Cronofy

Cronofy Data Management Policy

July 26, 2021

Table of Contents

Cronofy Data Management Policy

The Data management policy outlines how Cronofy handles customer and end-user data collected in the course of its operations.

Data Management Policy

Introduction
This policy describes how personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

This data management policy ensures that Cronofy:

- Complies with data protection law and follows good practice
- Protects the rights of customers, staff and partners
- Is transparent about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data classification
What is personal data?
Personal data is defined as "*information that relates to an identified or identifiable individual*". This could be as simple as a name or a number, or could include other identifiers such as an IP address or a cookie identifier, or other factors. Cronofy has two groups of people from which data is collected and managed.

- **Integrators**: Our direct customers who develop services using our API
- **End-Users**: People who authorize Integrator's applications to access their calendar.

We differentiate between the different types of event data according to the source of that data.

- **Partner Events**: Events created by an Integrator's application in an End-User's calendar
- **Third-Party Events**: Events originating in an end user's calendar that exposed to the Integrator's application is required authorization is obtained.
- **Smart Invites**: Calendar invites created using an application's credentials.

What data we collect and manage
As part of providing a service, Cronofy must collect the data listed below. We will only store that data for as long as is reasonable, in line with providing a service. The exact information that we store, can be found below.

Data from Integrators
The data collected from integrators is that required for the operation of, and billing for, their usage of the Cronofy service. This information includes but is not limited to.

Operational Information	Name Email address Company name, optional Phone number, optional Application name Application url

Billing Information	Billing contact name Billing contact email address Billing contact address Company name Company national tax identifier

Partner Event Data Fields	Summary Description/body Start and end time and time zone where available Recurrence rule Location description, latitude and longitude Attendees: Email address, display name and attendance status Category Colour

Data from End Users
When an end-user authorizes an application to access their calendar through Cronofy, an onboarding process is triggered that builds a cache of the end-users calendar data.

Calendar account information and event data is copied and kept synchronized on in the Cronofy data store to support the Integrator's application query window. By default, this is **42 days** in the past and **201 days** in the future. Reduced or extended synchronization windows are supported and are configured on a per integrator application basis. These can be requested by emailing support@cronofy.com.

Calendar Account Information

Calendar Account Fields	Credentials required to access the calendar account Name associated with the calendar account The email address associated with the calendar account Time zone Names of all calendars linked to the calendar account

Calendar Account credentials data stored depends on the method of authorization supported by the calendar provider.

End-User Direct Authorization

Provider	**Credentials stored**
Google	OAuth token
Office 365	OAuth token
Outlook.com	OAuth token
Apple iCloud	Email address and an app-specific password
Exchange	Email address and password. Optionally username if Exchange server requires it.

Enterprise Connect Authorization
With Enterprise Connect authorization only the credentials associated with the service account are stored by Cronofy. No end-user credentials are accessible or stored.

Provider	Credentials stored
Google	OAuth token
Office 365	OAuth token
Exchange	Service account email address and password. Optionally username if Exchange server requires it

Event Data
We keep event information for good reason – we get asked a lot – what fields do you store? Well – here you go.

Third-Party Event Data Fields	Summary Description/body Start and end time and time zone where available Recurrence rule Location description, latitude and longitude Attendees: Email address, display name and attendance status Category Colour
Smart Invite Data Fields	Summary Description/body Start and end time and time zone where available Recurrence rule Location description, latitude and longitude Attendees: Email address, display name and attendance status Category Colour

Event data fields available do vary by provider so this list represents the data fields that the Cronofy sync process attempts to obtain. Currently, files attached to events are **NOT** synchronized.

Synchronizing this data into the Cronofy Third Party Events database allows us to provide the following features of our service.

Optimized Data Access Model
By maintaining a cache of the data, the Cronofy calendar sync platform can optimize access to the end-user's calendar server. This is especially relevant in self-hosted Exchange scenarios where typical application access patterns can be detrimental to Exchange server performance. Cronofy optimizes access to just synchronize changes and store data in a manner suited to application access patterns.

Rich Permissions Model
Calendar services in general do not have a rich permissions model. Once access has been granted, all data is available to the application. A Cronofy authorization however can limit data access to just free-busy for example. By caching the data we can provide optimal access to data that is appropriately filtered according to the permissions granted at authorization level.

Effective Change Tracking
Changes are synchronized into the Cronofy database using the most effective access pattern for each calendar

service. These changes can then be aggregated and delivered to Integrator’s applications in a manner that is most efficient for them. A centralized cache allows us to separate these concerns and deliver optimal performance for both sides of the sync process.

How is Data protected?
Cronofy uses Amazon RDS for PostgreSQL as the database technology for integrator and end-user data. Data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots.

All transfer of information between the integrator’s application and the Cronofy API requires TLS to encrypt data in transit.

Communication between the Cronofy calendar sync platform and the end-user calendar service is protected by TLS encryption, subject to support by the calendar service.

Backup Procedure
Backups are generated every 24 hours and stored on Amazon S3 in the same region as the RDS instance. The backups are retained for 7 days before they are deleted.

Data Retention

Data Related To Integrators

Application logs	Up to 90 days
Billing records	Permanent
Application configuration	Permanent
Credit card details	Not stored by Cronofy but handled by payment provider Stripe

Data Related To End Users
Event data that falls outside the queryable window is kept for a period of up to 31 days before being removed permanently.

Data related to end-users is retained whilst an authorization is active between an end-user’s calendar and one or more integrator’s applications. When there are no authorizations active against a user’s data is retained against the following scheme.

Data type	Retention period
Third-party events (events that originate in the end user's calendar service)	30 days from termination of last authorization

Partner events (events created by the Integrator’s application in the end user's calendar)	90 days from termination of application authorization
Calendar account credentials	30 days from termination of last authorization.
Calendar account structure	90 days from termination of last authorization.
Smart Invites	30 days after the end date of the event.

Data Removal Requests
Should a user wish to have their data removed from our system they will first create a support ticket by emailing data@cronofy.com. The support engineer assigned to the ticket should then issue a right to be forgotten request in the Cronofy admin system for the user. This process will remove any records from our database and flag the user in a GDPR report so that external systems can be updated.

The process of removal from external systems will be controller by the Data controller, this process will be a manual process and progress will be documented on the GDPR request in our system.

Data Deletion

When data falls outside of Cronofy's data retention periods, or when an end-user request that their data is removed, that data is removed permanently from our infrastructure. Any associated or temporary files are also deleted. This data is subsequently impossible to recover.

Internal Records
Internal records and policies are kept for as long as they're needed. Once that time has passed, they are securely and permanently deleted.