



GDPR



GENERAL DATA PROTECTION REGULATION

Forging ahead of the United States in protecting the privacy of their citizens, the European Union passed landmark regulations in 2018 that govern how businesses collect, store and protect personal information.

WHO NEEDS TO COMPLY

It's simple, if your business is within the European Union (EU), or has customers from the EU, you must comply. While some argue that if your business is based outside the EU you don't need to comply, it's better to be safe than sorry and the EU regulations are overall, a net positive for your customers.

HOW DO I COMPLY?

For those familiar with PCI Compliance, GDPR compliance should look very similar. It involves determining what information you store about your customers, and what techniques and policies you use to protect that data.

While it's tempting to "just install a plugin" or just add a disclaimer to the footer of your website, compliance is more nuanced and involved. See the links below, for helpful guides on what to consider, and what actions to take.

RESOURCES

GDPR Checklist (official): <https://gdpr.eu/checklist/>

GDPR Checklist (non-official): <https://gdprchecklist.io/>

American Bar Association: Key Provisions and Best Practices

Disclaimer: This guide should not be considered legal advice, or authoritative in nature.