



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

# Genesys Security Deployment Guide

General Data Protection Regulation (GDPR)

---

## Contents

- 1 General Data Protection Regulation (GDPR)
  - 1.1 What is GDPR?
  - 1.2 What data comes under the scope of GDPR?
  - 1.3 How does Genesys support compliance with the rights defined by GDPR?

# General Data Protection Regulation (GDPR)

This page provides general information about Genesys support for customer compliance with the General Data Protection Regulation (GDPR).

## What is GDPR?

GDPR is a regulation in EU law passed by the European Union in 2016, setting new rules for how companies manage and share personal data. It addresses the export of personal data outside the EU. The GDPR is applicable for enterprises across globe that store EU citizens data.

The regulation applies if the data controller, an organisation that collects data from EU residents, or processor, an organisation that processes data on behalf of a data controller like cloud service providers or the data subject (person) is based in the EU. The regulation also applies to organisations based outside the EU if they collect or process personal data of individuals located inside the EU.

### Important

The purpose of this document is to help organizations understand how Genesys Services can be utilized to help them comply with certain regulatory requirements, including EU General Data Protection Regulation. Some of the Genesys Services features described herein may or may not be available based upon an organization's specific environment and Genesys Services acquired.

The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their processing of personal data, including through the use of Genesys' products or services.

## What data comes under the scope of GDPR?

According to the European Commission, "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address." This data is called personally identifiable information (PII).

## How does Genesys support compliance with the rights defined by GDPR?

Genesys holds EU citizens' data for the purposes of executing processing on behalf of customers. While Genesys customers are the data controllers for GDPR purposes, Genesys has a responsibility to support customer compliance with GDPR requests. The following table describes Genesys support for GDPR rights.

Right	Genesys Support
Right of Consent	Requirements to meet Right of Consent apply outside the Genesys platform. In general, Genesys does not collect data unless it has been determined to be necessary to meet the use cases of customers, who are the data controllers from the point of view of GDPR compliance. Although Genesys might collect aggregate or pseudo-anonymized information for purposes such as statistical and best-practices analysis, Genesys does not utilize customer data for purposes that require consent from consumers. However, be aware that some information you collect for business purposes might incidentally be captured in the Genesys platform (for example, in a transcript record).
Right of Access and Portability	Genesys provides processes to export PII if the data is held for more than 30 days, so that customers can comply with Right of Access requests from consumers.
Right of Erasure (Forget Me)	Genesys provides processes to delete, redact, or pseudo-anonymize PII if the data is held for more than 30 days, so that customers can comply with Right of Erasure requests from consumers.
Breach Notification	Genesys maintains a Product Security Incident Response Team (PSIRT) to collaborate with customers in data breach scenarios.
Privacy by Design	As described on other pages in the <a href="#">Genesys Security Deployment Guide</a> (this document), security measures that protect customer data are part of standard Genesys design requirements.