In The Know *Checklist*

Privacy Policy Must-Haves

Let's cut to the chase – if you have a website, you need a privacy policy. Even if you only collect visitors' names and email addresses (when they sign up for your newsletter, for example), then you need to have a privacy policy in place explaining what you do with that information. Data Privacy is no joke, and it's only getting more serious.

Remember a few years ago when your inbox got bombarded with emails from what seemed like every website you had ever visited? That was because the European Union's data privacy law (the GDPR) went into effect – and even companies in the United States must comply. While there is no standard data privacy law in the US, individual states are slowly proposing their own - and if you have a website, you will need to comply with each of them.

So, to help save you from running afoul of the laws, here's the minimum your policy should address:

1. **What Data do you collect?** Be clear and concise about what data you collect and how. Simple clear language is best. Does the user supply the information directly – by providing payment information or an email address for your newsletter? Do you collect it yourself – such as collecting the visitor's IP address?

2. **What do you do with the Data you collect?** Why are you collecting the data? What are you doing with it? How is it stored? Examples might be for marketing research, enhancing the consumer's website experience, processing orders, or to provide technical support.

3. **Do you share the Data and with whom?** Do you only keep the data internally? Do you share it with third parties, such as a payment processing company or shipping partner? Do you sell the data to third parties? Transparency is key here.

4. **What are your visitors' rights?** The GDPR lists several rights of website visitors: the right to access the data you've collected, the right to be forgotten (erasure), the right of the visitor to have their data moved elsewhere (portability), the right to change their data (accuracy and correcting errors), and the right to object to how you handle the data. You must clearly explain these rights within the policy. California's Data Privacy Law (CCPA) requires that consumers have the right to opt out of their data being sold by data brokers.

5. **You must have a cookies policy.** That annoying pop up that you close as soon as you visit a new website? That's alerting you to that site's cookie policy. Cookies are delicious, and in this case, they make navigating a site easier on subsequent visits by depositing little bits of data

onto the visitor’s computer (better than crumbs in the keyboard). You must explain what you use cookies for and instruct your visitor as to how to refuse cookies.

6. **What about kids?** We all know kids are savvier about the internet than most adults. However, technical prowess aside, protecting children’s data is another layer of compliance. Websites aimed at or marketing to children under the age of 13 must comply with the Children’s Online Privacy Protection Act (COPPA). This includes getting parental consent and providing a mechanism to alert parents about the collection of children’s data, and remove their children’s data, if they choose.

7. **How do users reach you?** At a minimum you need to provide visitors with two methods of communicating with you, and in some cases one of the methods must be a toll-free phone number.

8. **Update your Policy.** The effective date of the policy should be updated with each revision.

9. **Do you use third party software, apps, or plugins?** You may need to alert users as to which software, apps, or plugins you are using. Many have their own language in their user agreement that they require to be present in your policy (for example, Google has specific terms if you use Google Analytics; Facebook has language if your website or mobile app allows consumers to use their Facebook account to log in to your site).