



Genesys Cloud privacy policy

This Privacy Policy outlines our practices for collecting, using, maintaining, protecting and disclosing Customer Data, including Personal Data, through Genesys Cloud, and what we do with that information. Additionally this Privacy Policy describes the privacy principles followed by Genesys Telecommunications Laboratories, Inc. (“Genesys”) with respect to international transfers of Personal Data (defined below). If you have questions about this Privacy Policy, or how we respect your information, contact us at DataPrivacy@genesys.com. For the purposes of this Privacy Policy, “Customer Data” means the Genesys customer’s proprietary information and information about its customers (including Personal Data) submitted through Genesys Cloud by the customer and its agents. Customer Data does not include aggregate data and information related to the performance, operation and use of the Cloud Services. “Personal Data” means any information relating to individuals that is protected by applicable privacy law.

What Customer Data does Genesys collect through the Genesys Cloud services?

In general, Genesys Cloud manages consumer engagements via various media channels. Genesys Cloud processes information related to the consumer engagements (audio call recordings, call meta-data, chat messages, etc.). Genesys Cloud also collects information that a customer organization already stores by connecting with services such as Active Directory and Customer Relationship Management (CRM) software. Additionally, a customer may choose to provide information to Genesys Cloud, such as through importing information from third party websites, uploading files, screensharing, video or audio calls, or chat messages.

Genesys will only collect Customer Data when it is voluntarily made available to us by a customer.

How may Genesys use Personal Data collected through the Genesys Cloud services?

Genesys will use this information to provide Genesys Cloud services. If recording is enabled, Genesys will collect and store interaction recordings. Genesys also uses some Personal Data to route calls or webchats and maintain records of these interactions. There are additional functions that Genesys Cloud can provide. For example, Genesys Cloud can facilitate a customer agent to share files with other members of their organization. As another example, a customer agent may share their screen with other members of the organization.

Genesys will also use this information to comply with Customer requests. For example, if a customer requests technical support assistance, Genesys will use data to help troubleshoot the issue (location, call data, customer agent data, etc.). If a customer is interested in signing up for a Genesys webinar, the Customer Data provided will enable Genesys to tailor the webinar more closely to specific needs. In addition, Genesys may refer to Customer Data to better understand customer needs and how Genesys can improve our products and services. Genesys may use that information to contact customers.

Genesys does transfer Customer Data stored outside the country where customers are located in order to carry out the Services and other obligations under the Agreement.

Genesys has developed and maintains a privacy program designed to respect and protect Customer Data under its control. Genesys will not rent or sell any Customer Data.

Genesys may aggregate data and information related to the performance, operation and use of the Cloud Services to create statistical analyses, to perform benchmarking, to perform research and



development, and to perform other similar activities (“Service Improvements”). Genesys will not incorporate Customer Data in Service Improvements in a form that could identify customers or their consumers, and Genesys will use industry standard techniques to anonymize Customer Data prior to performing Service Improvements. .

How may customers direct or restrict the use of their information?

The customer can limit the amount of data that is processed by Genesys by limiting the collection of data through the Genesys Cloud service. For example, if the customer does not wish to collect government identification numbers, agents should be trained to not ask for those numbers or use a secure-pause feature to prevent that information from being recorded. Certain features, such as screensharing and video chat, allow users to direct the use of their information. For example, when a user initiates a screensharing session, the user may choose which aspects of the screen to share, who can view those aspects of the screen, and when to stop sharing the screen.

Some Personal Data is considered Sensitive Personal Data, such as any Personal Data that reveals race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, information that concerns health or sex life, and information about criminal or administrative proceedings and sanctions. Genesys will not disclose Sensitive Personal Data to a third party that is not authorized or use Sensitive Personal Data for a purpose other than the purpose for which it was originally collected, unless Genesys has received affirmative and explicit consent to do so (opt-in).

For additional information regarding how customers may restrict the use of Personal Data please contact Genesys at DataPrivacy@genesys.com.

What steps will Genesys take before transferring your information to third parties?

Genesys Cloud uses third-party data processors around the world to provide certain services, such as a cloud storage, security monitoring, and troubleshooting. These third-party data processors may process Personal Data provided by Genesys, on its behalf and under its instruction. Genesys ensures that it obtains assurances from these third-parties to safeguard Personal Data in accordance with this Privacy Policy.

Such assurances include:

- Requiring third parties to provide at least the same level of protection as is required under this Privacy Policy;
- The use of Standard Contractual Clauses as a basis for transfers of data from the European Union to non-adequate countries;
- Requiring the third party to comply with governmental data protection regulations, such as EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR), or other applicable laws.

How can a customer access or correct information held by Genesys?

The Genesys Cloud service has built in tools in order to respond to subject right request under GDPR. More information on these tools can be found at: <https://help.mypurecloud.com/articles/gdpr-overview/>

How will your information be protected?

Genesys is committed to protecting the Personal Data. Genesys have implemented appropriate physical, electronic and administrative procedures to safeguard and secure this information from loss, misuse, unauthorized access or disclosure, alteration and destruction.



More information about the technical and organizational measure used by Genesys, please see: <https://help.mypurecloud.com/articles/genesys-cloud-security-policy/> .

What information may be gathered from children?

The Genesys Cloud services are not intended or designed to attract children under the age of 13. Genesys does not collect personally identifiable data from any person it knows to be under the age of 13.

How will we ensure compliance with this policy?

Genesys conducts compliance audits of our privacy practices to verify compliance with this Privacy Policy. Any Genesys employee that is determined to have acted in violation of this Privacy Policy will be subject to disciplinary action up to and including termination of employment.

Any questions or concerns regarding Genesys' use or disclosure of Personal Data should be addressed to DataPrivacy@genesys.com. Genesys will investigate and attempt to resolve any complaints and disputes regarding the use and disclosure of Personal Data in accordance with the provisions of this Privacy Policy.

International Data Transfers Under GDPR

Genesys uses Standard Contractual Clauses ("SCCs") as a basis for personal data transfers from the EU to non-adequate countries. Genesys enters into SCCs with customers in its role as a data importer, and it enters into SCCs with third-party vendors in its role as a data exporter. Genesys understand that controllers are required to perform a transfer assessment in some instances when using SCCs. To that end, Genesys has prepared a transfer assessment for the Genesys Cloud service. Customers may contact Genesys if they wish to receive a copy.

While the Privacy Shield framework is no longer a valid mechanism for the transfer of personal data from the EU to the US under GDPR, Genesys remains a party to Privacy Shield and continues to follow its obligations and responsibilities. To learn more about the EU-U.S. or U.S.-Swiss Privacy Shield Framework and to view Genesys' certification, please visit www.privacyshield.gov.

Changes to this Privacy Policy

Any changes made to this Privacy Policy will be posted on this page. The date the Privacy Policy was last revised is identified at the bottom of the page. If Genesys make material changes to how Genesys treats Personal Data that falls within the scope of this Privacy Policy, Genesys will notify customers by email, as specified in the customer records, or through a notice in the Genesys Cloud services.

The customer is responsible for ensuring Genesys has an up-to-date, active and deliverable email address, and for periodically visiting the Privacy Policy to check for any changes.

Who should a customer contact if they have any questions concerning this Privacy Policy?

Genesys encourage customers to inform Genesys of any complaints or disputes it may have regarding the use of Personal Data. Genesys will investigate the matter and attempt to resolve the issue quickly.

Please contact Genesys at DataPrivacy@genesys.com with any questions or concerns about this Privacy Policy or the use of Customer Data.

Revision date

December 2020