FICHE NO 7

IMPLEMENTING ACT ON THE EXCHANGES OF INFORMATION BETWEEN THE MEMBER STATE AND THE COMMISSION (SFC2014)

VERSION 2 – 4 JUNE 2013

Regulation	Article
Common Provisions Regulation (CPR)	Article 63(4) Responsibilities of Member States

This document is provisional, without prejudice to the on-going Trilogues between the Council and the European Parliament (in line with the principle that "nothing is agreed until everything is agreed"). This document is a draft that shall be adjusted following the expert meeting.

It does not prejudge the final nature of the basic act, nor the content of any delegated or implementing act that may be prepared by the Commission.

1. EMPOWERMENT

Article 63(4) of the CPR sets out that:

4. All official exchanges of information between the Member State and the Commission shall be carried out using an electronic data exchange system established in compliance with the terms and conditions laid down by the Commission by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 143(3).

As the empowerment for the implementing act is provided for in Part II of the Common Provisions Regulation (CPR), it shall apply to all European Structural and Investment Funds (ESI Funds)[1].

2. MAIN OBJECTIVES AND SCOPE

This fiche is intended to provide explanation on aspects related to an implementing act which will contain uniform conditions for Article 63(4) of the proposed CPR concerning all official exchanges of information between the Member State and the Commission.

It should be emphasized that the modalities of exchange of information described in this document should be treated separately from the exchanges of information between beneficiaries and relevant authorities pursuant to Article 112(3) of the CPR (e-Cohesion).

3. MAIN ELEMENTS

The implementing act will contain the following main elements:

- The requirements as regards the content of computer system for data exchange (as set out in section 4.1 of this fiche);
- The requirements as regards the operation of computer system for data exchange (as set out in section 4.2 of this fiche);
- The rules on electronic transmission of data through a computer system for data exchange (as set out in section 4.3 of this fiche);
- The minimum rules in terms of security that should be respected in the data exchange by the European Commission and the Member States (as set out in Section 4.4 of this fiche).

4. CONTENT

4.1. CONTENT OF COMPUTER SYSTEM FOR DATA EXCHANGE

The computer system for data exchange between the European Commission and Member States (SFC2014) should contain all relevant information, rules and controls for the concerned ESI Funds as specified in the general regulation and in the delegated and implementing acts including but not limited to the formats and models defined within these acts. It should cover all official exchanges in both directions.

[1] Previously, CSF Funds.

Electronic data exchange refers to a medium of exchange of documents (see definition in Article 2(14) of Commission proposal for the Common Provisions Regulation - CPR) and data, either structured or unstructured.

The information provided in the electronic forms embedded in the electronic data exchange system shall be referred to as structured data. Data defined as structured cannot be replaced by non-structured data. This includes the use of hyperlinks or other types of references provided by Member States by which information is accessed in the form of non-structured data. Such references shall not be considered as having been transmitted to the Commission. Where Member States transmit inconsistent information in the form of non-structured data in the same system (e.g. as attachments), the structured data shall prevail.

A paper transmission of the formats/models would be possible only in case of *force majeure*[2], and in particular of malfunctioning of the computer system for data exchange or a lack of a lasting connection. As soon as the cause of force majeure ceases, the Member State or the European Commission will have to record the corresponding documents and data into the computer system for data exchange without delay.

4.2. OPERATION OF COMPUTER SYSTEM FOR DATA EXCHANGE

The Commission and relevant authorities within the Member State would record into SFC2014 the documents and data for which they are responsible, and any updates to these documents and data, in the electronic format required.

To guarantee a high quality of data and documents exchanged, any transmission of information to the European Commission would need to be verified by a member of staff of the relevant authorities other than the one who initiated the operation. This separation of tasks should be supported by SFC2014. It should mean in practice that the data recorded in the exchange system by one member of staff will have to be verified by another member of staff of the relevant authorities before being transmitted to the European Commission.

Member States would nominate, at the national or regional level, a person/s responsible for managing access rights to SFC2014. This Liaison Officer/s would be responsible for the following tasks:

– Identifying users requesting access in order to ensure they are indeed employed by the relevant authority responsible for the implementation of cohesion policy;

– Verifying the entitlement of users to the required privilege level in relation to their tasks and their hierarchical position;

– Requesting termination of access rights when no longer needed or justified;

– Promptly reporting any suspicious event that may result in prejudice to the security of the system;

– Ensuring continued accuracy of user identification data by reporting any changes;

[2] According to the ECJ, certain criteria need to be fulfilled in order for an event to qualify as a force majeure event. Essentially, this concept covers abnormal and unforeseeable circumstances beyond the control of the person invoking force majeure (i.e. of an insurmountable character) whose consequences could not have been avoided in spite of the exercise of all due care. The criteria are cumulative, i.e. force majeure is deemed to occur only when all conditions are met. See McNicholl v Ministry of Agriculture (Case 296/86).

– Taking the necessary precautions in terms of data privacy protection in accordance with the EU and national law;

– Informing the Commission of any changes affecting:

  o the capacity of their institution to act as such,

  o their personal capacity to act as such.

4.3. ELECTRONIC TRANSMISSION OF DATA THROUGH THE COMPUTER SYSTEM FOR DATA EXCHANGE

SFC2014 will need to be accessible to the Member States and the Commission either directly or via an interface for automatic synchronisation and recording of data with national, regional and local computer management systems.

For the functioning of the system it would be necessary to take into account:

- a compulsory electronic signature within the meaning of Directive 1999/93/EC[3];

- the protection of privacy of personal data for individuals according to Directive 2002/58/EC, Directive 1995/46/EC and Regulation 45/2001

4.4. SECURITY OF DATA TRANSMITTED THROUGH THE COMPUTER SYSTEM FOR DATA EXCHANGE

Member States and the Commission are responsible to implement and monitor the effectiveness of the security measures adopted to protect the data stored by them and transmitted through SFC2014.

Each Member State would adopt a national or regional IT security policy[4] dedicated to SFC2014. The scope of this IT security policy will need to include the IT aspects of the work performed by the Liaison Officer/s in case of web application use, and in addition to data processing and storage of data within the national, regional or local computer systems which are connected to SFC2014[5]. This IT security policy should be available on request to the European Commission. As a minimum the following areas should be included:

- Physical security
- Data media and access control
- Storage Control
- Access and Password Control
- Monitoring
- Interconnection to SFC2014
- Communication Infrastructure
- Human Resources
- Incident Management

[3] In light of the Directive, a closed-user group can agree to use a basic electronic signature in the framework of the contractual relations between the group and its members as a handwritten signature. SFC2007 signature elements have been defined as a closed-user group under article 41.3 of Commission Regulation n°1828/2006 of 08/12/2006. The same solution is valid for SFC2014.

[4] If Member States use only web application, there is no need for an IT security policy for SFC2014.

[5] If available, Member States can refer to their existing IT practices dealing with IT security. National documents on IT security can be re-used to meet this requirement.

The IT security policy will be based on a risk assessment. The measures described by this policy will need to be proportionate to the risks identified.

The risk assessment and the security policy will have to be updated if technological changes, identification of new threats or any other circumstances make it necessary. The security policy will need to be reviewed in any event on an annual basis to ensure that it is still appropriately responding to the latest risk assessment or any other newly identified technological change, threat or other relevant circumstance.

Each Member State would designate, at the national or regional level, a security officer responsible for maintaining and ensuring the application of the security policy for SFC2014 to all authorities using this system.

The European Commission would designate from among its personal a security officer responsible for defining, maintaining and ensuring the right application of the security policy for SFC2014.

Member States would need to abide by the IT security measures implemented in SFC2014 to secure the transmission of data, in particular in case of automatic interface.

5. MAIN CHANGES COMPARED TO THE PERIOD 2007-2013

The proposal for 2014-2020 programming period set out in Article 63(4) does not introduce any new particular responsibilities for Member States. It will consolidate only the current practice for 2007-2013 period (the relation between MS IT systems and SFC2007).

Currently, all official information concerning programme management has to be exchanged via SFC2007. In SFC2007, a typology of documents guides the user in this exchange (including "other MS document" or "other EC document"). In that sense, e-mail use should be restricted only to informal exchange of information (such as draft versions of documents) or information about project management (excluding major projects).

The system for an electronic data exchange (SFC2014) will be, as in the previous programming period, established by the European Commission.

This system will facilitate electronic exchange of the ESI Funds related information between the Commission and relevant bodies at the Member State level, in order to improve overall administration and management of these Funds, will give a more transparent reporting towards Member States and a comprehensive set of tools to manage the Funds.

Exchange of information between Member States and the Commission via the new SFC2014 system will support communication and collection of operational information from the Member States' administrations necessary for the follow-up and the financial management of the programmes in the 2014-2020 programming period.

The system will ensure proper transfer, management and monitoring of financial transactions.