ANNEX Security Policy for users accessing SFC and Privacy Statement

1.1. Terms of Service

SFC is a software application accessible via the Internet, developed and hosted by the European Commission. The objective of SFC is to facilitate electronic exchange of information between the Member States of the Union and the European Commission in the context of shared management. ("The Service").

By using the SFC system user agree to be bound by the following terms and conditions ("Terms of Service").

The European Commission reserves the right to update and change the Terms of Service. In that event you will be asked for your acceptance of the new terms. Any new features that augment or enhance the current Service, including the release of new tools and resources, shall be subject to the Terms of Service. Continued use of the Service after any such changes shall constitute your consent to such changes. You can review the most current version of the Terms of Service at any time at SFC website.

1.2. Security Policy for access from National Authorities

Authentication

Users must accurately provide full legal name in ECAS to open an account in SFC.

Each login will correlate to only one user. Accounts created are available only with a username and password.

Authorisation

Users will create its own ECAS account (or via National Liaisons Officers) and later they will be will be given specific access rights to SFC according to their role. National Liaisons and DG Liaisons Officers must assign roles to users according to their expected role in SFC. SFC Security model ensures that users have access only to the specific data they need according to their role in the application.

National Liaison Officers and DG Liaison Officers together with user support agents in SFC are the only ones that can manage user accounts and roles.

National Liaison Officers and DG Liaison Officers are the only ones authorised to request the creation or deletion of user accounts.

Users are responsible for all actions done under the username and passwords attributed to them, (even when those actions have been carried out by others who are using your username and password).

Integrity

The Commission ensures that SFC complies with the requirements applicable to all IT systems at EU level set out in Commission Decision 2017/46 on Security of Information Systems and its implementing rules. This means that appropriate technical security measures are integrated in the SFC system. In particular, authentication (a username/password combination) and access control mechanisms ensure confidentiality and integrity of the SFC system and the information it contains.

Information during transmission is protected by using Secure Sockets Layer (SSL) software, which encrypts information you input when signing on, uploading and downloading content to and from SFC.

In addition, each SFC user must implement organizational security measures applicable to the processing of personal data in accordance with national legislation. In particular, appropriate security measures must be applied to personal data extracted from and further processed outside SFC (e.g. in a printed report or otherwise archived outside SFC or stored in national systems)

Also users must implement appropriate measures to protect they access credentials:

- Login and password credentials must not be shared with others. Users are responsible for keeping your account login and password private.
- Users must not misrepresent other people or take on the identity/role of someone else while using the Service.
- Users may not use the Service for any illegal or unauthorized purpose. The role provided in SFC should be appropriate to the role user have in the national authority
- In the event that users change their in their national authorities and this affects the role in SFC they must inform immediately National Liaison officers to make the corresponding update.
- In the event that users notice a security incident or come to the knowledge that an SFC account is used inappropriately or shared among different people users agree to notify their corresponding National Liaison officer or DG Liaison Officer.

1.3. Privacy Statement

Introduction

This privacy statement covers the part of SFC for which the Commission is responsible, i.e. the collection, registration, storage and deletion of personal data of SFC users (i.e. natural persons working on behalf of Member States in national authorities, European Commission desktop officers, National Liaisons officers, European Commission staff working in the operation and support of SFC, DG Liaisons officers). Thus, it does not concern those data processing acts which fall under the responsibility of Member States. This privacy statement explains the way in which this system uses personal data, and the way in which the privacy of this data is being protected.

Why and how do we process your personal data? Purpose of the data collection?

The processing of personal data is necessary in order to cooperate effectively with the Member States on shared management. Examples of such interactions are the notifications of failure of the system, reminders of actions that should be taken or notification of specific events to which users are subscribed.

These contact details may be processed for purposes compatible with the provision of the service, including monitoring of the use of the system by DG and National Liaisons Officers and the Commission, communication, training and awareness-raising initiatives, and gathering information required for the exchange of information.

On what legal ground(s) do we process your personal data?

The processing operation is compliant with the principle of lawfulness and fairness. Processing is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the Union institution or body. SFC is the official System used in the European Commission for Shared Management Funds in accordance with article 74(4) of the Regulation (EU) 1303/2013 and Implementing Regulation (EU) 184/2014, article 69 (8) of the Regulation (EU) 2021/1060 and Annex XIV. As such, its publishing and processing falls within the provisions of the Regulation EU 2018/1725 on the protection of natural persons with regard to the processing of personal data.

Which personal data do we collect and further process?

The Commission collects the necessary contact details. These personal data are stored on databases at Commission's Data Center.

The following data is required:

- First name
- Last name
- E-mail address
- Preferred language
- Telephone, fax and additional information only when specified by the data subject (optional)
- Business details (name, address, country, type and code) in regards to users
- Authority details (name, address, country and code) in regards to Member State and Accession Country Administrators

How long do we keep your personal data? (Data retention)

Personal data of SFC users (staff working for the national authorities) will be stored as long as they continue to be users of SFC. In principle, 3 years after the final closure of all the programmes.

How do we protect and safeguard your personal data?

All personal data in electronic format (eg.: e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the European Commission. All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

Security measure taken
The data is safeguarded in the Commission and covered by the numerous defensive measures implemented by the Commission to protect the integrity and confidentiality of the electronic assets of the Institution. SFC is hosted in DG DIGIT Datacenter. DG DIGIT is responsible for all the security associated to hardware assets.

Technical means
The data collection and processing is done using the Commission's IT standards and telecommunication infrastructure. SFC access control is managed by the User Security Module (USM) that is accessed directly by the SFC user administrators in the respective nodes (Member States or the Commission one). MS and EC Liaisons submit access requests for the users they represent. Such requests do contain also users' information. In any event, this data is only accessible for users which have been officially nominated as Liaison and later received the specific role in the SFC System.

Who has access to your personal data and to whom is it disclosed?

SFC access control is managed by the User Security Module (USM). Therefore, the SFC user administrators in the respective Member States or the Commission's support (in involved DGs) and maintenance team (in DIGIT) have access.

SFC does not transmit any data to parties that are outside the above-listed recipients and the legal framework mentioned, without prejudice to a possible transmission to the bodies in charge of an inspection tasks in accordance with Community legislation, e.g. OLAF, or an investigating purposes.

Information exchanged is not meant to include personal data with exception of an annual account. Such annual account may contain the name of beneficiaries and information on claims and payments.

This information is only accessible to particular auditors in charge of the file (AGRI) and is transferred to an internal support and management system, processing covered by record DPR-EC-00354, (CATS/COMBO – Clearance of Accounts Audit Trail System & Audit Management; https://ec.europa.eu/dpo-register/detail/DPR-EC-00354).

General public won't see the relevant personal contact details.

What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access your personal data and to rectify them in case your personal data are inaccurate or incomplete by contacting the Data Controller that is HoU IT (REGIO.A.4). Under certain conditions, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing and the right to data portability.

Contact information

If you want to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you want to submit a complaint regarding the collection and use of your personal data, please feel free to contact Data Controller that is HoU IT (REGIO.A.4): REGIO-A4-SECRETARIAT@ec.europa.eu

If you have further queries or complaints, you can also contact:

- The Data Protection Coordinator of DG REGIO: regio-data-protection-coordinator@ec.europa.eu
- The European Commission Data Protection Officer: data-protection-officer@ec.europa.eu

Where to find more detailed information?

The Commission Data Protection Officer publishes the register of all operations processing personal data. You can access the register on the following link: http://ec.europa.eu/dpo-register.

This specific processing operation has been included in the DPO's public register with the following Record reference: DPR-EC-00741.2

1.4. Web Services considerations:

Data Sending and Validation

According to Article 3(2) of Commission Implementing Regulation (EU) No 184/2014, *"any transmission of information to the Commission shall be verified and submitted by a person other than the person who entered the data for that transmission. This separation of tasks shall be supported by SFC2014 or by Member State's management and control information systems connected automatically with SFC2014."*

SFC2014 and SFC2021 enforces the "four-eyes" principle, which means that the user who last validated an Operational Programme cannot submit it. Two different users are required; one to validate and another to send. In the case of the SFC2014 and SFC2021 graphical user interface, this control is made by the SFC system itself. Given the impossibility to implement the four eyes principle in a machine to machine interface, when **accessing SFC2014 and SFC2021 via Web Services, each member state should take care of the implementation of the "four-eyes" principle internally in its own information system.**

Sample Application

The SDK/Sample Application provided by the European Commission is a sample source code delivered "as is", it is provided as an example showing a possible integration with the SFC2014 web services based on a particular technology.

At any time without prior notice, the European Commission may make changes to the software.

Without limiting the foregoing, the European Commission makes no warranty that:

- The software will meet your requirements.
- The software will be uninterrupted, timely, secure or error-free.
- The results that may be obtained from the use of the software will be effective, accurate or reliable.
- The quality of the software will meet your expectations.
- Any errors in the software obtained from the sample application will be corrected.

The SDK and its documentation made available on the portal:

- Could include technical or other mistakes, inaccuracies or typographical errors.
- It will be only available on a specific technology
- Not all Webservices will have an associated SDK
- Errors will be corrected on a best effort basis.
- May be out of date and the European Commission makes no commitment to update such materials.

1.5. Cookies Directive

All the cookies are used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, and they are only used when is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service".

1.6. Contact Addresses:

Support

sfc2007-info@ec.europa.eu

ec-sfc2014-info@ec.europa.eu

ec-sfc2021-info@ec.europa.eu

Contacts for each DG involved in SFC:

DG AGRI

http://ec.europa.eu/agriculture/contact/index_en.htm

DG EMPL

http://ec.europa.eu/social/main.jsp?catId=2&langId=en

DG HOME

http://ec.europa.eu/dgs/home-affairs/who-we-are/contact-us/index_en.htm

DG MARE

http://ec.europa.eu/fisheries/about_us/contacts/index_en.htm

DG REGIO

http://ec.europa.eu/regional_policy/contacts/index_en.cfm

Contact for European Data Protection Supervisor and national data protection authorities

http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Contact/pid/156

http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm