Genesys Predictive Routing Deployment and Operations Guide

Predictive Routing support for GDPR

2/5/2026

Contents

This page describes product-specific aspects of Predictive Routing support for the European Union's General Data Protection Regulation (GDPR) in hybrid and Genesys Multicloud CX deployments.

Related documentation:
-

Data anonymization

PII, or personally identifiable information, and sensitive data, such as passwords, must be hidden when you upload it to the GPR Core platform. To ensure that sensitive data is secured, instruct Data Loader to anonymize the fields containing such data. For more information, see Data anonymization.

Data at rest

Data at rest is data which is not actively moving within the system or network and does not interact with any third-party applications such as data stored in hard drives, mobile phones, flash drives, laptop, and so on.

The data GPR uses for predictor or model creation is anonymized before it is uploaded. As a result, GPR does not store, access, or use non-anonymized data.

Data in transit

Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network. GPR supports TLS v1.2 for the data in transit.

For more information, see Secure connections.

Data retention policies

GPR follows standard Genesys data retention guidelines for Genesys Multicloud CX as outlined in Section 14 of the Genesys Multicloud CX User Guide.

Most objects and data are deleted automatically after 90 days during which they are inactive. For more information, see Data retention policies.

Updating or removing GDPR-related data

If you need to update, view, or delete any data that might be affected by GDPR controls, contact Genesys Professional Services for assistance.