Global Data Privacy Regulation Compliance Overview

Companies are *legally required* to fulfill the privacy regulations determined by the geographical location of both the company and their customers. Examples of the most stringent regulations include GDPR (EU), PIPEDA (Canada), LGPD (Brazil) and CCPA (California). These regulations include the following ten *requirements*. Each has to be met to ensure compliance on a global scale.

Compliance is a large task, but when done properly the first time, it becomes simple to maintain. Doing due diligence helps mitigate risk to customers, protects a company's reputation, and drastically reduces fines.

1	***Privacy Engineering & Privacy by Design (PbD)***	*Privacy by Design* is a 7-principle framework that ensures that privacy is paramount in the operation and maintenance of a system. Products and services should follow these guidelines.
2	***Data Categorizations***	All personal data records must be identified by source and have *legal basis*. Your data must be distinguished in terms of *Personal Information* (PI), *Personally Identifiable Information* (PII), and the sensitivity of the data.
3	***Vendor Management***	A company's vendors and third party partners must be compliant with regulation as well. This applies to internal software and services if employees fall under a regulation (ex citizen of a country within the EU), and third party software and services, such as cloud storage, for customers and clients.
4	***Privacy Impact Assessment***	The *Data Protection Impact Assessment* (DPIA) or *Privacy Impact Assessment* (PIA), lists, reviews, and records all the ways data is handled, used, stored, and protected. It should include both a system map and a data map.
5	***Data Subject Access Requests (DSAR), Portability, Retention and Removal***	Companies are required to comply with a *user's rights* with respect to their data. Depending on the legislation, these may include right to access, check for accuracy, request correction, portability (readable format), and deletion from the system. Data must be deleted when no longer required for business purposes.
6	***Privacy Policy***	The *privacy policy* must explain to users what their rights are and how to execute on those rights. It is also important to establish a legal basis for which data is being collected.
7	***Consent***	Users must have the mechanism to opt in and opt out of having their data collected, stored, and transferred. That consent must be stored and updated if data use is changed.
8	***Incident Response Plan***	The *Incident Response Plan* is key to mitigate harm when any kind of breach occurs. The plan includes stakeholders, process, and communications.
9	***Notification to Data Protection Authorities & Users***	Depending on risk of harm of an incident, the appropriate data protection authority (or authorities) must be notified and/or users must be notified individually or by public statement.
10	**Employee Training**	To ensure privacy of both the company and the customers, employees must receive privacy training and be made aware of internal processes and protocols.

We provide assessments, complete checklists, compliance playbooks, and full service consulting.
Questions? Reach out to info@binarytattoo.com