AVAYA

PERSONAL DATA CONTROLS FOR ENABLING GDPR COMPLIANCE PROGRAMS

DISCLAIMER This document has been prepared by Avaya. The intent of this document is to provide information to Avaya customers and business partners that will help them with their privacy programs. It may help customers and business partners in preparation for their own implementation of privacy as well as working towards General Data Protection Regulation (GDPR) compliance. This information is based on Avaya's understanding of the regulation and is not intended to be a definitive interpretation of GDPR. In preparing for the GDPR, all organizations must take responsibility for understanding the GDPR and their responsibility as data handlers, whether that be as controllers or processors.

GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) has been introduced by the European Union to strengthen and unify data protection for European Union residents. The Commission's primary objectives via the GDPR are to give individuals back the control of their personal data and to simplify the regulatory environment for international business.

GDPR came into effect on May 25, 2018. All companies and government organizations that offer goods and services to individuals within the European Union or collect and analyse the personal data of EU residents are subject to the new legislation—regardless if the entity is physically located within the EU or not.

HOW DOES GDPR AFFECT AVAYA CUSTOMERS?

Organizations that use Avaya products to handle personal data, will be doing so as either data controllers or processors. They are obliged to implement technical and organizational measures that demonstrate how personal data is protected. They will need to be cognisant of data protection principles and how they should be applied. Below are some basic requirements they will need to comply with-

- **Understanding the Personal Data Processed –** Organizations must identify what personal data they hold on an individual—a customer or employee.

  This includes information relating to an identified or identifiable person, and any information which may be subsequently linked to that individual.

- **Data Protection by Design and Default -** An organization has a general obligation to implement technical and organizational measures to show that it has considered and integrated data protection principles into processing activities.

- **The Rights of the Individual –** Under the GDPR, an individual can exercise rights against data controllers. These include the rights to access, erasure, portability and rectification. The ability to effectively process and service these rights must be considered by the controller.

As GDPR principles seek to regulate organizational behaviours in the collection and processing of personal data, a product by itself cannot be said to be either "GDPR-Compliant" or not. Still, there are important product features and controls outlined below that can facilitate an organization's achieving GDPR compliance when they handle personal data.

WHAT IS PRIVACY?

Privacy is the right to be left alone, or freedom from interference, observation, evaluation or intrusion. Information privacy is the right to have some control over how your personal information is collected and used.

Data privacy is focused on the use and governance of personal data—things like putting policies in place to ensure that consumers' personal information is being collected, shared and used in appropriate ways.

For example, the mere fact that you made a phone call to a doctor or that you are planning visiting a doctor, or a specific specialist is a matter of your own privacy.

WHAT IS PERSONAL INFORMATION?

Personal data is any information relating to an identified or identifiable natural person. "Identifiable" means data that can be traced back to an individual. Even if personal data is published, it remains classified as personal data and subject to privacy rights.
For example, the following are considered personal data:

- Name, including maiden name, family name(s) and names of identifiable relatives
- Image of a person
- Employee personnel number
- Address/ email address
- Telephone number
- Passport number/ national ID
- Driver's license number
- Insurance policy number
- Education/ CV information
- Website user ID
- Payroll data
- Date of birth
- IP address leading to end-user PC
- Certain usage/ performance statistics
- Racial or ethnic origin, political opinions, religious or philosophical beliefs
- Trade union memberships, social security number, tax or other similar identification numbers used by government agencies
- Personal financial information including but not limited to bank account numbers, credit card numbers or debit card numbers
- Health, criminal record, sexual orientation, genetic and biometric data, etc.

SECURITY OF PROCESSING

All personal data in transit and stored must be protected by suitable technical and organizational measures. This means measures such as, for instance, encryption and/or access-control.

Avaya products store personally identifiable data in different locations and transport data using different protocols. Details are provided in each product's "Data Privacy Controls Addendum" document.

It is generally understood that proper information security policies and practices must be in place as a pre-requisite for compliance with GDPR.

INDIVIDUAL'S RIGHTS UNDER GDPR

The GDPR not only includes security and accountability principles that requires controllers to consider all aspects of their data processing activities, it also empowers the individual with some new and additional rights over the storage and use of their data.

Under the GDPR an individual can require data controllers to grant them rights of access, erasure, portability and rectification over their personal data. The ability to effectively process and service these rights needs to be considered by the controller, who must assess if any changes are required to policies, business processes and supporting systems.

The purpose of this section is to describe the functional capabilities of Avaya products, relative to each individual right. Consideration and examples will be provided for an 'employee' and an 'end-customer'.

THE RIGHT OF ACCESS

Within the GDPR, an individual has the Right of Access, which provides for various rights, including confirmation from a data controller as to what data is being processed about them, to whom this is disclosed or transferred and whether the personal data is subject to automatic decision making. A data controller must, without charge, provide a copy of the personal data held and processed by it to the data subject in electronic form and has up to one month to comply with the request (unless the requests are complex or numerous, in which case the deadline is extended to no more than three months in total).

In servicing the individual's right, the controller must verify the identity of the person making the request, and, if the request is made electronically, should provide the information in a commonly used electronic format. Compliance to this part of the GDPR requires the ability to find an individual's data across all information systems, and then produce a report.

THE RIGHT OF RECTIFICATION

Under the GDPR an individual has the Right of Rectification, meaning the individual is entitled to request to have their personal data rectified if it is inaccurate or incomplete. A controller has up to one month to comply with the request or show cause for denial (unless the requests are complex or numerous, in which case the deadline is extended to three months).

THE RIGHT TO DATA PORTABILITY

The GDPR offers the Right to Data Portability for an individual. This right allows the data subject to obtain and reuse their personal data for their own purposes across different services. In effect, this right means that the individual has the right to access and transfer personal data from one controller to another without being obstructed due to "technical limitations" claimed by a controller. This right arises on personal data which the data subject has provided the controller with. To service the individual's right, the controller must provide the personal data in a structured, commonly used and machine-readable form, such as .CSV files (although GDPR does not prescribe the format).

Compliance to this part of the GDPR may require the ability to find and copy an individual's data across all information systems and deliver a copy to the individual.

THE RIGHT TO ERASURE

The Right to Erasure, also known as 'the right to be forgotten', enables an individual to request the deletion or removal of personal data where there is no lawful reason for its continued processing or where the data subject withdraws consent. The organization can refuse to comply with a request for erasure where the personal data is processed to comply with a legal obligation or for other "public interest" reasons, such as to exercise the right of freedom of expression and information. As such, the right to erasure does not provide an absolute "right to be forgotten".

Compliance to this part of the GDPR may require the ability to find and delete an individual's data across all information systems.

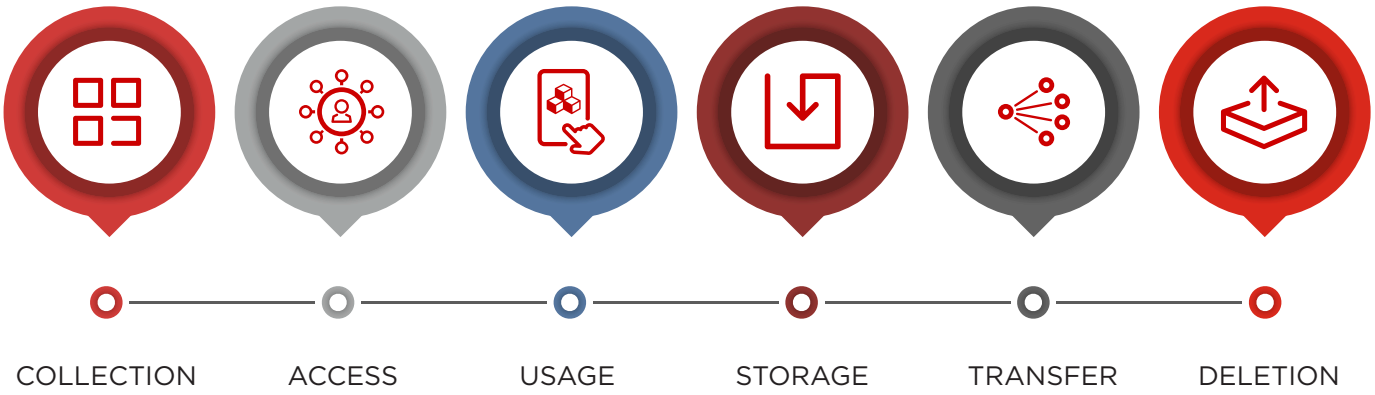
THE OBLIGATION TO HAVE A LAWFUL BASIS TO PROCESS PERSONAL DATA

A Data Controller is obligated to have a legal basis for the personal data they collect and process. For information systems that have the capability to track or record communications or transactions, an individual may have the right (depending upon the legal basis for the tracking or recording) to give or withhold consent at any time.

Compliance to this part of GDPR will in some instances require the ability to gain consent as a legal basis prior to data collection. Certain Avaya products provide the ability to customize the user experience. These customizations may aid in obtaining informed consent. For example, special announcements may ask a caller to acknowledge their understanding that a call is to be recorded before granting admittance. On screen-based interfaces, customized banners can convey a privacy policy prior to account creation, login, etc.

DATA LIFECYCLE

When developing business processes around individual's rights under GDPR, it is useful to consider the lifecycle of personal information in the business.



From the lifecycle diagram, you can determine the key aspects that must be considered in the development of a business's GDPR processes and procedures.

- What is the use of the data collected?
- How is it collected and where is it stored?
- What is the legal basis for processing the data?
- How is consent to collect and process the data obtained, if required?
- How is the data accessed for the defined usage?
- How is unauthorized access to the data prevented?
- How and when will the data be transferred out of your control?
- How and when is the collected data destroyed, deleted or returned?

AVAYA PRODUCTS AND PERSONAL INFORMATION

In evaluating the questions noted above and developing company compliance processes, it is important that all IT systems – including the Avaya systems- be considered. Within the scope of Avaya products, personal information may be involved in almost all transactions of the system including voice and video calls, conferences, and text messages. This information will be stored in multiple places including recordings, databases, system logs, directories, histories, and backups.

PERSONAL INFORMATION COLLECTION

Avaya products collect personal information for specific needs -- for example, collecting a name and a phone number in a phone directory to allow connection with the person at a later date, or collecting the assigned user and IP address of a phone to route calls.

Some information may be saved in system logs for future diagnostic or audit purposes. When the information is no longer needed, these logs may be destroyed.

System backups may also capture some personal information to the extent it exists in the data being backed up. For this reason, both the active system data and backups must be considered when assessing the information in Avaya products.

Details of personal information collected by Avaya products are captured in the Data Privacy and Controls document for each product.

SUPPORTING THE PERSONAL DATA LIFECYCLE

Avaya products incorporate multiple capabilities to support the data lifecycle and compliance with GDPR. Some of the different types of capabilities are described below.

ENCRYPTION

Encryption at rest secures the content of a file or database in a manner that makes it un-usable by anyone who does not have the proper authorization. Some Avaya applications have options to support encryption, while others do not. For those that do not, compensating controls can be put in place. (See Access Controls below.)

Encryption in transit needs to be applied to all data communication in the systems. Most Avaya applications and product support TLS1.2 with the latest encryption (AES256 for confidentiality and SHA-2 for hashing, and digital signatures for authentication).

MENUS

Some Avaya products support the development of interactive menus where customers can be prompted and provide feedback. In many cases, these menus can be used to acquire the consent needed to collect and use the personal information.

ACCESS CONTROLS

Most Avaya products provide access controls that can be used to limit the ability of individuals or systems from accessing collected data. A variety of access controls may be provided as follows:

Passwords – Passwords are used to gain access to the system. These can be defined by the system or linked to a larger, corporate directory. When system passwords are used, password policy controls are provided such as complexity rules, lock-outs on failed attempts, required change intervals, etc.

Multi-Factor Authentication – Some products support multi-factor authentication. Access is forbidden unless the configured type and number of authentications are provided. This is typically configured to be a password and special authentication card.

Role Based Access Control – Role based access controls or "RBAC" allows for the system to grant fine-tuned capabilities to each log-in that has been assigned to a "role" in order to manage what they can access and change in the system.

Certificates – Avaya products leverage X.509 certificates that are used to secure the communication exchange between two different system elements ensuring that the communication is authentic and confidential. Communications exchange can be further protected by requiring each communication element to mutually authenticate the other side before exchanging information. Mutual Authentication requires certificates to be generated and installed on each communication element. Certificates can be generated directly by the system, by the enterprises certification generation facilities, or by 3rd party public entities.

Filesystem Access Controls – File access controls restrict ownership, and the type of information access granted to individual accounts within the operating system of the product.
These controls should be configured to adhere to the security principle of least-privilege.

Network Access Control Lists – Access control lists restrict network connections according to predefined "allow" and "deny" lists kept local to the system.

AUDIT LOGS

Audit logs, especially security audit logs, are also a key part of managing compliance. Audit logs record system activity and can be used to identify possible problems or cyber-attacks.

CUSTOMER SPECIFIC CUSTOMISATIONS

Avaya products are meant to be general purpose and can be configured and integrated into a customer's overall business information processing architecture. It is expected that Avaya and non-Avaya equipment work together to perform overall information processing for the business. It is also common to use certain Avaya products (such as Avaya Aura Experience Portal) to execute information processing scripts that have been written or customized by the customer or other agents.

Whenever customized configurations or application scripts are in use, the GDPR concerns must be assessed across the overall solution.

SUMMARY IN SUPPORT OF GDPR REQUIREMENTS

The GDPR provides individuals with rights of access, rectification, erasure and portability over their personal data held by organizations. The regulation will affect all systems which process personal data used by an organization, including their Avaya communications infrastructure.

Avaya products must be therefore considered when developing strategies and processes that enable businesses to comply to the GDPR. The Data Privacy and Controls Addendum document produced for each product provides the details of personal information collected by the product as well as the controls available to meet the data lifecycle denoted above.

FINDING SPECIFIC INFORMATION

Details of privacy-related security controls and available methods of access and manipulation in Avaya products are captured in the Data Privacy and Controls Addendum document for each product.

The Data Privacy Controls Addendums for each product is located on support.avaya.com. To find and access the documents, log in and navigate to the product in question and select the documents tab. You will find the document in the list produced. For easier access, you can elect to search for “GDPR” in the search box at the bottom of the page selecting all the documents types to search. For a list of all the GDPR document available, navigate to the support.avaya.com home page and then search for “GDPR” in the search box for the full site.


AVAYA