Summary of Uplevel's Privacy by Design Features

Uplevel has designed its services with privacy by design principles to help our customers meet their data protection requirements. This summary describes the deletion, de-identification, and individual rights features of our service. You, the customer, control the data that Uplevel processes on your organization's behalf.
When you submit an individual rights request, Uplevel uses a common identifier (often work email) to locate data related to that individual and fulfill the request.

Uplevel supports data protection requirements (including GDPR) by providing the following data deletion capabilities:

- Uplevel supports "***de-identification of the user"*** in Uplevel's system. When you initiate a de-identification request, the individual's identifiable information will be de-identified with a one-way hash so that the individual can no longer be identified, while still maintaining the underlying analysis from the aggregated and de-identified data. In summary, aggregate analysis will not change and personal information will be deidentified in our system using a one-way hash.
- The customer can also request "***full deletion of the user"*** of a customer's individual's data. Uplevel can support this additional request but this will adjust the underlying analysis of the aggregation. In summary, all elements of the individual's data will be removed in our system and the aggregate analysis will change.

Additionally, Uplevel supports other individual rights requirements:

- If you wish to access data about an individual, Uplevel can locate the data (meta data or otherwise) related to the individual using the common identifier (often work email)
- You can correct data about an individual by sending Uplevel an updated source file (ie. extract of calendar, messaging, or similar system) to replace the incorrect data
- For restriction of processing requests, Uplevel recommends that you initiate the de-identification of the user workflow. Since Uplevel is not a source system for the data, an individual's identifiable data can be removed from Uplevel's system to stop any further processing. If the restriction is lifted, the individual's data can be submitted back to Uplevel.

Uplevel’s deletion process

Overview

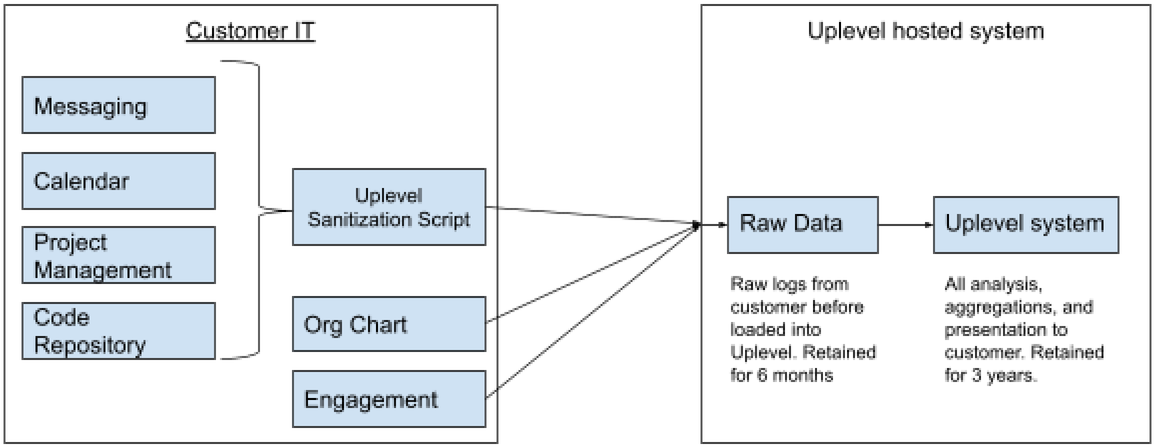
Uplevel receives data from customers source systems. These vary by customer but typical systems include:

- Organization chart of the engineering team (any org tool from Workday to Excel)
- Calendar (Office 365, G-Suite, ...)
- Project Management (Jira, ...)
- Code Repository (Github, Bitbucket, ...)
- Optional Messaging: Meta only data from Messaging (Slack, Teams, Email ...)
- Optional: HR Engagement: HR Survey data (Qualtrics, CultureAMP, Glint, ...)

Data from these sources is sanitized by the customer using Uplevel tools before sending to Uplevel. Specifics on this are found in a separate technical spec provided to your IT group. These tools can be customized but key steps include:

- Calendar: Only pulling calendar for named users in engineering. Dropping all private messages and all body content of all invites.
- Project Management: Excluding projects outside of engineering
- Code Repository: Source code is ignored. Only activity (check-ins, comments, ...)
- Optional messaging data: Drop subject and body text and only keep “meta” content (to/from/time) for all private messages.

In all cases, a common identifier (which is typically a corporate email such as sally@acme.com) is used to identify user data from each system.


Customer IT
Messaging
Calendar
Project Management
Code Repository
Uplevel Sanitization Script
Org Chart
Engagement
Uplevel hosted system
Raw Data
Uplevel system
Raw logs from customer before loaded into Uplevel. Retained for 6 months
All analysis, aggregations, and presentation to customer. Retained for 3 years.

Deletion of user data

Uplevel supports deletion of your users data for when instructed by you to do so. This could be a request under a data protection regulation, such as GDPR, or just personal preference of the employee. Uplevel supports two methods to remove a users' information:

Method 1: De-identification of the user

1. Customer sends a message to Uplevel with the identifier of the user they wish to de-identify. For example: "Please de-identify sally@acme.com"
2. Uplevel takes the following actions
    a. All individual records initiated or created by sally@acme.com are de-identified. For example:
        i. All Calendar events sent by Sally are de-identified. Note: Uplevel's sanitization tools do not extract calendar body text so this will not be shared with Uplevel's systems.
        ii. All Jira or Github comments made by Sally are de-identified.
        iii. All Slack messages (if Slack is included) sent by Sally are de-identified so they are shown to be sent by an anonymous identifier. NOTE: Uplevel's sanitization tools remove all contents of communications in private channels or DMs so there is no messaging text from Sally in the Uplevel system, unless it was sent in a public channel.
        iv. All of Sally's engagement data results are de-identified
        v. Sally is de-identified from the org chart data.
    b. All records where Sally is a recipient are maintained but Sally is de-identified. For example, if a calendar invite is sent from another employee to many employees including Sally, Sally's email address will be de-identified so that the record of the meeting is maintained but Sally cannot be identified within Uplevel as a recipient.
    c. All "aggregate counts" that include Sally will be maintained but the records that identify Sally will be de-identified. So if Jim's team had 10 hours of uninterrupted work time in a week and this includes 2 hours from Sally, all numbers will be maintained but the 2 hours of 'contribution' from Sally will be de-identified or presented as an autonomous person.
    d. Upon receipt of your written request, Uplevel will provide you with a written confirmation of the de-identification of all of sally@acme.com's user data.

Method 2: Full deletion of the user

a. Customer sends a message to uplevel with the identifier of the user they wish to delete. For example: "Please fully delete sally@acme.com"
b. Uplevel takes the following actions

i. All individual records initiated or created by sally@acme.com are fully deleted. For example:
    1. All Slack messages sent by Sally are deleted.
    2. All Calendar events sent by Sally are de-identified.
    3. All Jira or Github comments made by Sally are deleted.
    4. All of Sally's engagement data results are deleted.
    5. Sally is deleted from the org chart data.

ii. All records where Sally is a recipient are maintained but Sally is deleted. For example, if a calendar invite is sent from another employee to many employees including Sally, Sally will be deleted so that the record of the meeting is maintained but Sally will not be shown as an invitee.

iii. All "aggregate counts" that include Sally will be changed. So if Jim's team had 10 hours of uninterrupted work time in a week and this includes 2 hours from Sally, all numbers will be changed so that now Jim's team had 8 hours of uninterrupted work time in a week (the rows for Sally were deleted).

iv. Upon receipt of your written request, Uplevel will provide the customer a written confirmation of the deletion of all of sally@acme.com's user data.

Any questions or concerns on any of this document or Uplevel's policies and practices should be directed to Uplevel.

Joe Levy, CEO
Uplevel, Inc.
300 LENORA ST #952
SEATTLE, WA 98121-2411