Data Subject Rights Procedure

1. Purpose

This procedure explains how requests from individuals to exercise their rights under the UK GDPR are handled: access, rectification, erasure, restriction, portability and objection. It also covers the right not to be subject to solely automated decisions with significant effects, and the right to withdraw consent. It sets out who answers each request, the steps followed, the timescales, and the tools customers use to answer requests about data on the platform.

2. Scope

This procedure applies to every request made by an individual about their personal data held by or for Subcontext, however it arrives: by email, through support, through an AI agent conversation, by post or verbally. A request does not need to use legal wording or name the right being exercised to be valid. Anyone at Subcontext who receives something that may be a request passes it on the same working day to the person handling requests (section 9).

3. The Rights

Right	What the individual can ask for
Access	Confirmation that their data is being processed, a copy of it, and information about how it is used
Rectification	Correction of inaccurate data, or completion of incomplete data
Erasure	Deletion of their data where there is no good reason to keep it
Restriction	A pause on the use of their data, for example while its accuracy is checked
Portability	Data they provided, in a structured, machine-readable format
Objection	That their data is no longer used for a purpose, including direct marketing, which must always stop on request
Automated decision-making	Human involvement in a decision made solely by automated means that has legal or similarly significant effects
Withdrawal of consent	That processing based on their consent stops

4. Who Handles a Request

- **Our customers' end users:** for personal data processed through the platform (contacts, conversations, applications), our customer is the controller and Subcontext is its processor. Requests are answered by the customer, and we help them do so.

- **Our own users and contacts:** for platform users' accounts and our own marketing and sales contacts, Subcontext is the controller and answers the request directly.

Who is asking	About what data	Who answers
A customer's customer or enquirer	Their conversations, lead record, application, policy or claim	The customer, using the tools in section 7
A user of the Subcontext dashboard or apps	Their user account	Subcontext
A sales or marketing contact of Subcontext	Their contact record	Subcontext
A customer's staff member	Their user account on the platform	Subcontext, informing the customer where relevant

5. Timescales

- Requests are answered within one month of receipt
- The period may be extended by two further months for complex or numerous requests, in which case the individual is told within the first month, with the reasons
- Identity is verified before personal data is disclosed or erased

Where we need to verify identity or clarify a request, the one-month period starts once we have what we need, and we ask for it promptly. Requests are free of charge. A reasonable fee may be charged, or a request refused, only where it is manifestly unfounded or excessive, and the individual is told why and of their right to complain.

6. Requests to Subcontext as Processor

If an end user contacts Subcontext directly about data we process for a customer, we forward the request to that customer without undue delay and do not respond to the substance ourselves, unless the customer instructs us to.

The steps are:

1. Identify the customer whose data the request concerns, from the details the individual gives
2. Forward the request to the customer's account owner, with any information that helps them find the records
3. Tell the individual that their request has been passed to the organisation responsible for their data, naming it where it is safe to do so
4. Record the request, the customer it was passed to and the date
5. Where the customer asks, help them answer it, for example by retrieving data their own tools cannot reach

If we cannot identify the customer, we ask the individual for more information.

7. Tools Customers Use

The platform gives customers what they need to answer requests themselves:

Right	How it is met
Access and portability	Export a lead's full record as JSON, and conversation transcripts
Rectification	Edit contact and lead details directly in the CRM
Erasure	Erase a lead: CRM records are deleted, raw data is scrubbed and the contact is reduced to a minimal record so they are not contacted again
Restriction and objection	Opt a contact out of each messaging channel, or block them
Tracking	Log a data rights request against a lead, which opens a task due in one month and is recorded in the audit log

Erasure is refused, and the reason explained, where records must be kept: for example where the person holds a live insurance policy, has an application in progress or has made a claim. Conversation transcripts, the insurance file and the compliance trail are kept where the law or the customer's own retention rules require it, and the customer is told what remains.

Further points for customers:

- Erasing a lead is available to owners and managers in the customer organisation, and a reason must be given. The erasure is recorded in the audit log
- Agents can request human review, and escalation to a person is always available, which helps customers meet requests for human involvement in a decision
- Where health data has been collected for an insurance application, the consent recorded before it was captured is part of the record
- If a customer needs help with a request its tools do not cover, it can raise a support ticket in the app or email support@subcontext.com

7.1 Worked example

An applicant emails an insurer asking for all the data held about them and for it to be deleted. The insurer logs a data rights request against the lead, which opens a task due in one month. It exports the lead's full record and the conversation transcripts and sends them to the applicant. The applicant has an application in progress, so the platform refuses erasure and explains why. The insurer tells the applicant what has been kept and why, and records the outcome against the task.

8. Requests to Subcontext as Controller

- Platform users can update their profile, and delete their account from their settings: their personal details are removed, and their sessions, tokens and devices are revoked
- Other requests go to hello@subcontext.com
- Every request is logged, with its outcome and the date it was answered

The steps are:

1. **Log** the request on the day it is received, with the date, the requester and the rights exercised
2. **Verify identity** in a proportionate way, normally by replying to the email address on the account, or asking for confirmation through the signed-in account. We do not ask for more information than we need
3. **Find the data** across the platform, billing records, support tickets and email
4. **Apply exemptions** only where they genuinely apply, such as legal privilege or records we must keep by law, and record the reason
5. **Respond** in clear language, in a commonly used electronic format where the request was made electronically, explaining what was done and anything withheld or kept, and the reason
6. **Close** the request in the log, with the outcome and the date it was answered

Data about other people is removed or redacted from anything disclosed unless they have consented or it is reasonable to disclose it without consent.

9. Roles and Responsibilities

Role	Responsibility
Security Officer	Owns this procedure, handles requests to Subcontext as controller, maintains the request log and checks deadlines
Support	Recognises requests that arrive through support and passes them on the same working day
Directors	Decide on refusals, fees and extensions, and approve responses to complex or contentious requests
Customers	Answer requests about data they control on the platform, using the tools in section 7

10. Compliance

- The request log is reviewed at least quarterly to confirm deadlines are being met
- Anyone handling requests is briefed on this procedure when they join and when it changes
- Customer feedback and any complaint about the handling of a request are used to improve this procedure

11. Complaints

Anyone unhappy with how their request was handled can complain to us under the Complaints Handling Policy, or to the Information Commissioner's Office at ico.org.uk. Subcontext is registered with the ICO under registration number ZC098511.

12. Related Documents

- Data Retention & Deletion Policy
- Data Classification Policy
- Data Protection Impact Assessment
- Complaints Handling Policy
- Exit Plan & Data Return Policy

- Sub-Processor List

13. Document Control

Item	Detail
Owner	Security Officer
Approved by	The directors of Subcontext Ltd
Review	At least annually, and when the law, ICO guidance or the platform's tools change
Effective	October 2026

Subcontext Ltd, registered in England and Wales, Company No. 17019645. Registered office: 124 City Road, London, EC1V 2NX. The current version of this document is published at subcontext.com.