GDPR Guide for Online Businesses

by

AMY PORTERFIELD

GDPR Guide for Online Businesses

What it is. Even if your business is located in the U.S., the European Union's General Data Protection Regulation ("GDPR") will have a direct impact on the way you collect and use other people's information. This is a basic primer about the steps you may need to take in order to comply with the new GDPR requirements, which took effect on **May 25, 2018.**

The U.K. and Canada have also recently adopted similar requirements to GDPR.

Why it matters to you and your business. Failure to comply with GDPR could potentially result in steep fines, penalties, and monetary damages against you or your business.

GDPR compliance to do list:

1. Take inventory of everyone you share other people's data with
2. Change your website forms for email marketing
3. Set up a cookie opt-in on your website
4. Update your privacy policy
5. Take a fresh look at whether you need to form an LLC or corporation and insurance
6. Store other people's data securely
7. Report any data breaches to the authorities within 72 hours
8. Make sure your vendors are GDPR compliant

Compliance To-Do #1: Make a list of all apps, plugins, and other tools and vendors that you use with other people's data

The new rules are different for different kinds of businesses, depending on what tools you use in your business and how you process or store other people's data. The first step is a tech audit to see how your business is using data, so you can figure out what else you need to do.

Examples include:

- Cloud-based e-mail or calendar software (like Gmail / G Suite)
- Messaging tool like Slack
- Project management software like Asana or Trello
- E-mail marketing service provider like MailChimp, ConvertKit or ActiveCampaign
- Online course hosting platform like Kajabi, Teachable, or Thinkific
- Customer relationship manager (CRM) software like HubSpot, Honeybook, or Dubsado

Compliance To-Do #2: New "consent" rules - Change your website forms for email marketing

If you collect e-mail addresses or other data using forms on your website, landing pages, or as part of checkout, you must tell visitors exactly what you will do with their data AND get their affirmative consent to do each of those things.

This requires one of the following:

- A checkbox (not pre-checked!) that they agree to receive a newsletter, marketing emails, or any other way you will use their email address; OR
- A clear notice their email address will be added to your newsletter list (or marketing list, etc.); OR
- A double opt-in sent through your email marketing provider, confirming they would like to receive your newsletter, or marketing emails, etc.

You should also link to your new updated privacy policy (see below) on or very near the form collecting data.

Compliance To-Do #3: Set up a cookie opt-in on your website

If you use cookies at all in your business – that includes the Facebook ad pixel and Google analytics among many others – you will need to get affirmative consent from visitors. This can't be hidden in your privacy policy or terms of use. Many tech solutions are available for this; common methods include requiring visitors to:

- Navigate beyond a banner, notice, or pop-up saying you use cookies and how you'll use their information (with link to privacy policy); OR
- Dismiss a banner, notice, or pop-up
- Click on an "I agree" button

Compliance To-Do #4: Update your privacy policy

If you collect any personal information through your website, even just an e-mail address through an opt-in or contact form, you are required by U.S. laws and GDPR to post a policy on your website telling your users what you will do with this information. Here are some important items to include (This list is not exhaustive! What you must include depends on your particular business - you may want to purchase a privacy policy template to be sure you're totally covered):

- List of the data you collect, why you collect it, how you'll use it, and how long you keep it, and whether you require that it be provided;
- List of the third parties with whom you share or from whom you receive individuals' data
- How the visitor can request their data, review and request corrections to their data, or ask that you erase their data
- How the visitor can withdraw consent for you to use or store their data;
- How you notify visitors of changes to your privacy policy
- How the website responds to Do Not Track signals from Web browsers.
- Choices a consumer has regarding the collection, use and sharing of his or her personal information.
- The effective date of the privacy policy.
- Whom to contact with questions about the privacy policy
- Disclose visitors' rights under GDPR, including the right to lodge complaints with a supervisory authority

Compliance To-Do #5: Take a fresh look at whether you need to form an LLC or corporation and insurance

Because the penalties can be very serious (up to 20 million euros or 4% of a business' gross annual worldwide income, whichever is higher), we recommend that all entrepreneurs consider whether they should protect their *personal* assets by forming an LLC or corporation, and *business* assets with appropriate insurance.

Compliance To-Do #6: Store other people's data securely

Do your best to store data in a secure way; how you do this will depend on your business and the law allows your efforts to be proportionate to your size and the amount and nature of the data you collect. It's best practice to limit access to other people's data only to those who really need it.

Examples include:

- Use a password on your computer, mobile phone, and any other devices that may contain other people's data
- Choose strong passwords for your software or apps that are hard to guess, and avoid using the same password for multiple accounts. Password managers are great for creating and storing strong passwords so you don't have to remember them.
- Add two-factor authentication to your accounts - this requires someone trying to log in to enter their password (the first factor) and a temporary code sent to another device like a mobile phone (the second factor) and makes it that much more difficult for someone to access your account
- Look for software and apps that encrypt data for you as part of their services
- Prioritize who on your team needs access to other people's data - it's likely not everyone needs to be able to log into your CRM or e-mail marketing software

Compliance To-Do #7: Report any data breaches to the authorities within 72 hours

If you discover a data breach, you must report it within 72 hours, no exceptions. The breach must be reported to the Data Protection Authority (DPA) in the EU country in which your company is based, or if you don't have a presence in the EU, you must report to the DPA in each European country you are active in.

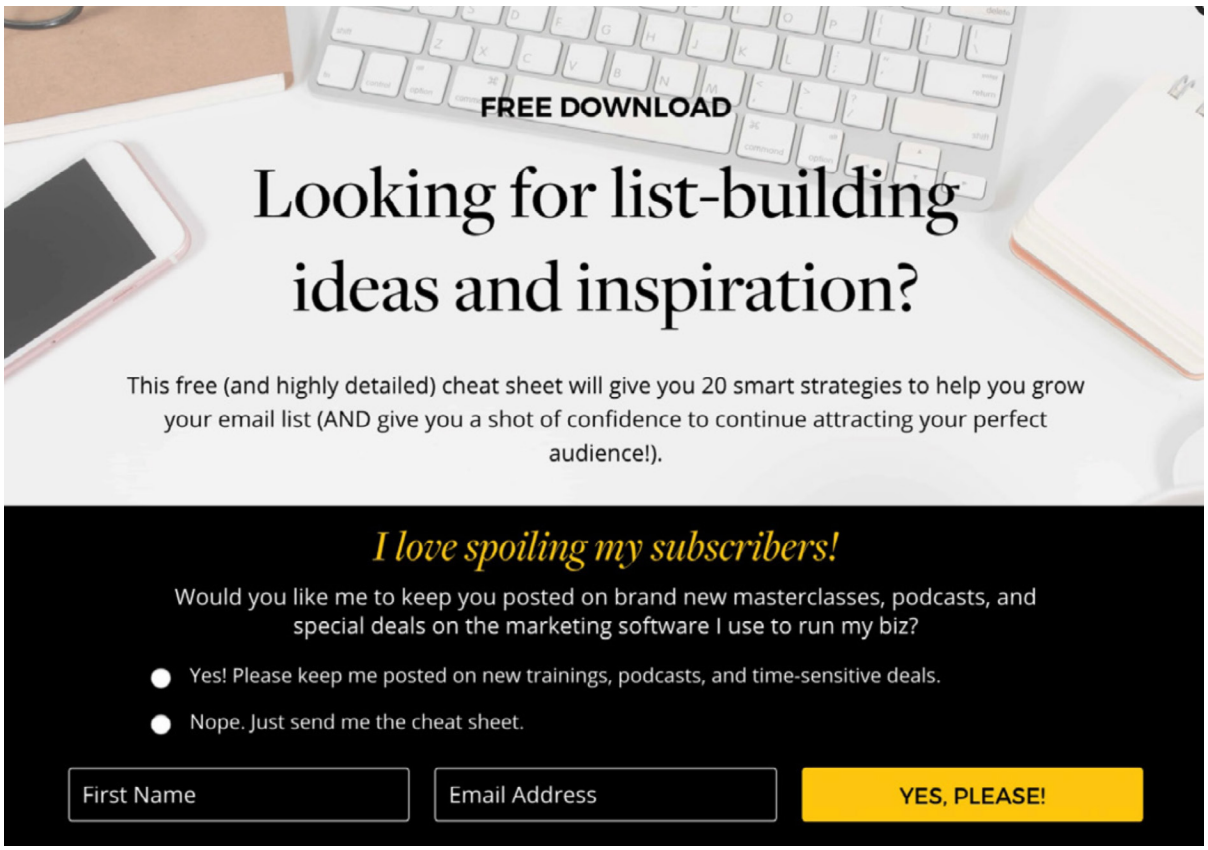
The DPAs for each EU member state are listed by the European Data Protection Board here: https://edpb.europa.eu/about-edpb/about-edpb/members_en

Compliance To-Do #8: Make sure your vendors are GDPR-compliant

You can be held responsible if you store other people's data with a vendor that's not GDPR compliant. You should vet your vendors (e-mail, apps, and anyone else that handles data that's not yours) carefully and include terms in your contracts that they bear any liability and indemnify you for non-compliance with the law.

Examples of GDPR-compliant website opt-in forms

Example #1: The first image below is a freebie opt-in, pop-up box that people come to from the amyporterfield.com home page.



Why this opt-in form is GDPR-compliant:

- The language clearly communicates what a subscriber can expect to receive after signing up
- Visitors have an option to CONSENT to be on the main email list by selecting "Yes! Please keep me posted on new trainings, podcasts, and time-sensitive deals" or the option to just receive the freebie without being added to the list by selecting "Nope. Just send me the cheat sheet."
- A visitor is NOT required to sign up for my email list to get the freebie
- NOTE: You are NOT allowed to have one of the options pre-selected as the default, but you do want to require an answer (yes or no), so they are forced to make a choice.

What happens behind the scenes:

In the backend of Amy's ESP, they tag those based on which of the boxes they select above so they can manage the data properly for those who do not wish to be added to the general list.

Example #2: Here's another example from lawyer Autumn Witt Boyd's website that doesn't require the visitor to check a box, because it gives clear notice that if they click "Yes Please" to sign up, they're getting the freebie, as well as other legal resources:

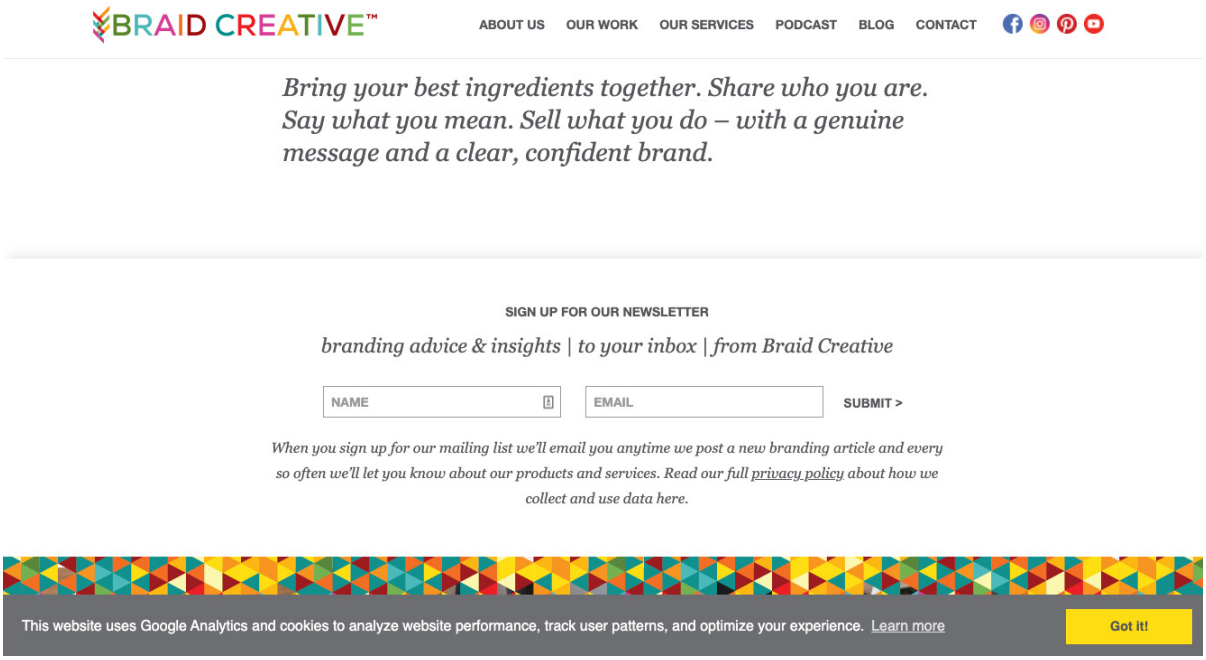
Why this opt-in form is GDPR-compliant:

- The language clearly communicates what a subscriber can expect to receive after signing up: both the freebie *and* other legal resources for online & creative entrepreneurs
- The language under the "Yes Please" button further explains what they'll receive: "When you sign up for our mailing list, we'll email you when we release new podcast episodes and every so often we'll let you know about promotions on our products or services. We will never sell your email address."

What happens behind the scenes:

In the backend of Autumn's ESP, they send out the initial freebie followed by an automated sequence of emails with legal resources. Every email has the option to unsubscribe at the bottom.

Example #3: Branding agency Braid Creative doesn't offer a freebie at all on their website, just a simple newsletter sign up:



Why this opt-in form is GDPR-compliant:

- The form is identified as a newsletter sign up
- The language clearly communicates what a subscriber can expect to receive after signing up: "When you sign up for our mailing list we'll email you anytime we post a new branding article and every so often we'll let you know about our products or services."

You can also see an example of their cookie notice above, with a yellow button to click ("Got it!") to dismiss the notice.

What happens behind the scenes:

No special tech is required for this option. After they sign up, visitors start receiving any newsletters or promotional emails Braid sends out to its general list.

GDPR guidance from top ESPs (email service providers)

- Mailchimp
- ConvertKit
- Kajabi
- ActiveCampaign
- Constant Contact
- Drip
- Aweber

About this Guide:

This Guide does not constitute legal advice. GDPR is a complex regulation. This Guide is not all-inclusive, and you may wish to consult an experienced attorney to determine how these regulations will impact your particular business.

The content in this Guide was drafted by U.S. licensed attorneys with the Law Office of Autumn Witt Boyd, PLLC and was last updated in June 2021.