

Data Subject Request Handling Policy

How Workplacer receives, verifies, and fulfils data subject requests under the GDPR.

1. PURPOSE & SCOPE

This policy describes how Workplacer handles requests from individuals to exercise their rights under the GDPR — including access, portability, rectification, erasure, and restriction. It applies to personal data Workplacer processes both as a controller (for its own account/login data) and as a processor (on behalf of customer organisations).

2. ROLES & RESPONSIBILITY

Accountability for data subject requests sits with the founder, who acts as the point of contact and coordinates fulfilment. Requests may reach Workplacer directly from an individual, or via a customer organisation acting as controller. Where Workplacer acts as a processor, it assists the customer in responding rather than responding to the data subject independently.

3. SUPPORTED RIGHTS & HOW THEY ARE FULFILLED

Right	How it is fulfilled
Access / portability (Art. 15, 20)	Individuals can export their personal data as a structured, machine-readable file through built-in self-service functionality.
Erasure (Art. 17)	Individuals can request erasure of their account through self-service; administrators can also erase a user's data. Erasure removes the account, sessions, and access records.
Rectification (Art. 16)	Personal and account data can be corrected directly in the application, or on request.
Restriction / objection (Art. 18, 21)	Handled on request; access can be suspended and processing limited pending resolution.

4. VERIFICATION

Before actioning a request, the identity of the requester is verified. Self-service requests are authenticated through the individual's own logged-in account; requests received by other means require confirmation of identity and, where the data belongs to a customer's environment, coordination with that customer as controller.

5. TIMELINES

Self-service requests (export, erasure) are actioned immediately by the individual. For requests requiring manual handling, Workplacer responds without undue delay. Where Workplacer acts as a processor, it assists

the customer in meeting the GDPR one-month response deadline. Under our Data Processing Agreement, customers may extract their data during the agreement and for 30 days after termination, after which data is deleted or anonymised.

6. ERASURE & RETAINED RECORDS

Erasure hard-deletes the individual's account, sessions, and access records, and removes associated uploaded files from storage. Where records must be preserved for audit or legal integrity, personal identifiers are anonymised (user identifier and IP address removed) rather than retained. Deleted data ages out of the rolling backup window and is not restored to live service outside a documented recovery event.

7. RECORDS & REVIEW

Data-changing operations, including erasures, are recorded in an immutable audit log. This policy is reviewed at least annually and when significant changes to the platform or applicable law occur.

This policy should be read alongside our Data Processing Agreement, Privacy Policy, and Data Retention Schedule.
Point of contact for data subject requests: jesper@workplacer.ai.