LANDO & ANASTASI

IP ESSENTIALS

A Toolkit for Entrepreneurs, Innovators, and Business Owners

DATA PRIVACY

DATA PRIVACY

Data privacy or information privacy is a branch of data security concerned with the proper handling of data—consent, notice, and regulatory obligations. Practical data privacy concerns often revolve around whether or how data is shared with third parties, how data is legally collected or stored, and regulatory restrictions such as various privacy laws.

Q&A SERIES

Q ***What are the basic components of data privacy?***

A Complying with data privacy requires the creation of a data security protocol to safeguard data collected and a privacy policy that sets forth practices in terms of the collection, use, and handling of users' personal data. Protocols and policies provide information and transparency for users regarding collection of personal data. Privacy policy agreements are mandatory for collecting data that can be used to identify an individual. There are several laws around the world which require a privacy policy in order to legally collect personal data.

Q ***What types of information are protected under privacy laws?***

A While the specifics of the various data privacy regimes vary, information that is considered personal data, or information relating to an identified or identifiable natural person, is typically protected under privacy laws. Personal data include but are not limited to:

- first and last name
- email address(es)
- contact number(s)
- shipping or billing address(es)
- Social Security number
- birthdate
- social media handle(s) or profile image(s)
- credit card information
- financial statements
- current location and travel data
- medical records
- IP address(es)
- genetic information

L&A | LANDO & ANASTASI

Q ***What kinds of data are not governed under privacy laws?***

A Most data privacy laws do not cover anonymous or deidentified data that cannot be traced to a particular person. “Deidentified” data is information that cannot be reasonably traced to a particular individual because the data that points to an individual has been removed. Care must be taken in anonymizing or deidentifying data to ensure that it is both properly deidentified and is not subject to re-identification.

Q ***What countries have laws governing data privacy?***

A There are privacy laws in many countries throughout the world. The European Union, Canada, the United Kingdom, Australia, and Singapore all have national privacy laws with somewhat similar components.

Q ***Does the United States have laws governing data privacy?***

A There is not one comprehensive federal law governing data privacy in the United States. Instead, there is a complex patchwork of sector-specific and medium-specific data privacy laws and regulations at the federal level addressing privacy policies in telecommunications, health information, credit information, financial institutions, and marketing.

The following federal laws include privacy provisions and should be considered when preparing your privacy policy:

- The Federal Trade Commission Act (15 USC § 41 et seq.);
- Children’s Online Privacy Protection Act (15 USC § 6501 et seq.);
- Health Insurance Portability and Accounting Act (HIPAA—P.L.104-191);
- The Gramm Leach Bliley Act (15 USC § 6802 et seq.); and
- The Fair Credit Reporting Act (15 USC § 1681).

Q ***Do any states have comprehensive laws governing data privacy?***

A The United States has hundreds of data privacy and data security laws among its states, territories, and localities. As of 2021, twenty-five U.S. states have laws governing the collection, storage, safeguarding, disposal, and use of personal data collected from residents, especially regarding data breach notifications and the safe use of Social Security numbers. Some laws apply only to governmental entities, others to private entities, and some laws apply to both.

"There is not one comprehensive federal law governing data privacy in the United States... instead there is a complex patchwork of...laws and regulations"

Q ***Which jurisdiction has the most comprehensive privacy laws?***

A Internationally, the European Union's General Data Protection Regulation (GDPR) that regulates the processing of personal data within the European Union is considered to be the most stringent and comprehensive. Within the United States, California's CalOPPA and CCPA combine to form the most robust privacy regulations among the currently existing privacy laws. For companies dealing with medical information within the United States, additional consideration should be given to HIPAA and GINA requirements.

Q ***What are the compliance requirements for sharing consumer data with a third party?***

A Most data privacy laws include procedures and restrictions on sharing consumer data with a third party such as notification and opt-in requirements and limitations on data processing. These procedures and restrictions apply to the selling of customer data, and also to the transfer of data to third parties for the purposes of storing information collected from customers in "the cloud" through a cloud storage provider, using a mail carrier to ship products, collecting online analytics or cookies, sharing a mailing list with an email marketing company, and more.

Q ***How can my company ensure compliance with the privacy law requirements?***

A As a company, you should focus on creating a robust a data security protocol for internal use and a data privacy policy to be provided to consumers. Among the things to be considered are:

- taking stock of the types of personal information you are collecting from consumers and creating different level of security depending on the sensitivity of the data;
- scaling down the amount of data collected to only what is absolutely necessary to run your business, and keep the data only as long as you need it;
- developing physical and electronic security protocols to protect the data you collect and to limit access on a "need-to-know" basis;
- implementing a policy for safe and responsible information disposal; and
- creating a plan for responding to security incidents. Additionally, your data policy should be easily accessible and clearly spelled out for the consumer, and detail what data you collect and how that data is used, with clear instructions on how consumers can access and consent to the collection, sharing and use of such data.

Q ***How can my company ensure compliance with privacy law(s) while sharing data with third parties?***

A To ensure privacy law compliance, consider the following while developing a third-party data sharing policy:

- legitimacy (lawful basis for sharing data);
- benefit vs. risk;
- whether you have rights to share the information;
- safeguards governing the data transfer;
- developing sharing protocol and agreements; and
- keeping the shared data up-to-date and accurate.

Q ***What are the potential penalties for failure to comply with a privacy law?***

A Failing to comply with the privacy policies and resulting data breach can lead to significant fines that vary on the degree of non-compliance and efforts to alleviate the damaging nature, and the gravity and duration of the violation once discovered.

The GDPR allows for fines of ten million Euros *or* two percent of the noncompliant firm's worldwide annual revenues, whichever is greater, for less severe infractions. These fines can be doubled for more serious infractions. Additionally, being embroiled in a data breach controversy can also erode trust among the customer base leading to loss of revenue.

California provides for fines up to $7,500 for every record affected by the instance of noncompliance. In addition, the CCPA provides for a private cause of action for California residents whose personal information is exposed in connection with a data breach resulting from a company's failure to implement and maintain reasonable security practices and procedures. The greater of actual damages or statutory damages of up to $750 per incident are permitted.

Q ***What rights does a consumer have under the privacy laws?***

A Most data privacy laws require consent from the consumer before collecting and using personal data and require notification when a data breach occurs. Specific details vary among jurisdictions.

Under the GDPR, a consumer also has the right to be informed about the collection and use of their data once obtained, a right to access their data, and a right to demand deletion of their data or to restrict processing.

Under California law, consumers have the right to seek an easily accessible and understandable privacy policy and the right to non-discrimination (businesses are not allowed to discriminate against consumers who have used or exercised any of the privacy rights given to them by law).

Q ***Are there any specific privacy law requirements to protect genetic data from a consumer?***

A Genetic information connected to personal identifiers is generated and used in a variety of contexts that may or may not be health-related such as clinical genetics, direct-to-consumer (DTC) testing, and forensics. A variety of laws govern the collection, use, and sharing of this highly sensitive type of data. Genetic data is covered by HIPAA, which prohibits use or disclosure of non-deidentified genetic data.

The Genetic Information and Nondiscrimination Act of 2008 (GINA) protects the genetic privacy of the public, including research participants, and prohibits health insurers or employers from requesting or requiring genetic information of an individual or of a family member and further prohibits the discriminatory use of such information.

The collection and use of genetic data for government-funded biomedical research containing human subjects in the U.S. is governed by the Common Rule, which sets forth disclosure and informed consent requirements for genomic research.

Additionally, there are various state laws governing genetic data, such as Florida's DNA Privacy Law and California's Genetic Information Privacy Act (GIPA) that govern the use of an individual's genetic data collected by direct-to-consumer genetic testing companies.

This IP Essentials Topic is one of a series:

IP Essentials Toolkit for Entrepreneurs, Innovators, and Business Owners

The information provided on this document does not, and is not intended to, constitute legal advice; instead, all information, content, and materials are for general informational purposes only. Readers should contact an attorney to obtain legal advice with respect to any particular legal matter.

L&A | LANDO & ANASTASI

60 State Street, 23rd Floor

Boston, MA 02109

lalaw.com | 617.395.7000