interactions

Preparing for the GDPR

Introduction

Interactions offers Intelligent Virtual Assistant solutions that enable enterprises to deliver automated customer care with a human touch. This white paper was written for companies seeking to use Interactions' solutions and comply with the General Data Protection Regulation ("GDPR"). It highlights aspects of the GDPR that are relevant to our business relationship and describes what we are doing to comply. We take data privacy and protection seriously. Our GDPR program is intended to help our clients comply with GDPR.

Due to the unique nature of your business, you may be subject to other privacy laws in the EU and other jurisdictions where you process personal data. As a result, we encourage you to consult with your legal counsel to determine your GDPR compliance responsibilities.

The GDPR

Rapid advances in data-driven technologies, human behavior and globalization have resulted in evolving data privacy laws, including the GDPR. The GDPR was adopted in 2016 and goes into full force May 25, 2018 with transparency, choice and accountability at its core. It will replace the existing Data Protection Directive, which was adopted in Europe over two decades ago.

The primary intent of the GDPR is to harmonize data privacy law in the thirty-one states that make up the European Economic Area ("EEA"). The GDPR applies to any company performing data processing within the EEA and companies outside the EEA that collect and use personal data by offering goods or services in the EEA or that monitor customer behavior in the EEA, for example, by tracking online activities or profiling for advertising purposes, regardless of where the data is processed or stored.

The GDPR puts data subjects in the driver's seat and holds businesses accountable for protecting personal data and honoring individual control over it.

Data Controllers and Data Processors

The GDPR achieves its objectives by preserving some of the Data Protection Directive's core concepts, including the distinct roles of data controller and data processor. These distinctions are important because compliance obligations flow from them. The GDPR defines a data controller as a person or other entity “which, alone or jointly with others, determines the purposes and means of the processing of personal data.” In other words, if an organization collects and processes personal data for its own purposes and needs—not merely as a service provider acting on behalf of another organization—it is likely to be a data controller. Businesses that process personal data solely on behalf of, and as directed by, data controllers are data processors. In other words, when a data controller outsources a data collection and processing function to another entity (i.e., a service provider), that other entity is generally a data processor.

In supporting its clients’ applications, Interactions acts as a data processor and its clients act as data controllers. To support its clients’ applications, Interactions uses data to both carry out customer transactions and to improve the performance of speech and language models. Improved automation models benefit the client by providing improved speed and consistency of responses when the transaction is automated. Businesses that use service providers to process personal data of EU data subjects are required to use providers that are both GDPR compliant and support compliance with the GDPR. Interactions is committed to ensuring that our products and service can be used by our clients to support their GDPR obligations.

Interactions’ Approach to GDPR

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

- GDPR Compliance Program: Interactions has an ongoing, fully-funded internal effort under way to address our organization’s compliance with the GDPR and to support our clients in this effort. We are partnering with external data privacy experts and have an internal cross-functional team dedicated to implementing a compliant solution, including integrating GDPR compliant protections into our products, systems and commercial agreements.

- Retrieval/Deletion of Data Subject Personal Data: We are architecting our service to implement a private API to allow our clients who are subject to the GDPR to address data subjects’ rights requests, including the rights to retrieval (Rights to Access, Rectification, Portability) and deletion (Right to be Forgotten) of personal data.

- Confirmation of Erasure: Interactions is implementing a feature that will confirm the date and time of the retrieval or erasure requested by its client so the client will have a record of the task.

- Data Breach Notice: Under GDPR, data controllers may be required to notify the appropriate data protection authority within 72 hours of becoming aware of a personal data breach, and data processors like Interactions may be required to notify their clients “without undue delay” upon discovering a data breach.

Because Interactions currently processes personal data for clients in regulated sectors with breach notification requirements, including PCI DSS and HIPAA, our systems are configured today to satisfy the breach notification requirements of the GDPR.

- EU-U.S. Privacy Shield Certification for Data Transfer from the EU to the U.S.: The transfer of personal data from the EU to the U.S. will be made pursuant to the EU-U.S. Privacy Shield to ensure a level of data protection deemed "adequate" by the EU Commission.

- Use of Standard Contractual Clauses for other Data Transfer: Interactions uses standard contractual clauses approved under the European Commission as a valid mechanism for transferring personal data from the EEA to other countries where appropriate.

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. We operate data centers in Somerville (Boston) MA, Wood Dale (Chicago) IL, Dallas TX, Frankfurt Germany and Dublin Ireland (online April 30, 2018). It should be noted that GDPR in no way prevents enterprises from taking advantage of cloud services. These relationships are covered under the data controller-processor framework.

- *Encryption:* Our platform encrypts media recordings using industry standard techniques recognized by the PCI-DSS Security Council.

- *Secure Data Transport:* Typically we provide for transport of data between our clients' facilities and our data centers over secure MPLS data services.

- *Data Retention:* Data retention policies are 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 applications designs are documented in an "Application Design Document" (ADD) that is approved by our client, and often including the client's information security staff.

- *Credit Card Data Handling:* Interactions is certified "PCI DSS Level 1" 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 onsite compliance audit; self-certification is not permitted.

Conclusion

Interactions was engineering privacy into our solutions before the GDPR was approved, and the GDPR's foundational principles are fully integrated into our "privacy and security by design" approach to our business. In an environment where business-controllers are accountable for the data practices of their service providers, we have engineered a solution to enable our data controller clients to comply with data subject rights and other GDPR obligations. These features, combined with the privacy and security architecture that has been central to our services since day one, ensure that our clients' customers enjoy a safe, secure communications experience. Should you wish to engage with us further on GDPR or any other topic, we would be pleased to arrange a web conference or onsite meeting at your earliest convenience.