Writing Your Ecommerce Privacy Policy

Author : lauren-shufran

Categories : Building Your Ecommerce Website

Here's a fundamental fact: As an ecommerce business, you *cannot* operate without collecting data about your customers. This includes the information required to complete basic transactions—customers' home addresses, credit card or bank details, phone numbers, account passwords, purchase histories. It includes *other* information you collect directly from visitors—email addresses through opt-in forms, for example. But as we've just discussed, it includes more than the data you collect to *execute transactions*; it *also* includes the data you collect to improve user experience, optimize your online offerings, and serve up personalized ads.

Gathering *that* data requires monitoring IP addresses, browser clicks, page views, in-site navigation, ad interactions—all the *indirectly-provided* data that your ecommerce platform and supplemental analytics tools collect. It includes the browsing histories stored by browser cookies. It includes all the data your commerce platform's software integrations (live chat, email campaigns, etc.) collect and manage. And more.

Ultimately, that's a lot of information. And while it's terrific for your business to *have* that wealth of intelligence about your target market, it also means you've got a lot to write down for your site visitors... because they need to know exactly what you're collecting on them. Remember, *individuals own their personal data*. As a business that collects, processes, and manages it, you must disclose what you're doing with the information that *they* own. This is one of the reasons a privacy policy is so important.

What *is* a Privacy Policy?

A privacy policy is a legal document that gives site visitors information about how a business collects and manages personal and sensitive data ("personally identifiable information") about its visitors and customers. Broadly, it covers the topics of collection, use, confidentiality, and security. More *specifically*, it covers:

- exactly *what* information your website (and third-party providers) collects about visitors and customers—including whether cookies or other tracking software are used
- *why* you collect it (what specific purposes that data is used for)
- *how* that data is used—including under what conditions it might be shared or disclosed
- how it's stored and what measures are in place to protect it
- how users can access, review, or contest the accuracy of the collected information
- how users can opt *out* of data collection or distribution if they so wish

The privacy policy is typically regarded as a subsection of a website's Terms & Conditions, though it should be offered as a standalone agreement. (You can then incorporate it *into*, or link to it *from*, your T&C). Burying your privacy policy in your T&C exposes you to the risk of angry consumers claiming they didn't see it. What's more—depending on where you're doing business—you might be legally required to keep it separate. According to the California Online Privacy Protection Act (CalOPPA), for example, the hyperlink to a site's privacy policy must contain the word "privacy," in effect necessitating a separate resource. In Australia, the privacy policy must "only include information that is relevant to the way your entity handles personal information," which means you'll need a separate T&C for other matters you need to cover.

Why Do I Need a Privacy Policy?

As is the case with your Returns & Refunds policy, there are both *business* and *legal* reasons for having a privacy policy. The business case is simple enough. For one, it promotes transparency and evokes trust in your visitors and prospects. When you *don't* have this policy on display, prospects may become suspicious about doing business with you and move on to your competitors, who may be more willing to disclose. Online consumers have every right—*especially* in the wake of recent data breaches—to be concerned about the safety and security of their information. It's in your business's best interest to demonstrate your commitment to their security.

What's more, Google requires you to post a privacy policy if you don't want to be penalized in search results. And some third-party platforms you might integrate with (your payment gateway, for example) will require you to have a privacy policy in place before they approve or connect you.

The other reasons you need a privacy policy are legal in nature. It protects you from potential lawsuits: If a customer tries to sue your ecommerce site, you'll be able to show that you had an accessible policy in place that disclosed what you do with customer information. And consider this: In May 2018, the European Union's General Data Protection Regulation (GDPR) went into effect. It introduced unprecedented levels of privacy protection for EU residents, and harsher penalties for violators than any other privacy law out there. And if your online shop offers goods to residents of the EU—*or if your site collects data on EU citizens as they navigate*—you must comply with the GDPR.

That said, familiarize yourself with privacy laws in the jurisdictions where your business is located and your site users live. As a consumer *yourself*, you can probably intuit the more fundamental requirements: that data should only be collected for limited (and lawful) purposes; that it should not be kept for longer than necessary; that users must be able to opt out of sharing data with you; that strong security measures must be put in place to protect the data; that you have a response plan in place in the event of a security breach; and so on. But there may be features specific to your jurisdiction/s that you'll have to adhere to. (Note: If your privacy policy satisfies the requirements of the GDPR, you're *probably* in compliance with most other privacy laws.)

The purpose of this document is to offer some general information about what your ecommerce privacy policy will need to cover, along with some examples. We *highly* recommend you seek legal advice in creating your own policy. There's a world of "privacy policy generators" out there; and while they might be valuable to play with to get a fuller sense of what a policy entails, we don't suggest you generate your policy with one. An experienced attorney will help you develop a policy that accurately reflects *your* business's relationship with consumer data. There's an expense to consider; but you *can* keep costs down if you use a generator (and the policies of businesses similar to yours) to create an initial draft, and then have a legal professional review it. This way, you'll ensure you're in line with government regulations and better shielded from legal liabilities in the long term. A boilerplate privacy policy is not necessarily going to protect you.

Finally, drafting your own privacy policy lets you grasp the totality of the personal data your company controls. It's a valuable exercise insofar as it prompts you to keep considering how you can put the data you're collecting to best use.

What Should My Ecommerce Privacy Policy Include?

According to the GDPR, individuals have eight rights over their personal data:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict data processing
- the right to data portability, the right to object
- rights in relation to automated decision-making.

Not all of these rights will apply to your ecommerce site, but you should familiarize yourself with them. The ones that *do* apply should be spelled out clearly in your privacy policy—and by "spelled out," we mean you need to describe both what these rights *entail*, and how visitors can *exercise* them.

The U.S. Better Business Bureau has its own "five core principles of privacy protection":

- notice/awareness
- choice/consent
- access/participation
- integrity/security
- enforcement/redress

These categories may be useful in helping you structure your policy—or at least in ensuring you cover all your bases. If you look at the policies of other businesses in your industry (and you

should!), you'll notice pretty quickly that they're not all structured the same. There's no particular order in which information has to be presented; what matters is that you cover all potential concerns consumers may have about their privacy while doing business with you. But you *will* begin to notice some patterns. Consider these patterns the norms for your industry, and use them as a starting point.

You might open your privacy policy with a brief statement about who your company is, including your business' legal name and address. You might open it by describing the purpose of the document and offering a summary of what it will cover. You might open it with a statement of intent to respect and protect visitors' and customers' privacy. ("Your privacy is important to us! We promise not to sell, misuse, or otherwise exploit any information you provide to us.") None of these is mandatory, but they each play a role: immediate transparency in providing contact information, the organization of information for better user experience, putting readers at ease up-front by prioritizing their security. Verve Coffee opens with a summary, while Bridge & Burn puts visitors immediately at ease:

Zappos—a bigger company that needed to update its privacy policy as it grew—opens the document with its legal business name, the date on which its policy was last updated, and links to previous iterations of the policy. (You'll want to state somewhere in your document the date on which your policy took effect):

Finally, you might open your policy with your company's principles for processing data. We'll call this "the ethical approach." Article 5 of the GDPR contains six principles according to which all personal data must be processed; perhaps you'll acknowledge these in your policy. Or perhaps you'll take a more personalized approach, listing *your* core beliefs about privacy, as Bibi's Bakery does:

Again, your opening content will be a matter of personal choice. The suggestions we've given above can be inserted anywhere in your policy; you'll determine which of them are important for you. Meanwhile, here are the questions your privacy policy *must* answer:

What personally identifiable information are you collecting and processing?

Email addresses, shipping addresses, credit card numbers, bank details, birth dates, phone numbers, IP addresses, login passwords, purchase history, date and time of site access, session duration, page views, product views, referring site, device used... the list of data you might be collecting is long. Regardless of how long your list is, you need a list.

The GDPR's definition of "personal data" is broad enough that you might consider breaking down the data you collect into two different types: "data you provide to us" and "data our website collects," or *directly provided* and *indirectly provided* data. Carbon38 breaks its data down into *three* categories (data users provide to the company, data users post publicly, and data the company's website collects automatically):

Kissmetrics itemizes the data it collects in a bullet-pointed, user-friendly format:

Depending on the complexities of your ecommerce site, you might categorize the data by collection *methods* (what data you collect when a customer makes a purchase; what data you collect when they send a message through a contact form; what data you collect when they create an account). The benefit of categorizing by method is it gives you the opportunity to describe how you treat data *differently* depending on the transaction—for instance, you might delete the data collected through a contact form once the query is answered, but you'll hold on to the data collected through account creation until the customer closes their account with you.

If you use Google Analytics or AdSense, notify your users. (Google requires it.) Take a look at any plugins and third-party integrations you have, and review *their* privacy policies. (Perhaps you'll link out to their policies from *yours* to cover your bases.) Describe how each tool collects information, and what it collects. Do the ad scripts running on your site collect demographic information? Do your social media integrations collect data on users' followers? Do your commenting plugins collect and store commenters' data? And so on.

Consider a separate paragraph or section for your cookie policy. If data is being saved into a visitor's web browser—whether to customize their site experience, track their browsing habits, make it easier for them to login, remember what products they added to their shopping cart, or so you can serve them up personalized ads—users need to know. (You should also let users know that if they *opt out* of tracking cookies, these features may no longer be available to them.) Of course, check the laws in your jurisdiction to find out if you need informed consent *before* you can place cookies on users' devices. Here's the separate cookie clause at York Athletics Mfg.:

Why are you collecting and processing that data?

You collect data for a variety of reasons—all of which, of course, need to be legally justifiable. As an eCommerce site, your legal bases for collecting information probably fall into one of these categories:

- consent (when, for example, users subscribe to your email)
- contractual necessity (when you can't process their transaction *without* payment data)
- legitimate interests (when you keep their email addresses to follow up with products they might be interested in after they've placed an order with you)
- compliance with a legal obligation (when you suspect a fraudulent transaction)

Of course, you don't have to use these legal terms in your privacy policy—we'd actually advise *against* it, since by law, your policy *also* has to be readable! Just make sure each of your "whys" falls into one of those four categories. Your reasons will probably include some (or all) of the following:

- to ship their products
- to send updates on order statuses
- to respond to inquiries
- to improve site content or make future transactions fast and convenient for returning users
- to personalize visitor experiences and provide future content tailored to their interests
- to provide or improve customer assistance or technical support
- to send promotional messages or use for future email marketing campaigns
- to improve services, or for internal review
- to present tailored ads to consumers after they leave your store (you *must* disclose if you use third-party remarketing services!)

Here's how Gap answers the "why" in its policy:

How long do you store the data?

There are plenty of reasons to retain records; but legally, you can't retain personal data longer than you need it. This is the GDPR's "storage limitation" principle. Tell users how long you'll be retaining their data, and confirm which data only "passes through" but isn't stored. For example, if credit card information is collected and stored by your payment processor rather than by your website, let visitors know this.

Granted, you might not be able to provide a specific time period (90 days, one calendar year). It may be a matter of how long the customer decides to keep their account open with you, for

example. The point is to give them a timeframe and tell them the reason for retention *within* that frame. Do you need to retain records for state, federal, or provincial taxes? Does your payment processor store credit card information for future use? It might be useful (or required) to be specific. Herman Miller is short and to-the-point:

Whom do you share the data with?

Under the GDPR, your business is allowed to share personally identifiable information with third parties as long as it's done *legally* and *transparently*. "Transparently," of course, means you must provide visitors with details about the sharing. The GDPR doesn't require that you *name* every company with whom you share data (though some companies—like Google—require you to name them); but it *does* require that you name the *types* of business you share with ("payment processors," "shipping providers," "affiliates").

You probably share credit card data with your payment gateway, addresses with your shipping extensions, browsing and demographic data with your marketing extensions—indeed, *any* plugin or integration you use is likely gathering data from your site. Again, the more detail you offer, and the more transparent you are, the better. What data gets shared with these applications; what do they do with that data; what are *their* privacy policies? (And *why* do you use those applications to begin with?) Of course, you won't ultimately have *control* over third-parties' data uses; and you should say as much in your policy. Limit your liability up-front.

How do you secure the data?

We don't have to remind you about the importance of security. Put visitors' and customers' minds at ease by telling them the steps you've taken to protect their information. Start by listing the security measures your ecommerce platform has in place. (With Commerce Plus, *all* data stored in our data centers have credential-level encryption.) What technologies does it use (SSL, encryption, secure passwords, firewalls), and what are those technologies in compliance with? Then move on to your payment gateways. If you're using Commerce Plus, your clause might look like this:

Our company is hosted on the commerceplus.zoho.com platform, which allows us to sell our products to you. Your data may be stored through Commerce Plus's data storage, databases, and applications. Commerce Plus stores your data on secure servers that are encrypted and protected by powerful IDS/IPS systems. Commerce Plus also comes with ISO/IEC 27001:2013 certification for Applications, Systems, People, Technology, and Processes and SOC 2 Type II compliance.

This is one section of your privacy policy where you *don't* need to go into great detail. Consumers will be less concerned about how IDS/IPS systems work than they'll be about whether you've taken every measure possible to secure their data. You might simply remind them that they can confirm

the security measures you claim are in place by looking for the "lock" icon in the address bar of their browser, or for the "https" at the beginning of the URL. *Seeing* this proof may be all the assurance users need. Here's another example from Equator Coffees & Teas:

How can users opt out?

If visitors can withdraw consent, explain the steps they must take to do so—and remind them of the consequences of opting out. (For example, if visitors disable browser cookies, it may inhibit certain site features like cart memory.) The right to "opt out" is often addressed in a section detailing user control *on the whole*: choice, access, and redress. In other words, don't just tell your visitors how to *opt out*; tell them how they can access and review the data you have about them, how they can request changes to (or corrections to, or deletions of) that data, and how they can get in touch with you to file a complaint. Here's how Bed Bath & Beyond breaks it down:

You'll decide the method of contact for privacy-specific requests. And remember, "data changes" are sometimes as simple as having users log into their own accounts to edit information. But make sure your "data controller"—who, if you're a small business, is probably *you*—can be easily contacted. And make that contact information clear.

Naturally, we haven't covered everything here. For example—depending on your product or target market—you might add a clause about minors who might visit your store (the definition of "minor" varies across jurisdictions). You might add a section called "definitions" if you find—again, depending on your product—that you have no choice but to use legal terminology or jargon in your policy. You *should* let users know that you may need to make changes to your policy: How will those changes will be communicated? (Users may simply need to regularly review your policy to stay up-to-date.) And so on.

By considering your business's own data practices, studying the privacy policies of other businesses in your industry, and collaborating with a legal advisor, you'll find your way to a comprehensive privacy policy.

Ensuring Consumers See Your Privacy Policy

You've been on the internet long enough to know that most ecommerce sites "display" their privacy policy through a tiny link in the site footer. As a practice, this is fine... but don't just leave it there. From a legal perspective, it's better to ask users to click on an "agree" or "consent" button to signal that they've read your policy—a practice that, as a consumer, you've probably seen more of since

GDPR passed.

And here's why. In the "browsewrap method"—in which you leave a link to your privacy policy for users to find—it's *presumed* that visitors have read your agreement by virtue of the fact that they're browsing your store. (These policies usually begin: "By using this website, you agree to be bound by the below terms.") But visitors don't tend to *seek out* privacy policies (how often do *you*?), so businesses that use this method run the risk of those same visitors later claiming they didn't know about the terms. With the "clickwrap method," on the other hand, users have to *actively agree* to your policy by ticking a checkbox or pop-up (before they can enter your store, before they sign up for an account with you, or before they hit the "Purchase" CTA) to signal their agreement with your policy. Indeed, the GDPR *requires* active consent to your privacy policy prior to account signup. Include a link to your privacy policy from the signup page... but *make sure your policy appears in a pop-up*, rather than sending users to a new page—you don't want them to forget that they were in the middle of signing up with you!

It's a best practice to offer a link to your privacy policy at *every* point at which you collect personal information from customers—registration forms, live chat, support request forms, opt-in forms, and so on. Place links to the policy in your email footers—*especially* when those emails contain direct marketing communications.

Of course, all of this is just words if you can't stand by your privacy policy. Before your site goes live, make sure you have compliance measures in place, and you know how to respond in the case of a security breach. And as your business grows, continue to be as careful with your visitors' and customers' data as you'd want them to be with yours.

By now, we've discussed almost all of the policies you'll want to have in place for your eCommerce site: your shipping and Returns & Refunds policies and your privacy policy. In the next section, we'll lead you through one final document: your Terms & Conditions.