

GDPR Data Subject Access Policy and Procedure

1. Introduction

STCU processes (including collecting, storing and transmission) different types of personal data about individuals who have been in contact with the Center to fulfil its role and to meet its legal obligations. STCU has a responsibility to protect this information and ensure its confidentiality, integrity and availability. This document sets out STCU's policy and procedures relating to responding to subject access requests, that is, requests from individuals to access their own personal data. This policy and procedure have been prepared in accordance with the requirements of SOP XXXIV Data Protection.

2. Scope and Purpose

2.1 Scope of this policy and procedure

STCU defines a 'personal subject access request' as a request in any form received by a member of staff where the data subject expresses a request to access some or all of their personal data.

STCU's Subject Access Request policy and procedure applies to permanent employees, and third parties who act as a data processor on behalf of the Center. For the purposes of this document, "STCU staff" refers to both permanent employees and third-party data processors.

2.2 Purpose of this policy and procedure

The STCU's Data Protection Policy requires that a procedure will be developed and maintained for dealing with subject access requests. This document contains the procedures to establish the methodology for handling a request from an individual who wishes to exercise their right to access their personal data.

3. Rights of the Data Subject

3.1 Right to Access

Under Article 15 of the Regulation (EU) 2016/679 (known as the General Data Protection Regulation (GDPR)), an individual has a right to access personal data which has been collected concerning them by the Center. Article 15 allows an individual to access that personal data and be provided with the following information;

- (a) The purposes of the processing;
- (b) The categories of personal data concerned;
- (c) The recipients or categories of recipients concerned, in particular recipients in third countries (where applicable), and the safeguards in place relating to the transfer of personal data;
- (d) Retention periods;
- (e) Information on the rights of the individual to have their personal data rectified, restricted, erased or objected to;
- (f) The right to lodge a complaint with a Supervisory Authority;
- (g) If personal data have not been collected directly, the source of the personal data;
- (h) The existence of automated decision making and/or profiling relating to the personal data;

Where a controller processes a large amount of data in relation to the data subject, prior to providing the information, the Center may request the data subject to specify the information to which the request relates (Recital 63, GDPR).

3.2 Right to Portability

GDPR Data Subject Access Policy and Procedure

Where the right to access requires personal data to be provided in a commonly used form, the right to portability goes further under Article 20 and requires the Center to provide the information to the data subject “in a structured, commonly used and machine-readable format” so it can be transferred to another controller “without hindrance.”

The right to portability applies to the following:

- Personal data processed by automated means;
- Personal data provided to the controller;
- Only where the legal basis is for consent or data is being processed to fulfil a contract;

This right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and, in particular, copyright protecting the software. However, the result of those considerations should not be a refusal to provide information to the data subject.

As outlined in the STCU’s Data Protection Policy, it is expected that this right will apply only to a small number of data subjects based on the lawful basis for the processing carried out by the Center.

4. Subject Access Request Requirements

4.1 Format of Response

The Center must provide a copy of the personal data to the data subject. In line with Article 15 of the GDPR, where the data subject submits an access request by electronic means, the information should be provided to the data subject by electronic means, unless otherwise requested by the data subject.

4.2 Costs

A SAR should be provided to the data subject free of charge. However, for additional copies provided to the data subject, the Center may charge a reasonable fee or where access requests are “manifestly unfounded or excessive” taking into account the administrative costs of providing the information as outlined under Article 15 and Article 12 of the GDPR.

4.3 Subject Access Request Form

The Center provides a Subject Access Request Form to individuals who inquire about their personal data. The form gives information to data subjects about how to make a valid subject access request. The form is included in Appendix A of this document.

4.4 Exemptions

A subject access request may be refused where it is deemed “manifestly unfounded or excessive, in particular because of its repetitive character.” The burden of demonstrating the manifestly unfounded or excessive character will rest with the Center as outlined under Article 12 of the GDPR.

There are other instances where the Center may decide to refuse the request. Examples of reasons to refuse a request include where the requester is involved in a claim against the Center, seeking compensation, and the information requested reveals details of the organisation’s decision process in relation to their claim; or if releasing the personal data requested would mean that the personal data of another individual would be unfairly disclosed.

4.5 Refusing a Request

Under Article 12 of the GDPR, where the Center refuses to respond to a subject access request, the Center shall inform the data subject without delay and at the latest within one month of receipt of the request of the following:

- Reasons for refusing to respond;

GDPR Data Subject Access Policy and Procedure

- The right to lodge a complaint with the Data Protection Authority;
- The right to seek a judicial remedy.

4.6 Deleting data

It is an offence under the GDPR to delete data that is the subject of an access request. Under no circumstances should the data be deleted even if it has been retained for a period longer than the Center retention schedule permits.

4.7 Data Processors

Where the Center uses a data processor, then it must notify the processor of the subject access request and ensure that contractual arrangements are in place to guarantee that such requests are dealt with efficiently by all data processors.

5. Review & Update

This policy and procedure will be reviewed and updated annually or more frequently, if necessary to ensure any changes to the STCU's organisation structure and operations are properly reflected in the policy.

6. Approval

This document was approved and came into effect September 2020

Subject Access Request Form

Requests for Access to Personal Data under Article 15 of the General Data Protection Regulation (GDPR) 2018.

Under the GDPR, you may receive a copy of your personal data held by STCU electronically or in manual filing systems simply by submitting a subject access request. Access requests can be submitted by written or electronic means. You may use the STCU’s subject access request application form, write a letter, or submit your request using other electronic means, such as an email. You may also submit a request verbally, although a written request is preferable if possible, so that there can be no doubt as to the details of the request.

All written applications along with proof of identity should be addressed to: the Data Protection Officer at STCU in writing or by email to: gdpr@stcu.int

To help us answer your request please be as specific as possible about the information you wish to see and give as much information as you can to help us find it.

You are legally entitled to a decision regarding your request within 30 days of STCU receiving your request. However, every effort will be made by the Data Protection Officer to deal with your request as soon as possible, and you will receive an acknowledgement on receipt of your application, which will outline the deadline for your particular request.

If you are unhappy with the decision of the Data Protection Officer, you have the right to complain to the relevant Data Protection Authority who will investigate the matter for you.

Important: A photocopy of your proof of identity (E.g. passport or driver’s licence) and a photocopy of proof of address must accompany this Access Request Form (see Note below).

Section A - please complete this section		
Full Name		
Postal address		
E-mail*		
Telephone*		
* we may need to contact you to discuss your Access Request		
Section B - please complete this section		
I,[insert name] wish to have access to data that I believe the STCU retains on me as outlined below		
Please include any relevant information to assist us		
Signed		
Date		
Checklist	Yes	No
Completed the Access Request Form in full?		
Attached a photocopy of proof of your identity and address?		
Signed and dated the Access Request Form?		

If you have ticked No to any question above the STCU cannot process your request. Please return this form to: Data Protection Officer, STCU Email: gdpr@stcu.int

Note: we require proof of the applicant’s identity and address to ensure that the person making this access request is acting legitimately.