LUNDIN & Co.
Security ◆ Privacy ◆ Technology
Audit ◆ Consulting

ISSUE BRIEFING –
SWEEPING NEW CALIFORNIA PRIVACY LAW
July 3, 2018

Just one month after the GDPR went in to effect and just in time to head off a November ballot measure, the California Consumer Privacy Act of 2018 was signed into law last week with an effective date of January 1, 2020.

- The implementation of the law should provide much greater transparency to consumers about what personal information is collected, how and why it is collected, and to whom it is shared or sold.
- The law will give California consumers greater control over the use of their personal information and will impose significant penalties if businesses misuse or fail to secure consumers' personal information.
- The law will drive companies to scrutinize how they collect and use consumers' personal information, how they use that information to provide services, and how they price those services.
- Businesses will need to build upon their GDPR preparations – enhancing their overall data governance, security and privacy program management to address these new requirements and the growing wave of global and domestic privacy regulations.

Applicability of the Law

The law applies to entities doing business in California with $25 million in annual revenue; possession of the personal data of more than 50,000 consumers, households or devices; or earning more than 50% of their annual revenue selling consumers' personal data. There are a variety of specific scenarios where the law is not applicable (e.g., for personal information already subject to HIPAA, GLBA, consumer credit reporting laws, etc.) According to a July 2018 article, the International Association of Privacy Professionals (IAPP) estimates the law could impact 500,000 U.S. companies.

Personal Information Defined

The law defines personal information broadly to include a long list of data elements – e.g., name, postal address, email address, IP address, government ID numbers, browsing history, geolocation data, and professional information. It also includes "inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

Additional Consumer Rights

Transparency about Data Collection	Consumers have the right to request that businesses disclose to them: • the specific pieces of personal information collected, • the categories of personal information collected, • the categories of sources such information is collected from, • the business purposes for collecting or selling this information, and • the categories of third parties with whom such information is shared. This may be requested two times per year and covers personal information collected in the preceding 12 months.
Data Portability	Such information must be provided in readily usable format so that it could be transferred to another provider.
Data Deletion	Consumers have the right to request deletion of any personal information collected about them, though businesses have the right to deny certain requests if they have a valid business purpose for retaining such information.
Opt Out of Sale	Consumers have the right to opt out of the sale of their personal information to third parties.

Key Impacts to Businesses

Levels of Services and Pricing	Under the law, businesses may charge different pricing or provide different service levels only if "directly related to the value provided to the consumer by the consumer's data." Businesses may offer financial incentives for the collection, sale and deletion of personal information.
Updated Disclosures	Businesses must enhance their privacy policy and websites to address various requirements of the law.
Consumer Access to Information	Businesses must promptly disclose and deliver within 45 days, or in some cases 90 days, collected personal information to the consumer based on a verifiable request.
Deletion of Information	Businesses must delete the consumer's personal information and direct service providers to do the same.
Deletion Exceptions	Businesses and service providers are not required to delete the consumer's personal information if there is a valid business requirement to retain such information. Valid reasons for retaining personal information are listed in the act and range from necessity to complete the associated transaction to detection of security incidents or fraud, debugging and complying with legal obligations.
Opt Out	Businesses that sell personal information must give explicit notice to consumers and provide them the opportunity to opt out.
Do Not Sell My Personal Information	Businesses must provide a clear and conspicuous link on its home page titled "Do Not Sell My Personal Information."
Third Parties	Third parties that receive personal information from a business cannot resell personal information unless the consumer has received notice and been given the opportunity to opt out.
Opt In (for children)	Businesses are prohibited from selling the PI of consumers if it has actual knowledge the consumer is between 13-16 years old unless the consumer or their parent/guardian has opted in.
Deidentified/ Aggregated Information	The law does not prevent a business from collecting, using, retaining, selling or disclosing consumer information that is deidentified or aggregated.

Penalties

The law includes penalty provisions that could be very significant depending on the number of consumers impacted by a given violation.

- Intentional violation of the new law may result in a civil penalty of up to $7,500 for each violation. If a cure is possible, the business will have 30 days to cure a violation without penalty.
- If consumers' nonencrypted or nonredacted personal information is the subject of a breach or otherwise disclosed due to failure to implement and maintain reasonable security procedures and practices may be subject to civil action with penalties of at least $100 to $750 per consumer per incident.

Key Actions

As businesses continue to operationalize and improve GDPR compliance, they will need to consider the impact of the new California law, plan for the eventual rollout of the supporting regulatory guidance, and plan for the increasing likelihood of further state and national legislative and regulatory action. While the effective date is 18 months away, most organizations will need to begin work soon. Several key actions, applicable to many organizations, are listed below.

Integrated Control Framework	We believe it is important to establish an integrated control framework that sets a high standard for privacy and data protection – a framework that addresses the GDPR and California requirements, and integrates with other security compliance requirements to the extent applicable (e.g., company security standards, SOC 2, ISO 27001, PCI DSS, industry requirements, etc.) Setting a high standard will enable the business to more easily address future laws, regulations and customer requirements – focusing on the incremental differences. The integrated control framework can be as simple or as complex as the business requires.
Data Governance	The California law and the regulatory trend illustrate the importance of establishing a strong data governance function. Businesses need to have a very clear picture of the data they are capturing, how to categorize and classify that data, how that data flows within the organization and with third parties, where that data resides, and how that data is protected. Strong data governance will be critical to executive management to have confidence and avoid penalties as their businesses prepare for greater transparency to consumers, specific disclosures of the categories of personal information collected, and a surge in consumer information access and deletion requests. A strong Data Protection Officer role may be helpful in driving action and accountability.
Handling Consumer Requests	Gathering all of a consumer's personal information in response to a request could be a challenging process depending on the nature of the business and its supporting systems. Manual processes will not be sustainable in most cases. Considerable engineering effort will be required to build a substantially automated solution in most cases. Businesses will also need to ensure they have a solid process for verifying consumer requests.
Data Deletion Requests	Data deletion is usually a very complex matter for a company as an individual consumer's data is often spread across multiple systems, perhaps multiple vendors, multiple databases, system logs, backup systems, and backup media with differing retention periods. Determining which data must be deleted and which data must be retained requires careful planning and strong data governance.
Effective Encryption	The California law illustrates the importance of encryption as it details penalties for the inappropriate disclosure of nonencrypted personal information through security breach or due to inadequate security measures. Businesses should make sure that unredacted personal information is stored in encrypted format using good practices for cryptographic key management. "Checking the box" that data is encrypted is not enough. Effective encryption requires good practices in encryption life cycle management considering factor such as the strength of the algorithms and key lengths used, how are the keys protected (e.g. hard coded or stored on secure cryptographic hardware), when keys are changed, the security of the processes for encryption and decryption, and so on. Now is a good time to take a fresh look at how the business manages data encryption. Many companies struggle in this area.
Third Party Management	Businesses will generally need to establish stronger control over third parties that play a role in processing or storing consumers' personal information. This includes a range of third parties from supporting technology vendors to channel partners. Businesses must have a clear picture of how these third parties factor into data governance and how personal information is handled from a contractual, security and privacy perspective.
Policies, Practices and Training	Businesses will need to update their privacy policies and supporting practices to address the new California requirements and necessary changes to business processes. Internal training is also required.

LUNDIN & Co.
Security ◆ Privacy ◆ Technology
Audit ◆ Consulting

Contact Us

Mark Lundin
Owner & Executive Consultant

Lundin & Co. provides audit and consulting services focused on security, privacy and technology. Our leadership brings over 20 years of experience providing innovative audit and consulting services focusing on cloud, security, privacy and changing technology.

We work with high growth, innovative companies ranging from startups to established global technology leaders. We provide practical solutions to help you proactively and effectively manage your cybersecurity, privacy, cloud, crypto, emerging technology, and compliance risks and obligations.

If you might need assistance or would like to have a conversation regarding your security, privacy and compliance programs, you can reach us:

Web: lundin.net **Email**: inquiries@lundin.net **Phone**: 925-308-5493