



interactions

Preparing for the California Consumer Protection Act (CCPA)



Introduction

Interactions is focused on making it easy for businesses and consumers to communicate and get things done. Our Intelligent Virtual Assistants (IVA) for customer care enable our clients to deliver effortless, differentiated customer experience during sales, service, and support stages. Under the new California Consumer Privacy Act (CCPA) rules for data protection and privacy, we are outlining Interactions role under this important statute and its related regulations. This document provides an overview of how Interactions solutions support compliance with aspects of the CCPA that are relevant to our business. At Interactions, we take data privacy and protection very seriously.

Please note that this overview is provided for information only. It does not constitute legal advice. Due to the unique nature of your business, you may be subject to CCPA and other privacy laws in the United States. As a result, we encourage you to consult with your legal counsel to determine your CCPA compliance responsibilities.

History of the CCPA

The CCPA, started as a California ballot initiative in January of 2018, creates rights for consumers and imposes subsequent obligations on organizations. The act and associated statutes are effective as of January 1, 2020.

Scope of the CCPA

The CCPA gives consumers the right to:

- request disclosure of personal information collected
- request disclosure of personal information sold or disclosed for a business purpose
- request deletion of personal information
- opt out of the sale of personal information
- access personal information collected in a portable format
- freedom from discrimination for exercising a consumer right

- receive notice of their rights
- sue for statutory damages in the wake of a data breach

Businesses, Service Providers

The CCPA achieves its objectives by establishing three major classes: businesses, service providers, and third-parties. These distinctions are important because compliance obligations flow from them.

A business is an entity doing business in California that collects, shares, or sells personal information relating to a particular California consumer or household and exceeds any one of the following thresholds:

1. annual gross revenues of \$25 million;
2. processes personal information of 50,000 or more California residents, households, or devices annually; or
3. receives 50% or more of its annual revenue from selling California residents' personal information.

Affiliated companies sharing the same branding may also be required to comply, even if they themselves do not exceed the applicable thresholds, if one of their affiliates qualifies as a business.

Among other things, businesses must:

- train their employees who handle the consumer requests
- create designated methods for consumers to assert the rights identified above and respond to consumers' rights requests in compliance with the CCPA
- execute contracts with service providers that limit the service providers' ability to use the personal information

Entities that process personal information for a business purpose on behalf of and as directed by a business are service providers.

In the context of the provision of our services, our clients are the business and Interactions is the service provider. Each of our clients, in contracts, define the data and how Interactions will process the scoped data. To support our clients' applications, Interactions uses data to carry out customer transactions. In order to improve the

performance of speech and language models, non-contextualized data is used. These automation models benefit our clients by providing improved speed and consistency of responses when the transaction is automated. Interactions does not use any scoped data to build or modify household or consumer profiles, or augment data acquired from other sources. If a client determines that our relationship is in-scope for CCPA, we are prepared to amend existing contracts/MSAs to establish a business-to-service provider relationship.

Interactions Approach to CCPA

Below is a summary of some of the actions we are taking to support our clients' CCPA obligations:

- **CCPA Compliance:** We are partnering with external data privacy experts and have an internal cross-functional team dedicated to supporting our clients' compliance needs including integrating CCPA-compliant protections into our products, systems, and commercial agreements.
- **Right to Access of Data Subject Personal Information:** In anticipation of changing CCPA regulations, a private API is now available to allow our IVA clients who are businesses, as defined by CCPA, to address data subjects' rights requests for rights to access of personal information. The Interactions CCPA API will produce a report in response to any Data Subject Personal information request within the scope of the CCPA containing any personal information on requestee in our system.
- **Deletion of Data Subject Personal Information:** Upon notification of a client request to delete a data subject's information within the scope of the CCPA, Interactions will do so. Interactions never deals directly with our clients' customers. If you believe your business to be in-scope, contact your account manager for more on this capability.
- **Data Breach Notice:** Data breach notification is incorporated into our client contract agreements. Because Interactions currently processes personal information for clients in regulated sectors with breach notification requirements, including PCI, DSS, and GDPR, our processes have been designed to satisfy breach notification requirements.

Additional Data Privacy and Data Security Features of our Services

As a service provider to over fifty Fortune 500 enterprises, including many of the world's most valuable brands, Interactions has always taken a "privacy by design" approach to architecting our platform and applications. Data privacy and data security are paramount to our clients and, as such, they have trusted us to handle their data responsibly and with the utmost care. But ultimately our clients determine what data we collect by defining the prompts and transactions for their application(s), and thus we allow our clients to make additional designations to ensure that data is handled appropriately. Among the data privacy and data security features of our services are the following:

- **Confidential Data Handling:** All information related to prompts that are marked by the client as "confidential" are deleted from our platform post-processing.
- **Secure Data Centers:** Our applications are hosted within highly secure enterprise-grade data centers around the world.
- **Encryption:** Our platform can encrypt sensitive information (using PCI-DSS compliant encryption algorithms) as defined within contract terms as well as to meet regulatory requirements.
- **Secure Data Transport:** Typically we provide for transport of data between our clients' facilities and our data centers over secure MPLS data services, or other encrypted transport methods.
- **Data Retention:** Our retention of data related to providing our services is under the full control of our clients, for both the audio and text that we process. Our clients may specify exactly how this process shall be managed and how long data shall be retained for quality assessment of application performance and improvement purposes.
- **Application Design:** Our application designers and developers are available to work with our clients to ensure that confidential data elements are carefully considered during the design and development process, and appropriate provisions are made to keep them secure. All of our application designs are documented in an "Application Design Document" (ADD) that is approved by our client, often including the client's information security staff.
- **SOC 2 Type 2:** Interactions engages an external audit firm for auditing and reporting against the Trust Services Criteria Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity,

Confidentiality, or Privacy. These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

- **Credit Card Data Handling:** Interactions is certified “PCI DSS Level 1 Service Provider” compliant with regard to the transmission, processing, and storage of credit card information. Level 1 is the highest and most stringent level provided for under the PCI framework. It requires a full on-site compliance audit; self-certification is not permitted.

Conclusion

Interactions has followed “privacy by design” principles to build our solutions from the beginning. These features, combined with the core privacy and security architecture of our services, ensure that our clients' customers enjoy a safe, secure communications experience.

Should you have any questions about any of the content presented here, we would be pleased to arrange a web conference or meeting. Please contact your Account Manager at your earliest convenience.