Tango Legal Documentation Updates

Legal Documentation

- ☑ Innovation Service List - remove Tymeshift Functionality - draft ready to go
- ☑ Sub-processor policy - draft ready to go
  - Remove the following Tymeshift sub-processors (Jeffrey Hatakeda):
    - The Rocket Science Group (Mailchimp)
    - Functional Software (Sentry)
  - Move Tymeshift sub-processors that remain under Zendesk Group sub-processors (Jeffrey Hatakeda):
    - Infrastructure Sub-processor list
    - Service Specific Sub-processor list
- ☑ Complying with Privacy and Data Protection Law in Zendesk products
- ☑ *New* Complying with Privacy and Data Protection Law in Tymeshift
  - Once this page is live, this page should be deprecated
- ☑ Add-ons → all of these can be disclaimed in the Tymeshift Functionality section of the Supplemental Terms
  - Enhanced Disaster Recovery - carve out Tymeshift
  - Advanced Compliance - **not necessary because coverage is enumerated**
  - FedRAMP Tailored Certification - **not necessary because coverage is enumerated**

Complying with Privacy and Data Protection Law in Zendesk products

This guide describes how certain features and functionality in Zendesk products can assist with your obligations under privacy law, for example, as a *data controller* under the General Data Protection Regulation (GDPR), or as a *business* under the California Consumer Privacy Act (CCPA). Zendesk is considered a third-party *data processor* under the GDPR, and a *service provider* under the CCPA, because it handles the personal data or personal information of its customers' end users on behalf of its customers (or subscribers).

Data controllers and businesses bear the primary responsibility for ensuring that their processing of personal data is compliant with relevant data protection law.

See the following articles in this guide:

- Complying with Privacy and Data Protection Law in Zendesk Support
- Complying with Privacy and Data Protection Law in Zendesk Insights
- Complying with Privacy and Data Protection Law in Zendesk Guide
- Complying with Privacy and Data Protection Law in Zendesk Chat
- Complying with Privacy and Data Protection Law in standalone Chat accounts
- Complying with Privacy and Data Protection Law in Zendesk Talk
- Complying with Privacy and Data Protection Law in Zendesk Explore
- Complying with Privacy and Data Protection Law in Zendesk Bime
- Complying with Privacy and Data Protection Law in Zendesk Connect
- Complying with Privacy and Data Protection Law in Tymeshift
- Complying with Privacy and Data Protection Law in Zendesk Sell
- Complying with Privacy and Data Protection Law in Zendesk Sunshine
- Complying with Privacy and Data Protection Law in Zendesk Sunshine Conversations

For instructions on deleting a user's personal data in Zendesk products, see Forgetting a user in Zendesk.

For more information on privacy law and Zendesk, see our Trust Center.

What is personal data

Personal data, or personal information,is any data that can be used to identify an individual. Obvious examples include an email address, a phone number, or a social security number. Personal data may also include any data that could be used indirectly to identify an individual. For example, a person's nickname such as "Gerry" may not be personal data because many people may have the same nickname. However, if the nickname can be combined with other data such as a work address, the nickname could be considered personal data because it helps identify the individual.

Your organization needs to decide what is personal data. Is it simply an email address or phone number, or do you further disambiguate using a combination of identities or attributes? This decision is up to you.

If you’re not sure whether or not a piece of information is personal data, it’s best to err on the side of caution. Another option is to seek legal advice.

Common terms

The following terms are sometimes used in this document.

Soft delete

Soft deleting an item deletes the item such that it is not visible to any users, including admins using either the product interface or the API. The item is still in the Zendesk database and accessible by Zendesk on a limited basis only to its employees with certain database privileges. Soft deleted tickets are automatically permanently deleted after 30 days.

Hard delete, permanently delete, scrub

Hard deleting or *scrubbing* an item permanently deletes the item. The item is completely removed from the Zendesk database. No one, including Zendesk employees with database privileges, can access the item any longer.

Complying with Privacy and Data Protection Law in Tymeshift

This article describes how certain features and functionality in Tymeshift can assist with your obligations under privacy law.

To learn more about meeting your obligations in other Zendesk products, see Complying with Privacy and Data Protection Law in Zendesk products.

Topics covered in this article:

Meeting an access obligation

Individuals from certain regions have a *right of access*. On request, you may have an obligation to inform a user where their personal data is being held and for what purposes.

If an individual requests a copy of their personal data, you can export the data from Tymeshift as described in Meeting a data portability obligation in this article.

Meeting a correction obligation

Individuals from certain regions have a *right to rectification*, or the right to have inaccuracies in their personal data corrected. On request, you may have an obligation to provide the individual with their personal data and fix inaccuracies or add missing information.

To meet the correction obligation, you may contact Zendesk customer support.

Meeting an erasure or deletion obligation

Individuals from certain regions have a *right to erasure*, or the right to be forgotten or deleted. On request, you may have an obligation to delete the personal data of an individual.

To request the deletion of an active user's data, you may contact Zendesk customer support.

Meeting a data portability obligation

Individuals from certain regions have a *right to data portability*. On request, you may have an obligation to provide an individual with their personal data or to transmit the data to another organization.

Agent data within Tymeshift can be exported to CSV files. Export of agent schedule is described here. Agent lists, which contain Agent ID, Name, Email, and Zendesk Role, can be exported as described here. System reports (see here) and custom reports (see here) can be generated and exported to reflect agent attendance and productivity metrics.

Meeting an objection obligation

Individuals from certain regions have a *right of objection*, or the right to object to direct marketing. You may have an obligation to stop processing personal data for direct marketing purposes when you receive an objection from an individual.

Tymeshift does not offer direct marketing as a feature, therefore it is up to the business to be aware of how the end user information is being used.

Disclaimer

This document is for informational purposes only and does not constitute legal advice. Readers should always seek legal advice before taking any action with respect to the matters discussed herein.

Enhanced Disaster Recovery

What's my plan?

Suite **Plan Availability** | Team | Growth | Professional | Enterprise | ✓ Enterprise Plus

This article describes Enhanced Disaster Recovery for Zendesk.

Note: Enhanced Disaster Recovery covers Guide accounts and Help Center Functionality.

This article includes the following sections:

About Enhanced Disaster Recovery

Enhanced Disaster Recovery enhances the protection of your Zendesk data and provides for faster recovery in the event of a disaster that interrupts your Zendesk service. With this feature, your Zendesk data is replicated in real-time and you'll receive priority cloud resiliency.

Key features of Enhanced Disaster Recovery

Key features of Enhanced Disaster Recovery include:

- **Real-time data replication**: Zendesk will replicate your data in real-time within and across Amazon Web Service (AWS) Availability Zones, ensuring extra redundancy and lessening the chance of data loss in the event of a significant disaster. This replication occurs within the same region as your Zendesk service data.
- **Availability Zone Redundancy**: Zendesk infrastructure within each region is spread across two, and sometimes three, physically diverse Availability Zones to provide increased redundancy. In the event of a significant issue impacting an Availability Zone, this structure allows Zendesk to recover within the surviving Availability Zone(s). The secondary Availability Zones, along with AWS elastic scaling capabilities, provide for quicker recovery of service, or in some cases, continuous operation.

- **Traffic Prioritization**: Enhanced disaster recovery combines AWS Availability Zone redundancy with our Cloudflare edge network capability to prioritize Enhanced Disaster Recovery Subscriber traffic while additional capacity is restored for other subscribers.
- **Priority Recovery Planning**: Zendesk maintains a program of test activities and events to validate that our plans for priority recovery of the Services are effective. The scenarios for these exercises vary and test different elements of Zendesk's business continuity and disaster recovery plans to validate the overall strength of the plan.

In the event of a disaster, the following objectives apply:

- **4 hour Recovery Time Objective (RTO)**: Zendesk will aim to restore normal operations for your Zendesk Support account within four hours from the time a disaster is declared, unless a disaster, or multiple disasters, impacts all of the Availability Zones used on an account.
- **Under 1 hour Recovery Point Objective (RPO)**: Zendesk will target one hour or less of data loss for your account. This is calculated from the point of the disruption, not from Zendesk's disaster declaration.
- **Service and traffic prioritization**: Recovery for your Zendesk account will be prioritized over the accounts of other subscribers who have not purchased Enhanced Disaster Recovery commitments. Additionally, your account's traffic will be prioritized over other accounts within the Zendesk Content Delivery Network (CDN).

Exceptions to Enhanced Disaster Recovery

Enhanced Disaster Recovery and the practices described in this article do not apply to the functionality within Zendesk Suite, Support and Chat integrations with third party messaging providers, or to Zendesk Sunshine Conversations, Zendesk Sell, Tymeshift functionality, Zendesk Sunshine, Custom Objects, Custom Events, and Unified Profiles, whether such functionality is available standalone or is available in Zendesk Suite and Support. If you purchase a Zendesk Suite, Zendesk Support Suite, or Sales Suite service plan that includes Enhanced Disaster Recovery, Enhanced Disaster Recovery will only apply to the underlying services that are covered by the feature.