POSSIBLENOW™

Consent, Preferences, Insights, Compliance

TRUST
Be Human

CALIFORNIA CONSUMER PRIVACY ACT:

AN OVERVIEW OF REQUIREMENTS AND TIPS FOR COMPLIANCE

Prepared by CompliancePoint, a PossibleNOW Company

Enabling responsible interactions between customers and the marketplace.

WHAT'S INSIDE

How did the CCPA come to be?

The California Consumer Privacy Act (CCPA), is a data privacy regulation intended to give California residents insight into how their data is monetized by organizations and power over how the data is treated. It started out as a ballot initiative in early 2018 and was signed into law in June of 2018. It went into effect on January 1, 2020 and was enforceable on July 1, 2020. The original CCPA ballot initiative was introduced by California real estate developer, Alistair Mactaggart, who realized the massive amounts of data companies collect and store regarding consumers during a conversation with a tech employee at a cocktail party. This realization came at a time when privacy was suddenly on the top of everyone's minds, around the time the Facebook Cambridge Analytica scandal news was breaking and being covered virtually everywhere and as the enforcement date of the General Data Protection Regulation (GDPR) was closing in.

With this in mind, Mactaggart worked to develop a privacy initiative focusing on three main principles:

- Transparency
- Control
- Adaptability

The new privacy ballot initiative received 630,000 signatures which is almost twice the required signatures to be included on the California ballot. Based on this strong indicator that the initiative would pass and the implication that it would be effective immediately and not go through the usual legislative process, politicians made a deal with Mactaggart to pass a regulation based on the original ballot's three principles of transparency, control, and accountability. The new ballot initiative had a later enforcement date and various other changes such as less in-depth disclosures that still provided consumers with fundamental rights. Thus, the California Consumer Privacy Act was developed and approved.

The CCPA as we know it today was passed with strong bipartisan support and California proved it continues to be on the cutting edge when it comes to consumer protections.

Who and what does CCPA apply to?

The CCPA applies to any business that collects California residents' personal data that either:

- Has annual gross revenues of at least $25 million
- Annually buys, receives, sells, or shares personal information of more than 50,000 consumers, households, or devices
- Derives 50% or more of its annual revenue from the sale of consumer personal information.

An important note here is that the CCPA applies to any business regardless of whether the business is located in or out of the state of California. Any business that meets the criteria above and collects California residents' personal data as defined by the CCPA is subject to its requirements.

Before getting into the requirements under the CCPA, there are a few key definitions to understand:

- A "Consumer" is defined as "a natural person who is a California resident." Keep in mind that "consumers" includes all California residents, including both customers and employees.
- "Personal information" is defined as "any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The CCPA explicitly outlines that personal information does not include any information that is publicly available.

Examples of personal information provided within the CCPA include (but are not limited to) the following:

- First and last name
- Postal address
- Online identifier
- IP address
- Email address
- Account name
- Social security number
- Driver's license number
- Passport number
- Biometric information
- Internet/electronic network activity
- Geolocation data
- Professional/employment-related information
- Education information not publicly available

- "Processing" means any operation or set of operations that are performed on personal data, whether or not by automated means. This essentially means that processing could include any action taken on personal data including collection, the act of processing, storage, and deletion.
- "Sell" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating a consumer's personal information to a third-party for monetary or "other valuable consideration.

What are the exemptions from the CCPA?

The CCPA does provide for certain processing activities that are exempt from the CCPA requirements. Businesses should take a conservative approach to analyzing when these exemptions apply. It is recommended the organization formally document any processing activities around California personal data that meet one of the exemptions below to outline why the business is not subject to the requirements of CCPA.

Specifically, the CCPA shall not restrict a business's ability to:

- Comply with federal, state, or local laws
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities
- Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law
- Exercise or defend legal claims
- Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information
- Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California
- For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing (including on a device) personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

Further, the CCPA provides for various exemptions to personal data collected related to the following:

- Personal information protected under the Health Insurance Portability and Accountability Act (HIPAA)
- Personal information collected by entities governed by the Confidentiality of Medical Information Act
- The sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report and use of that information is limited by the federal Fair Credit Reporting Act
- Personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act
- Personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994

Obligations if the CCPA applies to your business

As mentioned previously, the CCPA is based on three principles: transparency, accountability, and control. In order to meet the "transparency" principle, businesses must comply with the notice requirements included in the CCPA. Transparency has become a frequent commonality among recent data protection laws since the main goal of data protection is to provide consumers with more power and control over when and how their personal data is used. Transparency is key to provide consumers with this control.

Under the CCPA, businesses must provide the following notice disclosures within their privacy policies:

- Categories of personal information collected
- Purposes for which the personal information will be processed
- Categories of third-party recipients of the data
- The right to know what personal information is collected
- The right to know whether their personal information is sold or disclosed and to whom
- The right to opt-out of the sale of their personal information
- The right to access their personal information
- The right to request the deletion of their personal information
- The right to equal service and price, regardless if they exercise their privacy rights
- Two or more designated methods to submit requests for information to, including a toll-free number and a web page
- A link to a page titled "Do Not Sell My Personal Information" that allows consumers to opt out of the sale of their personal data

The privacy policy should be regularly reviewed and updated upon any changes in data collection and processing activities to ensure compliance with the CCPA principles. At a minimum, the policy should be reviewed annually. These notice requirements should be provided whenever consumers' personal data are collected or, if collected indirectly, within a reasonable timeframe after the data is collected. Failure to provide these disclosures will erode consumer trust and could lead to violations of the CCPA. The notice requirements are a cornerstone of the CCPA and should be made transparent. Consumers can easily check an organization's privacy to determine CCPA readiness and this should be a priority for all organizations the CCPA applies to.

Consumer Rights

CCPA provides consumers with several fundamental rights pertaining to their personal information. Businesses familiar with the data subject rights provided under the GDPR will have little trouble complying with the rights provided under the CCPA. Slight variations exist, but the process flows will be similar.

Consumer rights under the CCPA include:

- The right to know what personal information is collected. This right resides under the "transparency" principle of the CCPA and is tied closely to the notice requirements. Consumers have the right to receive clear, transparent information regarding the categories and specific pieces of personal data the business has collected, the purpose of collection and/or sale of the personal data, and the categories of third-parties with whom the data has been disclosed.

- The right to know whether their personal information is sold or disclosed and to whom. When consumers make this type of request, organizations must provide the categories of personal data that have been collected, the categories of personal data the organization has sold or disclosed to a third-party, and the categories of third-parties with whom the personal data has been disclosed.

  TIP: Through a completed data inventory and data mapping exercise, organizations will easily be able to respond to this type of rights request as they will have already mapped out where data comes from and where data flows. Businesses that do not yet have a personal data inventory or data map should prioritize mapping any California personal data processed first. The data map must be regularly reviewed to ensure it is continuously updated.

- The right to opt-out of the sale of their personal information. The right to opt-out of the sale of personal data encapsulates the importance of giving the consumer more control over their data. Businesses are required to provide consumers with a "clear and conspicuous" link titled "Do Not Sell My Personal Information" on the homepage of their website. This link should direct consumers to a separate page that allows them to opt out of the sale of their personal data.

  TIP: To give consumers the most control, organizations should consider offering a granular/layered opt-down with an overall opt-out option. This can be accomplished through a preference center similar to those commonly used for email opt-outs. Once a consumer does exercise this right, organizations must honor the request for a minimum of 12 months before seeking additional permission from the consumer to sell their personal data.

- The right to access their personal information.
  When a consumer exercises this right, organizations must provide the consumer with a copy of their personal data that is processed free of charge. The CCPA allows for this information to be provided via mail or electronically. If provided electronically, the information should be provided in a portable format that allows the consumer to transfer the data to another entity. Due to the potentially sensitive information that might be included in a right to access request, CompliancePoint and PossibleNOW recommend organizations develop a secure portal to allow access to this information for a limited timeframe.

- The right to request deletion of their personal data.
  When consumers exercise this right, organizations must delete all personal data it has on the consumer within the required 45-day (with an additional 45-day extension available) timeframe. Further, the organization must notify any third-party providers to delete the consumer's personal data as well. All requests for deletion should be carefully reviewed by the legal team as the CCPA provides for various caveats to the requirement to honor this right, such as when the organization is required to maintain the data to comply with a legal obligation or to complete a transaction with the consumer.

  TIP: The data inventory and data mapping exercise will allow for organizations to easily identify all systems that process the consumer's personal data to ensure the right is fully honored and/or determine to which data this right applies.

- The right to equal service and price, regardless if they exercise their privacy rights.
  Organizations are prohibited from discriminating against consumers because they have exercised any of the rights listed above. Specifically, organizations cannot deny goods or services to the consumer, charge different prices for goods or services, impose penalties, provide a different level of quality of goods or services, or suggest that the consumers will receive a different price for the goods or services. However, the CCPA does provide the ability to offer different levels of goods/services if they are equitable to the value lost by not being capable of monetizing the consumer's data. It is yet to be seen how organizations will approach this and how regulators will enforce this gray area of the regulation.

Prior to honoring a request, organizations must make reasonable efforts to authenticate consumers to ensure the request is valid. This could occur through verifying a customer ID number or using email verification, among other methods.

Businesses have 45 days to respond to consumer rights requests. If reasonably necessary, businesses can extend this timeframe by an additional 45 days but must notify the consumer of the extension within the initial 45-day period. Clarification has not yet been provided regarding when it would be "reasonable necessary" to request the extension. Due to the strict timeframe to review and respond to these rights requests, organizations should have a centralized source for all requests to flow to for review. Records should be retained indicating the day the request was received and the due date for response.

TIP: It is recommended organizations develop templated responses for each type of request to allow for easier and consistent responses. As with most compliance-related issues, it will be up to the business to demonstrate that it responded to the request within the allotted timeframe. Therefore, records should be retained documenting the action taken on the request (i.e., honored the request, denied the request due to an exemption, or requested an extension).

As previously mentioned, a completed data inventory and data mapping exercise will greatly reduce the burden on businesses in the event they receive a rights request. This exercise should document all California personal data collected both directly and indirectly from California residents. Therefore, all business units should be included in the data mapping exercise, including Human Resources, Legal, Business Intelligence, Customer Support, Marketing, Website, Sales, Information Technology, and Information Security. A data mapping exercise will allow businesses to document why personal data is processed and how the data is processed lawfully. As such, the data map will also allow businesses to determine when the various rights apply and must be honored.

New Requirements Surrounding Personal Data Breaches

Under the CCPA, consumers are only provided with a right to private action when they have been subject to a personal data breach. Under the CCPA, a breach is defined as any incident where consumers' non-encrypted or non-redacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. The CCPA refers specifically to personal data breaches defined under California's Breach Notification Law.

Therefore, private right of action becomes available when a breach, as defined above, occurs regarding the following personal information:

- An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
  - Social security number
  - Driver's license number or California identification card number
  - Account number or credit/debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
  - Medical information
  - Health insurance information
  - Information or data collected through the use or operation of an automated license plate recognition system
- A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

As noted previously, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Prior to initiating a private right of action, consumers must provide the business with a 30-day written notice identifying the specific provisions that have been violated. If the business can offer a resolution for the violation within the 30-day period, it must provide the consumer with a written statement notifying the consumer of the resolutions and that no class action may be initiated. If, however, the business continues to violate its security requirements to protect personal data, the consumer may initiate a class action against the business. Through a private right of action, consumers are granted the ability to seek damages of $100 - $750 per incident, or actual damages. When determining the amount of statutory damages to apply to a business who has experienced a breach, the court will consider the nature and seriousness of the breach, the number of violations, the length of time the breach occurred, whether the business's misconduct was willful, and the defendant's financials.

What are the consequences of non-compliance?

The CCPA is enforced by the California state attorney general. Businesses found to be in violation of any of their obligations imposed by the CCPA are subject to a civil penalty of up to $2,500 per violation and up to $7,500 per willful violation. All settlements will be directed towards a new "Consumer Privacy Fund," which will be used to offset future costs incurred by the courts or the state attorney general in relation to these requirements.

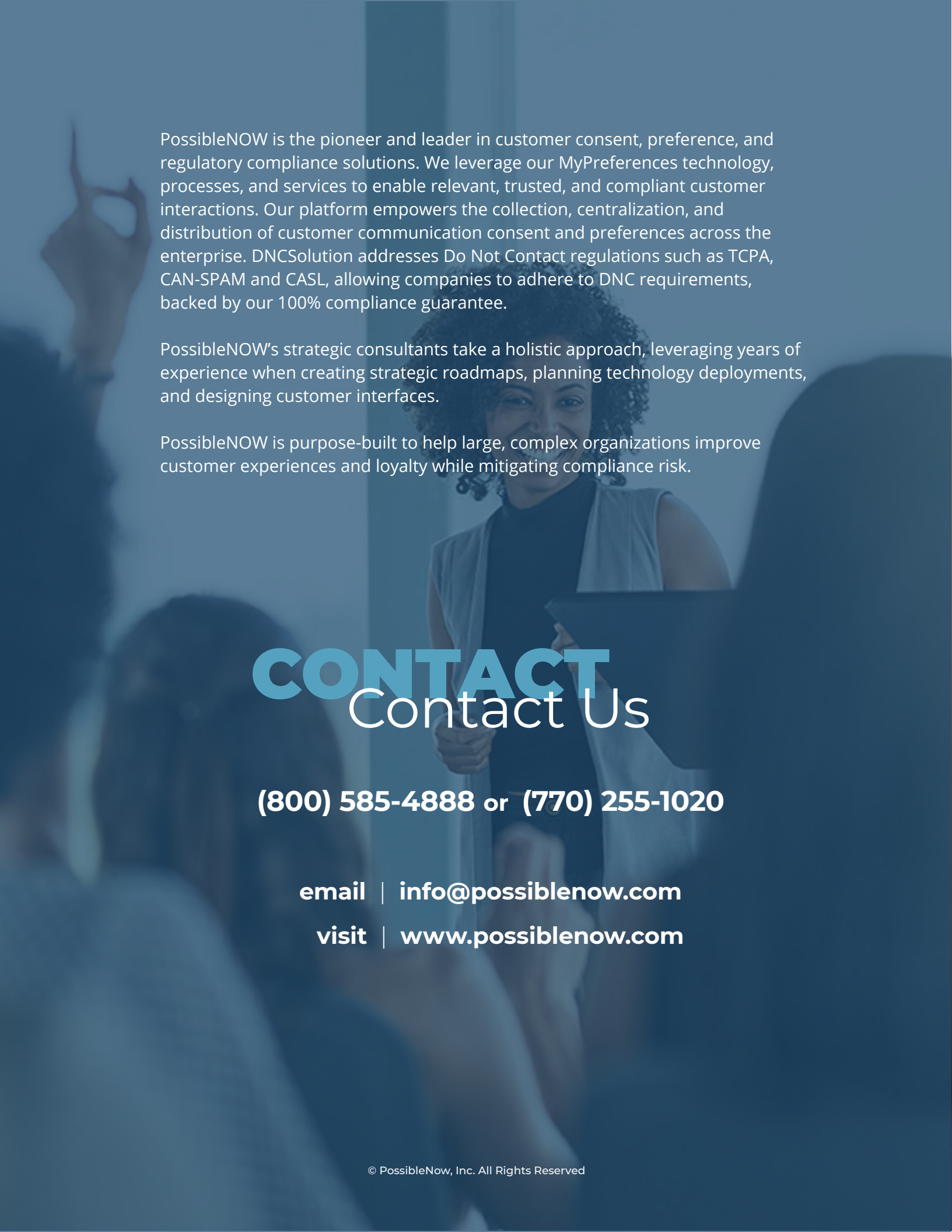
Conclusion

After Mactaggart's realization regarding the amount of personal data processed that consumers are completely unaware of, the Facebook Cambridge Analytica scandal that came to light in March 2018, and the EU's GDPR becoming effective, California became the first state in the United States to initiate a state specific privacy regulation. Chicago and San Francisco proposed privacy legislation to protect personal data processed within their city limits. Brazil recently passed its own privacy legislation, the Lei Geral de Proteção de Dados Pessoais (LGPD), that closely mirrors the GDPR. Finally, New Zealand is in the process of reviewing a new privacy bill to amend its previous data protection legislation to account for technological changes. We will likely see more privacy legislation passed here in the United States, at a city, state, and federal level, as well as on a global level.

Not only will compliance with the potentially various privacy legislations become difficult, but it will also likely serve as a decision-making factor for organizations when determining which third-party vendors and service providers to engage with. Those that already have comprehensive privacy policies and procedures in place will likely prove to be the most successful. So, if your organization has not started down this path, there is no time to waste.

Although the CCPA does not specifically require businesses to contractually oblige vendors and third-party service providers to comply with the CCPA, it is recommended businesses subject to these requirements, contractually require vendors to assist the business in complying with certain rights requests, specifically the right to deletion and the notice requirements. Moving forward, businesses subject to the CCPA should consider implementing a formal onboarding process for new vendors to ensure they have some level of data protection policy in place as well as an ongoing monitoring and enforcement program to periodically monitor vendors for compliance.

The GDPR set the "golden standard" for privacy legislation and brought privacy to the forefront of both consumers' and legislators' minds. Organizations that have prepared for their responsibilities under the GDPR will likely be ahead of the curve in implementing new or adjusting current policies and procedures to meet their obligations under the CCPA and future data protection requirements.



PossibleNOW is the pioneer and leader in customer consent, preference, and regulatory compliance solutions. We leverage our MyPreferences technology, processes, and services to enable relevant, trusted, and compliant customer interactions. Our platform empowers the collection, centralization, and distribution of customer communication consent and preferences across the enterprise. DNCSolution addresses Do Not Contact regulations such as TCPA, CAN-SPAM and CASL, allowing companies to adhere to DNC requirements, backed by our 100% compliance guarantee.

PossibleNOW's strategic consultants take a holistic approach, leveraging years of experience when creating strategic roadmaps, planning technology deployments, and designing customer interfaces.

PossibleNOW is purpose-built to help large, complex organizations improve customer experiences and loyalty while mitigating compliance risk.

CONTACT

Contact Us

(800) 585-4888 or (770) 255-1020

email | info@possiblenow.com

visit | www.possiblenow.com