GDPR white paper for clients and partners

Nuance GDPR overview

TThe General Data Protection Regulation (GDPR) has broad impacts on the collection and use of the personal data of EU Data Subjects (individuals within the EU). It strengthens EU data subject rights, increases data protection expectations, and provides regulators with the ability to impose up to four percent of worldwide annual revenue as fines. Significantly, the GDPR applies to anyone who collects and processes the personal data of EU residents, even if the processing is done outside of the EU. The new requirements build on the existing EU Data Protection Directive and necessitate enhancements to policies and procedures for handling Personal Data of EU Data subjects.

Nuance is committed to achieving GDPR compliance. This document outlines Nuance's approach to key GDPR requirements and outlines how Nuance supports our customers in their own GDPR compliance efforts.

Controllers and Processors
To use GDPR terminology, when Nuance provides cloud-based products and services that use personal data, we act as a processor of personal data on behalf of our **data controller partners.** The GDPR places obligations on both data controllers and processors. As a processor, Nuance is contractually bound to use EU Personal Data for specific purposes that have been described to data subjects. For additional information regarding Nuance's use of EU Personal Data for a particular product, please review your customer agreement and the Nuance Privacy Notice. For further information, you may also contact us at (privacy@nuance.com).

Personal data handled by Nuance
Commonly, Nuance handles voice information that is provided by partners for voice recognition services. Nuance does not store specific personal identifiers after a message is processed apart from the actual audio file itself. No contact information, data subject names or partner IDs are retained once the initial processing of the audio file is complete.

Voice recordings are collected in snippets a few seconds long and are not stored in a contiguous or consecutive fashion. Therefore, it is not possible to retrieve or isolate any individual voice recording in its entirety. The individual snippets are too short to permit the identification of the individual to which the file belongs or to retrieve files for a specific individual in the majority of our systems.

Nuance sells a variety of products and services that do store personal identifiers, including medical software and transcriptions services. The product and customer support services provided across all Nuance divisions also frequently involve the processing of personal information. Where Nuance holds personally identifying information, we work with customers to help them meet any data subject rights requests under the GDPR. Nuance does not use data provided by customers for purposes beyond contractual services and product enhancement (e.g. retaining a physician's voice recordings to improve the accuracy of future transcriptions).

More information on how Nuance handles Personal Information can be found on Nuance's Privacy Notice.

What Nuance is doing to comply with GDPR?

Like many companies operating in the EU prior to the GDPR, Nuance complied with the EU Data Protection Directive and incorporated privacy controls and de-identification capabilities into its products for many years. In 2017 Nuance completed a comprehensive assessment of the new GDPR regulation and evaluated Nuance's security and data protection practices to see if they met the prescribed requirements or needed enhancement. Nuance's responses to some key requirements of the GDPR are covered on the following pages.

What's required by GDPR

Privacy Oversight

Organizations collecting personal data in the EU should expect regulators to be increasingly active and should be able to demonstrate compliance with the GDPR. Penalties have substantially increased under the GDPR.

Nuance's Response

Nuance has a dedicated team of privacy experts overseeing and maintaining its privacy program and has policies to safeguard EU personal data in line with the requirements of GDPR. Nuance has also appointed a Chief Privacy Officer / Data Protection Officer with GDPR oversight.

In addition, we will be conducting routine privacy audits that will include GDPR compliance checks. Finally, all Nuance staff handling EU personal information receives privacy training that covers the GDPR.

Data Security

All data must be protected through adequate technical measures to ensure a level of security appropriate for the risk the data carries.

Nuance's Response

Nuance has implemented a robust set of security controls, in accordance with various industry standards. Technical, physical, and administrative controls are implemented at both the application and server levels to provide security, confidentiality, availability, processing integrity, and privacy controls. For example, Nuance has technical security controls in place to restrict access to personal data to individuals with a business need to know and retains information for specific, limited time periods and, for many products, de-identifies information once processing is complete.

Security Breaches

The GDPR requires data breach notification to the supervisory authority within 72 hours after the controller becomes aware, with notification to data subjects if warranted by the risk.

Nuance's Response

Nuance has established critical incident and breach reporting processes and regularly reviews its processes to evaluate compliance with regulatory requirements. Nuance is familiar with breach reporting requirements due to many years' experience as a processor of medical data to healthcare organizations in the United States under HIPAA. We also have processes in place to provide the required supporting information to generate a complete breach notification and report for partners. These processes can be used in concert with a specific external breach management process and communication plan developed in conjunction with specific partners.

Data Protection Officer

Controllers and processors are required to appoint a Data Protection Officer in certain circumstances, such as if they engage in regular, large-scale processing of data.

Nuance's Response

Nuance has appointed its Chief Privacy Officer, Catherine Castaldo, as Data Protection Officer for Nuance Communications, Inc. and its affiliated companies.

Personal Data Governance and Privacy by Design

Compliance with a number of GDPR requirements, including privacy by design and the performance of data protection impact assessments, requires a strong data governance structure.

Nuance's Response

Nuance has established a privacy team headed by the Chief Privacy Officer that includes a privacy program manager and privacy attorneys allocated to Nuance divisions and functions, including Healthcare, Enterprise and Automotive, and functions such as Marketing and Human Resources.

Nuance has a dedicated privacy team that provides support during all stages of product development. We have identified major requirements under the GDPR, which have been translated into specific design requirements. The resulting design controls are incorporated at the appropriate stages of product development.

The privacy team performs Privacy Impact Assessments (PIA), consults on contract issues that touch on data use and protection, and advises on a broad range of privacy issues.

Data Minimization and Limited Retention

Data Minimization must be ensured through all stages of processing:

- ***At the point of collection:*** **Collection of personal data shall be limited to the minimum amount of Personal Data (in nature and volume) that is strictly necessary to fulfill the consented purposes.**

- ***In personal data generation:*** **Where personal data is observed, derived or inferred by the system, it shall be restricted to the minimum amount of personal data that is strictly necessary to fulfil the consented purposes.**

Moreover, personal data should only be processed and retained as long as necessary to fulfill the purposes for which it was collected and no longer.

Nuance's Response

While the data collected is largely the responsibility of the controller, Nuance has a privacy review process in place that considers data collection and use.

Records of Processing

As a data processor on behalf of our customers, Nuance is required by the GDPR to maintain records of data processing activities, including the purpose of the processing, the categories of data subjects, and any cross-border transfers.

Nuance's Response

Nuance is documenting all major data processing activities affecting EU Personal Data that will provide appropriate records of Nuance's data processing.

If partners need further information from Nuance to complete their data mapping and processing libraries we will work to ensure that all data needed from Nuance is provided.

Data Subject Rights

The GDPR provides data subjects with stronger rights to control their data, including rights of access to data, to correction of inaccurate data, and in certain circumstances to data deletion.

Nuance's Response

Nuance is committed to responding promptly to all requests we receive from individuals exercising data subject rights. Customers should be aware that much of the data we hold is not attributable to any particular individual.

Where Nuance holds personally identifying information, we work with customers to help them meet any data subject rights requests under the GDPR.

Third Parties

Additional requirements will apply to the contracts between Nuance and its customers, as Article 28 of the GDPR requires specific data processing provisions in contracts between controllers and processors.

Nuance's Response

Where Personal Data hosting is performed by a third party vendor, Nuance reviews the vendor's policies, procedures and controls to ensure that an adequate level of security is maintained.

Nuance has revised its standard contracts for European customers to include new data processing provisions that address the requirements of Article 28, including control of sub-processing, assistance with data subject rights, and audit and inspections.

Lawfulness of Processing

Processing of personal data is lawful only if one of the six conditions listed in the GDPR is met (for example, if there are legitimate interests, if it is necessary for the performance of a contract or if it is required for another regulatory compliance or legal reason to hold). Consent is one of the six factors, but under the GDPR, consent requirements have become stricter. Among other key changes, the GDPR provides data subjects with an enhanced ability to withdraw consent at any time.

Nuance's Response

Determining the lawfulness of the processing of data is the responsibility of our clients, as Data Controllers. As a Data Processor, Nuance is required to abide by clients' lawfulness determinations and process the data in accordance with contractual requirements.

Cross Border Transfers

Transfers of personal data to countries outside of the EEA are generally permitted (a) to countries that are deemed by the European Commission to provide for an "adequate" level of personal data protection, (b) with the use of standard contractual clauses, (c) through binding corporate rules (BCRs), or (d) to the United States, through compliance with the Privacy Shield framework.

Nuance's Response

Nuance has standard data protection agreements that include model contract clauses to permit the transfer of data from the EU to the US. We also hold Privacy Shield certification. Finally, where our clients have adopted BCRs, we are willing to sign data processor agreements that bind Nuance to the terms of those BCRs.

Cloud Offerings and On-Premise Products

Nuance offers many products that store data in the cloud. In these instances, Nuance has access to the data and serves as a data processor. Nuance also offers a number of on-premise products that store data on servers owned or operated by our clients. In these instances, Nuance generally does not have access to the data, is not a data processor, and does not play a role in GDPR compliance activities. However, Nuance does provide customer support services for on-premise products, and our customer support activities occasionally involve access to personal data. To the extent that Nuance receives EU personal data in the course of providing customer support services, we fully comply with the requirements of the GDPR.

What to expect going forward

As the requirements of the GDPR gain additional clarity through regulatory guidance and enforcement, Nuance expects to further enhance its customer GDPR program. As the program is enhanced, we will update this guidance with more detail.

If you have specific questions about how Nuance will assist you with your obligations under GDPR please email (privacy@nuance.com).