GDPR white paper for clients and partners

Overview

The new General Data Protection Regulation (GDPR) regulation impacts companies in many ways. It will increase EU data subject rights, increase data protection expectations, and provide regulators with ability to enforcement options including fines of up to four percent of worldwide annual turnover. Significantly, the GDPR applies to anyone who is collecting and processing EU personal data, even if the processing is done outside of the EU. The new requirements build on the existing EU Data Protection Directive and present significant challenges to companies handing Personal Data of EU data subjects. This document is intended to outline Nuance's approach to the key GDPR requirements and outline how Nuance intends to support our customers in their own compliance efforts.

Controllers and Processors
To use GDPR parlance, when Nuance provides you with products and services that use personal data, we act as a **processor** of personal data on behalf of you, the controller. The GDPR places obligations on both controllers and processors. As a processor, Nuance is bound to use EU Personal Data for specific purposes that have been described to data subjects (Individuals within the EU). If you need further information on how Nuance may use EU Personal Data for a particular product please review your customer agreement and the Nuance Privacy Notice. For further information, you may 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. By design, Nuance does not store specific personal identifiers after a message is processed apart from the voice file itself, which Nuance cannot tie to any specific individual for most products. In virtually all products, the voice file itself is also insufficient to serve as an identifier either from the characteristics of the voice or from the content. Further, no contact information, data subject names, or partner ID's are retained once processing is complete. As such, Nuance does not and cannot identify the individual to which the file belongs nor can Nuance retrieve files for a specific individual in the majority of our systems.

For medical products and services that may include personally identifying information Nuance will work with customers to help them meet any potential data subject rights under GDPR. Commonly, identifiers are not held on any patient but

information may be held on a specific physician for a medical institution. Voice recordings are stored in snippets a few seconds long and are not contiguous. It is not possible to isolate any individual voice recording in its entirety. 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 accuracy of future transcriptions). More information on how Nuance handles personal Information can be found on Nuance's Privacy Notice.

If a partner wishes to receive a voice log to respond to a Data Subject Access Request, Nuance can only retrieve information that is less than 90 days old and can only locate voice files based on a partner ID.

What Nuance is doing to comply with GDPR?

Like many companies operating in the EU, Nuance already complies with the EU Data Protection Directive and has incorporated concepts of privacy and de-identification into its products for many years. Nuance has been actively working towards GDPR compliance. In 2017 Nuance completed a comprehensive assessment of the new regulation and evaluated Nuance's security and data protection practices to see if they met the described requirement or needed enhancement. Nuance's response in some key areas of 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 will be substantially increased from the current framework.

Nuance Response
Nuance has a dedicated team of privacy experts overseeing and maintaining its privacy program and policies to safeguard EU personal data in line with the requirements of GDPR and has 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 will receive privacy training that covers the GDPR.

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

Nuance 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. Specifically, Nuance has technical security controls in place and restricts access to personal data to only individuals with a business need to know and retains information only for specific time periods prior to deletion 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 response
Nuance has established critical incident and breach reporting processes and regularly reviews its processes to meet 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 response
Nuance has appointed a Data Protection Officer for Nuance Communications, Inc. and its affiliated companies. The contact information for the Data Protection Officer can be found in our Privacy Statement.

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 in organizations subject to GDPR.

Nuance response
Nuance has established an experienced 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 to 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 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. Nuance has created affirmative controls that minimize the amount of personal data crossing into Nuance's processing environment. Nuance is committed to assessing and re-evaluating these controls for potential enhancements over time as technologies continue to evolve.

Records of processing
As a data processor on behalf of our customers, Nuance is required by 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 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 data subject rights to control their data, including rights of access to data, to correction of inaccurate data, and in certain circumstances to data deletion.

Nuance response
Nuance is committed to responding promptly to all requests we receive for exercise of data subject rights. Customers should be aware that much of the data we hold is not attributable to any particular individual. In our Healthcare division, where Nuance has been required to support our customer's responses to access requests for some time, we have received few access requests given the nature of the data we hold.

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 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 is revising its standard contracts for European customers to include new data processing provisions that address the issues required by Article 28, including control of subprocessing, assistance with data subject rights, audit, and inspections.

Lawfulness of processing
Processing of personal data will be lawful only if one of the six factors listed in the GDPR is present (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 will become stricter. Among other key changes, the GDPR provides data subjects with an enhanced ability to withdraw consent at any time.

Nuance 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 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 are also in the final stages of completing 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.

What is Nuance doing to support data controllers?

Nuance is committed to supporting our customer's commitments under GDPR in a variety of ways and is actively working towards ongoing GDPR support. Some key topics are listed below:

Data Subject Rights
GDPR provides additional rights to data subjects including the right to be forgotten and portability to supplement the existing rights of access and correction. As Nuance does not hold identifiable information for most products beyond 90 days and that is only identifiable to partnerprovided identifiers. Nuance is unable to verify identity or retrieve information for a specific data subject's recording based on personal identifiers e.g. name, telephone number, VIN number, or similar identifier. Nuance already works with partners using products with identifiable Personal Data to provide access and correction as needed.

Data de-identification and deletion
Nuance retains data only for a limited time to support processing and then may retain some data longer to support the accuracy of voice recognition for customers. Information that is retained, for most products, has most individual personal identifiers removed at the point of entry to the Nuance processing environment and any remaining identifiers are removed once processing is complete. Nuance rarely has details on an individual for customer products. Information is then further de-identified prior to research analysis for product enhancement. Nuance is committed to an active cycle of evaluating data processed to minimize any personal data it holds.

What to expect going forward

As Nuance works to further enhance its customer GDPR program 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).