Beyond GDPR

Four steps for business leaders to begin data privacy compliance.

By Adam C. Johnson

In May 2018, the European Union released an expansive and comprehensive data privacy law known as the General Data Protection Regulation, or GDPR.

Since then, the state of California passed a substantively different privacy act, leaving many business leaders confused about conflicting regulations, guessing about extraterritorial jurisdictions, and uncertain about whether the United States will pass a federal data privacy law that may obviate them all.

Business leaders who operate multinational corporations are seemingly left in a bind. They face a quandary about what data is subject to which regulation and when.

U.S. laws such as the Health Insurance Portability and Accountability Act, known as HIPAA, and the Children's Online Privacy Protection Act, or COPPA, when layered onto state- or country-specific regulations, create a sea of compliance issues to navigate and a jungle of incompatible requirements to

untangle, further challenging business leaders. For such reasons, data privacy is seldom a pleasant conversation topic.

So why should companies dedicate precious time, personnel, and resources toward data privacy compliance?

Beside the legal obligations, it's in the financial and reputational interests of companies to evaluate and address privacy concerns today rather than deal with the blowback of incompliance tomorrow.

Further, data privacy is a fundamental right that is proliferating. Through the GDPR and the California Consumer Privacy Act of 2018 (CCPA), both the EU and the state of California assert that consumers have the right to data privacy—the ability to control their data with certain reasonable exceptions. The right to data privacy is indelible.

GDPR and CCPA are two of the newest laws that affect many U.S.-based companies. And although the laws are different in scope and intent, business leaders can be assured that there are some similarities between them that can serve as a starting point for compliance.

What data does the company collect? Business leaders must know what data their company collects and from whom they're collecting it. The type and origin of data, in turn, largely determines data requirements and is a best starting point for compliance.

(Fig. 1) **DATA TYPE COMPARISON**

GDPR		CCPA	
Reference:	Data Type:	Reference:	Data Type:
Article 4, (1)	**Identification number**	1798.140, A	**Personal identifier**
Article 4, (1)	**Any data relating to an identified or identifiable natural person**	1798.140, B	**Personal information**
—	—	1798.140, C	**Protected classifications**
—	—	1798.140, D	**Commercial information**
Article 4, (14)	**Biometric data**	1798.140, E	**Biometric information**
Article 4, (1)	**Online identifiers of identity**	1798.140, F	**Internet data**
Article 4, (1)	**Location data**	1798.140, G	**Geolocation data**
—	—	1798.140, H	**Audio, electronic, visual, thermal, olfactory, or similar information**
—	—	1798.140, I	**Professional identifier**
—	—	1798.140, J	**Educational information**
—	—	1798.140, K	**Personal preference information (real or inferred)**
Article 4, (13)	**Genetic data**	—	—
Article 4, (15)	**Data concerning health**	—	—
Article 10	**Criminal record data**	—	—
Article 9, (1) (2)	**Race, political opinion, religion, etc.**	—	—

Data type comparison table provides a high-level view of similar data types by regulation.
Always consult suitably qualified legal counsel regarding any specific questions on regulations or legal matter.

(Fig. 2) **RIGHTS COMPARISON**

GDPR RIGHTS	CCPA RIGHTS	RIGHTS SUMMARY
Right to Be Informed Ch 3, Art 12, 13 & 14	**Right to Know** 1798.100	Rights for informing consumers about data processing and transparency
Right to Access Ch 3, Art 15 **Right to Port** Ch 3, Art 20	**Right to Access** 1798.115	Rights allowing consumers to view and download their data
Right Erase Ch 3, Art 17	**Right to Deletion** 1798.105	Right allowing consumers to request erasure of their data
Right to Restrict (67); Ch 3, Art 4(3) & Art 23	**Right to Say No to Sale of Personal Info** Through opting out 1798.120	Rights allowing consumers to opt out or restrict the use of their data
Explicit Consent Ch 3, Art 7	**Opt Out** Say no to sale of personal info 1798.120 **Opt In** For consumers under age 16 1798.120 (c) & (d)	Rights allowing consumers to give and withdrawal consent
—	**Right to Equal Service & Price** 1798.125	Right ensuring that consumers receive equal treatment of products, services, and price fairness
Right to Rectify Ch 3, Art 16	—	Right allowing consumers to edit or correct their data
Rights Related to Automated Decision-making & Profiling Ch 3, Art 22	—	Right for consumers to know whether a company uses their data for automated decision-making and profiling
Right to Object Ch 3, Art 21	—	Right allowing consumers to object to the use of their data

Data Privacy Initial Focus Areas

Of the data a company collects, leadership should determine and codify which data it can associate with specific consumers—and classify it as personally identifiable information (PII). Each regulation outlines types of data, standards, and caveats for PII, but as a general rule, if a business can associate data directly to a consumer, that data may be subject to data privacy regulations.
[SEE FIGURE 1]

One best practice for managing consumer data is to collect the least amount of data necessary to achieve an immediate and intended outcome. This "minimalization" strategy may reduce exposure, storage requirements, and the cost of IT infrastructure. It also forces business leaders to think intentionally about data usage and solution design prior to collecting it: We collect this data from these consumers for that outcome. In short, it encourages responsible data collection and use.

How does the company store and process consumer data?
Knowing the type and origin of data is only half the challenge. The other half is understanding where the company stores it and the implications of each data set for business operations. This is typically achieved by mapping data by database down to the attribute level, ranking data elements by priority, and categorizing each with corresponding business outcomes.

When possible, business leaders should seek to de-identify data through pseudonymization to protect consumer data and reduce exposure in the event of a breach. Companies should also recognize that data stored in different countries may be subject to data localization laws not specified in GDPR or CCPA.

Joint controllers, third parties, and processors are all names for entities a company shares consumer data with or allows access to. As GDPR stipulates, all parties that process consumer data must jointly determine and formally record their responsibilities for data compliance practices and make the agreements public, possibly in each company's terms of use agreement.

Does the company allow consumers control of their data?
Providing consumers "rights" will likely be a new requirement for most companies, but one that business leaders ought to become increasingly familiar with. GDPR and CCPA both outline rights that empower consumers with functionality to control the use of their data.

Even though some of the specified rights aren't consistent in name or function, there are several similarities. Companies, however, must balance consumers' rights to control their data with the intended user experience. Too much control could be onerous and detract from their product experience.
[SEE FIGURE 2]

Is the company transparent about its practices?
Companies should strive to provide reasonable details about their data processing practices, allowing consumers to make more informed decisions about their personal information. This is what GDPR calls the "right to be informed" and CCPA labels as the "right to know."

To fulfill this right, business and legal teams must work together to document the items outlined in the previous steps, then determine what level of detail to disclose to consumers. Too little information is uninformative; too much can confuse consumers.

Being transparent means communicating about data processing practices with clear and plain language. Gone should be the days of legalese printed in 4-point type and packed into obscure or generic statements. Business leaders should also establish a regular cadence with privacy teams to reevaluate whether updates to consumer-facing statements are required, so all policies remain consistent with actual business practices.

Finally, GDPR compliance doesn't equate to CCPA compliance. Because many companies are obligated to comply with both, and because portions of each law seemingly conflict, business leaders are turning to trusted legal and business advisors to navigate data privacy challenges to take their first steps toward compliance. ★★

Adam C. Johnson
adam.johnson@jabian.com