

DATA PROTECTION COMPLAINTS PROCEDURE

DOCUMENT HISTORY

Document Owner:	Data Protection Officer
Document Number:	SCP-P-384
Revision Number:	1.0
Issue Date:	02 nd February 2026

This is a controlled document, please ensure that this document is the most recent version by checking on SharePoint. If you require a change to this procedure, please contact the quality assurance manager, who will review the suggested change(s), seek the relevant approval(s), update and re-issue.

Table of Contents

1.	Introduction	3
1.1.	Purpose.....	3
1.2.	Scope	3
1.3.	Data Subjects	3
1.4.	Rights of a Data Subject.....	3
1.5.	What is a Complaint	4
2.	Responsibilities.....	4
3.	How to Complain.....	4
4.	Investigation and Outcome	5
5.	Review	5
6.	Independent External Review	6
7.	Unfounded, Abusive or Excessive Complaints	6
8.	Use of Data from Complaints	6
9.	Revision & Approval	7
10.	Annex A – Data Protection Complaints Procedure Flowchart.....	8

1. INTRODUCTION

1.1. Purpose

The UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Privacy and Electronic Communications Regulations (PECR) (together, the Data Protection Legislation) provide individuals and, where applicable, third parties with rights relating to the processing of personal data. This procedure sets out how SecureCloud+ (SC+) will receive, manage, and respond to complaints from individuals and third parties about the organisations use of personal data.

1.2. Scope

This procedure sets out how the organisation will manage complaints from data subjects about any aspect of the organisation's processing of personal data, including individual rights requests. It also applies to complaints from third parties about the organisation's use of personal data, for example concerns arising from the handling of data-related requests from external bodies such as the Police or Local Government agencies. In addition, this procedure must be followed regarding complaints relating to the use of personal data for direct marketing and/or profiling activities.

1.3. Data Subjects

Data subjects are any natural living individuals whose personal data SC+ processes in any way, including collecting, obtaining, storing, retaining, using, sharing, or disposing of it. Data subjects may include staff, customers, job applicants, visitors, and natural living individuals captured by the organisation's CCTV systems.

1.4. Rights of a Data Subject

Under Data Protection Legislation, data subjects have the following rights, which may be exercised at any time:

- a. The right to be informed about the collection and the use of their personal data (UK GDPR Articles 12-14).
- b. The right to access personal data and supplementary information (UK GDPR Articles 12 and 15).
- c. The right to have inaccurate personal data rectified or completed if it is incomplete (UK GDPR).
- d. The right to erasure (to be forgotten) in certain circumstances (UK GDPR Article 17).
- e. The right to restrict processing in certain circumstances (UK GDPR Article 18).
- f. The right to object to processing in certain circumstances (UK GDPR Article 21).
- g. The right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services (UK GDPR Article 20).

-
- h. Rights in relation to automated decision making and profiling (UK GDPR Article 22).
 - i. The right to withdraw consent at any time (where relevant) (UK GDPR Article 7).
 - j. The right to complain to the Information Commissioner (Section 50 of the Freedom Information Act 2000).

1.5. What is a Complaint

A complaint is any expression of dissatisfaction about the organisations handling of a data subject's personal data, or the personal data of an individual they represent. This includes dissatisfaction with how the organisation has responded to a previous data request, including those set out in section 1.4.

2. RESPONSIBILITIES

The Chief Executive Officer (CEO) has overall responsibility for this procedure but has delegated day-to-day responsibility for overseeing its implementation to the Data Protection Team. All relevant members of staff have been made aware of the procedure and have received appropriate training.

All Employees/Staff are responsible for ensuring that any complaints that are made in relation to this procedure are reported to the Data Protection Officer/Data Protection Team at dataprotectionteam@securecloudplus.co.uk and for cooperating with the Data Protection Officer in reviewing these complaints.

The Data Protection Officer will review this procedure occasionally (and at least annually) to ensure that its provisions continue to meet our legal obligations and reflect best practice.

3. HOW TO COMPLAIN

Data subjects and third parties may make a complaint relating to SC+ use of personal data. Complaints should be sent directly to the Data Protection Officer/Team at dataprotectionteam@securecloudplus.co.uk. A member of the Data Protection Team will normally acknowledge the complaint within 5 working days. SC+ reserves the right to extend the period we need for response during leave and holiday closures.

A member of the Data Protection Team will issue a Data Protection Complaint Questionnaire (Microsoft Forms) to the complainant, who will be asked to complete and return it.

Although a complaint may be made at any time, there may be limits as to what the organisation can do in historic cases.

SC+ will only accept a complaint from a data subject's representative, if the representative provides the data subject's written consent authorising the representative to act on the data subject's behalf in relation to the complaint.

If there is any doubt about the identity of the complainant, the Data Protection Team will first seek to verify the data subject's identity or third party's entitlement to act on behalf of the individual. The forms of identification that are acceptable from a data subject are as follows:

- a. UK (Channel Islands, Isle of man or Irish) Passport or EU/other nationalities passport.
- b. Passport of non-EU nationals and other valid evidence relating to their immigration status and permission to work.
- c. UK full or provisional photo-card driving licence.
- d. EU/other nationalities photo-card driving licence (valid up to 12 months up to the date of when the individual entered the UK).
- e. Biometric Residence Permit (formerly known as identity cards for foreign nationals) (UK).
- f. HM Armed Forces identity card.
- g. ID cards carrying the PASS accreditation logo (UK and Channel Islands), for example a UK Citizen ID card.

4. INVESTIGATION AND OUTCOME

Once all identification requirements have been met, the investigation will be carried out normally within 20 business days. If further clarification is required from the complainant or more time is required for the response to be completed SC+ will inform the complainant prior to the original deadline.

The complaint outcome will be communicated to the complainant in writing, normally by email.

5. REVIEW

If the complainant does not agree with the outcome, they can request a review of the decision. This request must be made within 1 month of the original decision being communicated and should be sent to the Data Protection Team <mailto:dataprotectionteam@securecloudplus.co.uk>. The decision will be internally reviewed by the Data Protection Officer and/or the Chief Information Security Officer normally within 20 business days from the receipt of the request for Review.

Once the internal review has been completed, SC+ will communicate the outcome in writing, normally by email.

6. INDEPENDENT EXTERNAL REVIEW

If the complainant remains dissatisfied, they can escalate their complaint to the Information Commissioner's Office (ICO) at the following link: <https://ico.org.uk/make-a-complaint/>

To respond to the complaint, the Data Protection Officer will investigate the complaint based on the information provided by the ICO. This may necessitate access to personal data and other information held across SC+. The cooperation of any staff members able to assist with the investigation will be required. The reason for the investigation may need to be disclosed to the relevant staff members. The Data Protection Officer will draft and submit a response to the ICO in consultation with the SC+ Solicitor and the CEO.

7. UNFOUNDED, ABUSIVE OR EXCESSIVE COMPLAINTS

In some circumstances, we may decline to handle a complaint where it is considered manifestly unfounded, abusive, vexatious, or excessive. Each complaint will be assessed on a case-by-case basis. The following factors will be considered:

- a. The data subject has explicitly stated that they intend to cause disruption (whether in the complaint, or in other correspondence) and has threatened individuals.
- b. The data subject has made unsubstantiated accusations against individuals and is persisting in those accusations.
- c. The data subject is targeting individuals, against whom they have a personal grudge.
- d. The data subject makes frequent complaints intended to cause disruption.
- e. The data subject continues to repeat the substance of previous complaints which have already been investigated.

Where a complaint is deemed manifestly unfounded, excessive, abusive, or vexatious, SC+ will contact the individual within a reasonable timeframe to explain:

- a. The reasons for refusing to consider the complaint.
- b. Their right to make a complaint to the ICO.
- c. Their right to pursue their data subject rights through a judicial remedy.

8. USE OF DATA FROM COMPLAINTS

SC+ will collect data on complaint outcomes at each stage of this procedure and any complaints submitted by complainants to the ICO, and use the data:

- a. Internally for reporting, evaluation, learning and training.

-
- b. Externally for discussion with regulators.

Your personal data and special category personal data, as defined by DPA 2018 , may be disclosed to relevant SC+ staff and regulators only where necessary to handle your complaint (including any complaint arising from it) and/or to implement any recommendations.

Personal Data will not be shared with any other third parties unless SC+ has your express consent, is under a statutory obligation to do so, or is otherwise permitted under the DPA.

9. REVISION & APPROVAL

This policy shall be revised accordingly to SCP-P-001 (document control). The approvers for this policy shall be the Quality Assurance Manager and Document Owner.

REVISION RECORD

DATE	REV.	COMMENT	APPROVAL
02-Feb-26	1.0	First issue	QM. P. Jackson
			DO. S. Corcoran

10. ANNEX A – DATA PROTECTION COMPLAINTS PROCEDURE FLOWCHART

