

- What PII you collect;
- What you do with that PII; and
- Who you share the PII with.

HOW SMALL BUSINESS WEBSITES COLLECT PII

On the right-hand side of this page, you can see an example of a contact us form. This type of form is extremely common on small business websites. This particular form collects the following PII:

- Name; and
- Email.

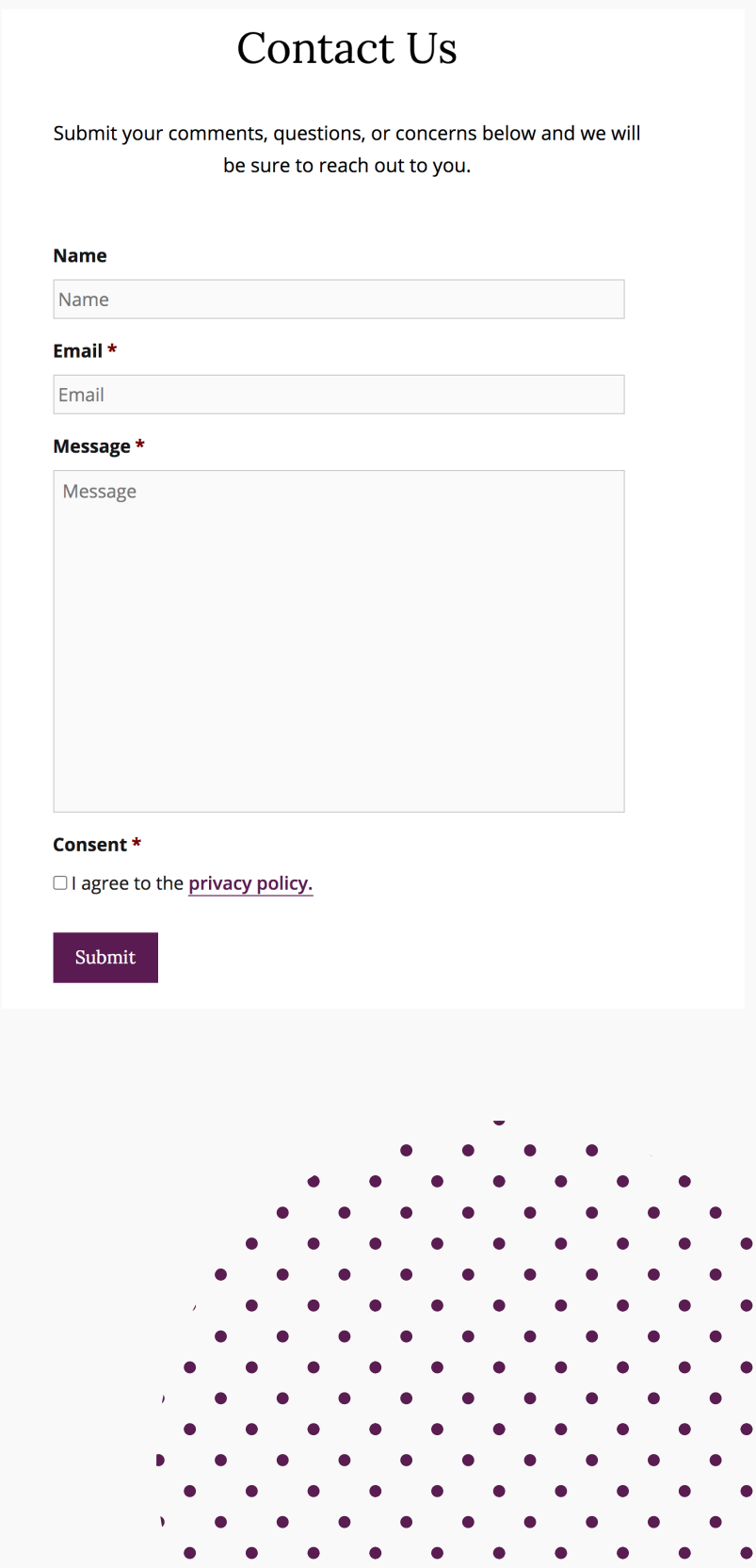
It is very common for businesses to share the PII collected by these forms with the following third parties:

- Email marketing vendors (if you upload the consumers' PII to a service such as MailChimp or Constant Contact to send them email newsletters);
- Customer management systems (if you upload the information onto HubSpot, SalesForce, or similar service);
- Parties that need to operate the website (if your website developer can access the information while performing maintenance or building new features);
- Content management systems (if you use a system such as WordPress or Wix for your website, that system can gain access to the PII submitted through your website.

Lastly, 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. If you have analytics installed, you will be collecting:

- IP addresses; and
- Information on how users interact with your website.

It is thus imperative that your Privacy Policy discloses that you use analytics programs and the PII that you collect through such programs.



WHY DOES THE COLLECTION OF PII MATTER?

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 truth, we need to "thank" Facebook and Cambridge Analytica for this slew of requirements and changes. In 2018, reports starting coming out that there was a PII leak in which millions of Facebook users' PII was harvested by Cambridge Analytica without consent. The company then used this PII for political advertising. The scandal was a big deal not just because millions had their privacy violated, but also because it caused consumers to consider the privacy of their PII online.

Quite understandably, consumers were upset about this event and started pressuring their legislators to create privacy laws that would prevent another such scandal. Fast forward to now and we have several privacy laws in place that govern websites that collect PII and many more are being considered.

The collection of PII matters for two reasons: one, consumers care about their privacy and failing to dispel their fears could cause you to lose business. Two, privacy laws govern the collection of PII online and failing to comply with these privacy laws could cause you to be fined or sued.

First, let's discuss the consumer views towards privacy and towards businesses that do not respect their privacy rights. The following study results show that consumer attitudes towards privacy have changed from the recent past:

- 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;
- 55% of Americans want privacy laws.

It is clear that consumers care about privacy and that they are willing to vote with their dollars for companies that prioritize privacy. Demonstrating that you are willing to follow privacy laws can go a long way towards retaining your existing customers and can even gain you new customers as well.

1. https://thedigitalstandard.org/downloads/CR_PrivacyFrontAndCenter_102020_vf.pdf?fbclid=IwAR2O9bVoBXZUaoSEBQfJqlo5be8-kG9-VLM5cKmwc6szCJ0Cey2dT9L5tHw
2. https://bit.ly/3kKFqm0
3. https://www.prnewswire.com/news-releases/kpmg-survey-american-consumers-want-more-control-visibility-into-how-companies-use-their-personal-data-301102131.html

WHY DOES THE COLLECTION OF PII MATTER?

In addition to the consumer views towards privacy, the collection of PII matters because such collection is governed by privacy laws.

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

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; and
- Who you track online via cookies, pixels, analytics services or other tracking technologies.

In this guide, we will discuss the following major privacy laws that can apply to small businesses:

- California Online Privacy and Protection Act of 2003 (CalOPPA);
- California Consumer Privacy Act (CCPA);
- Nevada Revised Statutes Chapter 603A;
- Delaware Online Privacy and Protection Act (DOPPA);
- General Data Protection Regulation (GDPR); and
- Personal Information Protection and Electronic Documents Act (PIPEDA).

Note that other countries such as Australia or South Africa have their own privacy laws as well. However, the privacy laws listed above are the ones most relevant for businesses based in the United States, Canada, and the European Union.

We will also discuss the following important points of each of these laws:

- Who the law applies to;
- What rights the law provides to consumers;
- Privacy Policy requirements; and
- Penalties for failing to comply.

PRIVACY LAWS THAT CAN APPLY TO YOU: CALOPPA

CALIFORNIA ONLINE PRIVACY AND PROTECTION ACT 2003 (CalOPPA)

California is a state that has a deep-rooted respect for privacy by the legislature. In fact, California's Constitution includes an inalienable right to privacy to each resident of the State. It thus should come as no surprise that California was the first state in the United States to pass a privacy law governing business websites by requiring them to have a Privacy Policy.

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 PII." CalOPPA was enacted to reassure consumers who were unsure of doing business online, thereby growing the Internet economy.

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.

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.

Note that CalOPPA does not discuss where the operator of the website is located. This means that the law is so broad that it can apply to you regardless of where you are located, in California or elsewhere. If you website has a contact form that could be collecting the PII of California consumers, you will need to have a CalOPPA compliant Privacy Policy.

CalOPPA also requires operators to "conspicuously post" the Privacy Policy on their website so, if your Privacy Policy is hidden behind multiple pages or cannot be easily seen on your footer, you may be in violation of this law.

CalOPPA is enforced by the California 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 California. Even if you have only a few dozen California residents visit your website per month, you can see how these fines can add up to a really large amount.

PRIVACY LAWS THAT CAN APPLY TO YOU: CCPA

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

The CCPA is a relatively new law which went into effect on January 1st, 2020 and became enforceable on July 1st, 2020. It is one of the most comprehensive privacy laws in the United States.

Like most privacy laws, the CCPA has a very broad application in that it can apply to businesses outside of California, reflecting the fact that consumers can submit their PII to websites all over the world. The CCPA applies to for-profit entities that collect the PII of California consumers, that do business in California and meet one or more of the following thresholds:

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

As the management of vendors and service providers is crucial to CCPA compliance, it is important to note that your larger clients may require you to comply with this law by via contract, even if your business is too small to meet the requirements above.

If you do need to be compliant with this law, you are required to have a Privacy Policy that makes certain disclosures or you could be fined or even sued.

The goal of the CCPA is to provide California residents with more control over their personal information by giving them the following privacy rights:

- The right to know what PII is collected about them;
- The right to know whether their PII is sold or disclosed and to whom;
- The right to say no to the sale of their PII;
- The right to access the PII that a business holds about them; and
- The right to equal service and price, even if they exercise their privacy rights.

It is important to note that the CCPA includes a right to be fully informed about a company's privacy practices, which means that websites that need to comply with this law need to have a Privacy Policy that makes all of the required disclosures.

Fines for non-compliance with the CCPA are $2,500 per violation or $7,500 per intentional violation. In this case, per violation means per consumers whose privacy rights you infringed upon. Therefore, the fines can add up quickly.

It is also important to note that the CCPA allows consumers to sue businesses directly for breaches of their PII. We have already seen multiple lawsuits arguing that the sharing of PII with parties not disclosed in the Privacy Policy is a breach and thus a cause to sue. This further highlights the importance of a complete and accurate Privacy Policy.

PRIVACY LAWS THAT CAN APPLY TO YOU: NEVADA

NEVADA REVISED STATUTES CHAPTER 603A

When it comes to determining what laws require websites to have a Privacy Policy, most people are surprised to learn that Nevada has a privacy law that governs the collection of PII by websites. Nevada Revised Statutes Chapter 603A, like many other privacy laws, has a broad reach and can apply to businesses outside of Nevada, has unique requirements for what a Privacy Policy must contain and imposes heavy penalties for not meeting those requirements. Nevada's privacy law was amended in late 2019, requiring businesses to disclose whether they sell PII.

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 PII of residents of Nevada through that website; and
- Purposefully directs its activities towards Nevada, enters into 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 it can be difficult to define "sufficient nexus", a good rule to keep in mind is that if you have customers in Nevada, then you need to comply with this law.

The Nevada privacy law requires websites to have a Privacy Policy that makes very specific disclosures.

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

PRIVACY LAWS THAT CAN APPLY TO YOU: DELAWARE

DELAWARE ONLINE PRIVACY AND PROTECTION ACT (DOPPA)

DOPPA was enacted to protect the privacy of residents of Delaware online. It is important to note that DOPPA is very similar to CalOPPA and most of the provisions of both of these laws are virtually the same.

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 that DOPPA does not discuss where the operator of the website is located. This means that the law is so broad that it can apply to you regardless of where you are located, in Delaware or elsewhere. If you website has a contact form that could be collecting the PII of Delaware consumers, you will need to have a DOPPA compliant Privacy Policy.

DOPPA also requires operators to "conspicuously post" the Privacy Policy on their website.

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.

PRIVACY LAWS THAT CAN APPLY TO YOU: EUROPEAN UNION

GENERAL DATA PROTECTION REGULATION (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. As arguably the most comprehensive and most frequently enforced privacy law in the world, GDPR provides extensive privacy rights to consumers, requires websites to have a Privacy Policy that makes specific disclosures and has a broad application, applying to certain websites all over the world.

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 are actually located.

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

However, the following exceptions do allow for the collection of PII:

- 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;
- Processing is necessary to protect the vital interest of the individual or of another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in you; and
- Processing is necessary for the purposes of legitimate interests pursued by you or by a third party.

When it comes to small business websites, PII is usually processed under the consent, contract or legal obligation exceptions. If you are allowed to process PII under one of the above exceptions, you need to ensure that your Privacy Policy clearly states which exceptions you are using.

PRIVACY LAWS THAT CAN APPLY TO YOU: EUROPEAN UNION

GENERAL DATA PROTECTION REGULATION (GDPR) (Cont.)

GDPR ensures the protection of PII by providing residents of the European Union with the following privacy rights:

- Right to transparent information: websites are required to have a Privacy Policy that makes the specified disclosures;
- Right of access: the individual has the right to know whether his or her PII is being processed and to receive additional context on what is done with that PII;
- Right to rectification: the individual has the right to correct the PII that a business holds on him or her that is incorrect and complete the PII that is incomplete;
- Right to erasure: the individual has the right to have his or her PII erased;
- Right to restriction of processing: the individual has the right to have his or her PII be processed for specific purposes only;
- Right to portability: the individual has the right to receive all of the PII that a business holds about them and the right to have that PII sent to a different business; and
- Right to object to automated decision-making, including profiling - the individual has the right to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning that individual.

GDPR is one of the most heavily enforced privacy laws in the world, imposing heavy fines for not honoring the privacy rights of individuals, not having a compliant Privacy Policy, failing to properly process PII and more.

For less severe violations, businesses can be fined up to €10,000,000 or up to 2% of annual turnover, whichever is higher. Especially severe violations can garner fines of up to €20,000,000 or up to 4% of annual turnover, whichever is higher. With hundreds of fines already levied on businesses both large and small, compliance with this privacy law is crucial to get correctly.

PRIVACY LAWS THAT CAN APPLY TO YOU: CANADA

PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

PIPEDA is a privacy law that was enacted to protect the privacy of Canadians. PIPEDA achieves this goal by providing Canadians with rights with regard to their PII, requiring certain websites to have a Privacy Policy, and imposing heavy fines for failure to comply.

PIPEDA applies to private sector companies across Canada that collect, use or disclosure PII 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 PII that crosses provincial or national borders, regardless of the territory or province 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 PII of Canadians may also need to comply with PIPEDA.

PIPEDA aims to protect the PII of Canadians by providing them with the following privacy rights:

- The right to access the PII that a business has collected about them;
- The right to request that the business amend any of the PII collect about that person;
- The right to withdraw consent to the processing of their PII; and
- The right to lodge a complaint regarding the processing of their PII.

If PIPEDA applies to you, then you need to respect the above privacy rights and you are also required to have a Privacy Policy that contains all of the disclosures required by this law.

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

THE FUTURE OF PRIVACY LAW REQUIREMENTS

Now that you have a better understanding of the various privacy laws that may apply to your website and their requirements, it is time to look at the future of privacy.

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 23 proposed privacy bills in the US (see the chart on the next page for a breakdown of these bills.

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 states 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.

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.

For more information on the privacy bills that have been proposed in the United States, please visit: https://termageddon.com/potential-new-privacy-laws-in-the-us/.

PROPOSED STATE PRIVACY BILLS

State	Bill Citation	Bill Name	Privacy Policy changes	Business size limit	Consumers can sue	Right to access data	Right to delete data	Right to correct data	Right to restrict processing	Right to opt out	Opt-in consent required	Right to portability	Against automated decision making	Imposes fiduciary duty	Prohibits discrimination	Right to be forgotten
California	A2414		x								x					
Hawaii	SB 418	N/A	x			x	x			x		x			x	
Illinois	SB2330	Data Transparency and Privacy Act	x	x		x	x	x		x					x	
Illinois	SB2263	Data Privacy Act	x	x		x	x	x		x		x				
Illinois	HB5603	Consumer Privacy Act	x	x		x	x			x		x			x	
Massachusetts	SD 341/S 120	Consumer Data Privacy Act	x	x	x	x	x			x		x			x	
Nebraska	LB746	Nebraska Consumer Data Privacy Act	x	x		x	x			x					x	
New York	S5642	New York Privacy Act	x		x	x	x	x	x	x		x	x	x		
New York	S224	The Right to Know Act of 2019	x			x						x				
New York	S2293	N/A	x													
New York	S2323	Online Consumer Protection Act	x							x	x					
New York	A7736	It's Your Data Act	x	x	x	x	x			x	x	x		x	x	
New York	A6351	N/A	x	x	x	x				x					x	
New Jersey	A2188	N/A	x			x				x						x
New Jersey	A3255	N/A	x	x	x	x	x			x	x	x			x	
New Jersey	A1181	N/A	x													
New Jersey	SB1257	Online Personally Identifiable Information Disclosure	x			x		x		x					x	
New Jersey	A3283	New Jersey Disclosure and Accountability Transparency Act	x			x	x	x	x	x	x	x	x			
New Hampshire	HB1680		x	x		x	x			x		x			x	
Pennsylvania	H1049	Consumer Data Privacy Act	x	x		x	x			x					x	
Rhode Island	S2430	Consumer Privacy Protection Act	x	x		x	x			x		x			x	
South Carolina	H4812	Sourth Carolina Biometric Data Privacy Act	x		x	x	x			x	x				x	
Vermont	VTH899		x													

PRIVACY COMPLIANCE CHECKLIST

Implementing privacy compliance can be a daunting task. Use the checklist below to help you get started:

- 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. We'll keep an eye out on privacy laws and bills for you and will notify you and update your Privacy Policy whenever existing privacy laws change or new privacy laws or regulations are implemented;
- Review your Privacy Policy and make sure that you follow it;
- Implement a cookie consent banner if you are required to do so;
- 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, 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.

If you are in need of a Privacy Policy solution for your website, we hope that you consider Termageddon.com. We generate Privacy Policies and will automatically update your policy when new laws are enacted, ensuring that your policy is always up to date.