THE LAW OFFICE OF AUTUMN WITT BOYD PLLC

GENERAL DATA PROTECTION REGULATION (GDPR) COMPLIANCE CHECKLIST FOR U.S. ONLINE & CREATIVE BUSINESSES

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 set to take effect on **May 25, 2018**. *Failure to comply with GDPR could potentially result in steep fines, penalties, and monetary damages against you or your business.*

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.

NEW "CONSENT" RULES - CHANGE YOUR WEBSITE FORMS FOR EMAIL MARKETING: If you have any forms on your website, landing pages, or as part of checkout that collect e-mail addresses or other data, 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 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.

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

 |

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, from anyone in the EU or UK, 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):

- 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

(You can download our firm's GDPR-compliant privacy policy templates here: http://awbfirm.com/contract-templates/)

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.

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.

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.

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.

**This PDF is attorney advertising and does not establish an attorney-client relationship, which is only formed when you have signed an engagement agreement. GDPR is a complex regulation. This list is not all inclusive, and you should consult an experienced attorney to determine how these regulations will impact your particular business.*

