Commission Implementing Regulation (EU) No 802/2014 of 24 July 2014 establishing models for national programmes and establishing the terms and conditions of the electronic data exchange system between the Commission and Member States pursuant to Regulation (EU) No 514/2014 of the European Parliament and of the Council laying down general provisions on the Asylum, Migration and Integration Fund and on the instrument for financial support for police cooperation, prevention and combating crime and crisis management

COMMISSION IMPLEMENTING REGULATION (EU) No 802/2014

of 24 July 2014

establishing models for national programmes and establishing the terms and conditions of the electronic data exchange system between the Commission and Member States pursuant to Regulation (EU) No 514/2014 of the European Parliament and of the Council laying down general provisions on the Asylum, Migration and Integration Fund and on the instrument for financial support for police cooperation, prevention and combating crime and crisis management

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 514/2014 of the European Parliament and of the Council of 16 April 2014 laying down general provisions on the Asylum, Migration and Integration Fund and on the instrument for financial support for police cooperation, preventing and combating crime, and crisis management[(1)], and in particular Articles 14(4) and 24(5) thereof,

Whereas:

(1) Regulation (EU) No 514/2014 together with the Specific Regulations referred to in Article 2(a) of Regulation (EU) No 514/2014, constitute a framework for Union funding to support the development of the area of freedom, security and justice.

(2) Regulation (EU) No 514/2014 requires each Member State to propose a multiannual national programme. To ensure that the information provided to the Commission is consistent and comparable, it is necessary to establish a model which the national programme should follow.

(3) Pursuant to Article 24(5) of Regulation (EU) No 514/2014 all official exchanges of information between Member States and the Commission are to be carried out using an electronic data exchange system. It is therefore necessary to establish the terms and conditions with which that electronic data exchange system should comply. In order to be cost-effective and ensure overall coherence with all Union shared management Funds, the terms and conditions of the electronic data exchange system are the same, to the extent possible, as those provided for in Commission Implementing Regulation (EU) No 184/2014[(2)].

(4) In order to improve the quality of information exchanged, and to render the information exchange system simpler and more useful, it is necessary to lay down basic requirements regarding the form and scope of the information to be exchanged.

(5) Principles and rules should be laid down regarding the identification of the party responsible for uploading documents into the electronic data exchange system and updating those documents

(6) Technical characteristics for an efficient electronic exchange system should be established in order to reduce the administrative burden for Member States and the Commission.

(7) To ensure that both Member States and the Commission can continue to exchange information in cases of *force majeure* that hinder the use of electronic data exchange system, alternative means to encode and transfer data need to be specified.

(8) Member States and the Commission should ensure that transfer of data through the electronic data exchange system is performed in a secured manner allowing for availability, integrity, authenticity, confidentiality and non-repudiation of information. Therefore rules on security should be set out.

(9) This Regulation respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, and notably the right to protection of personal data. This Regulation should therefore be applied in accordance with these rights and principles. Concerning personal data processed by Member States, Directive 95/46/EC of the European Parliament and of the Council[(3)] applies. Concerning the processing of personal data by the Union institutions and bodies and the free movement of such data, Regulation (EC) No 45/2001 of the European Parliament and of the Council[(4)] applies.

(10) In order to allow for the prompt application of the measures provided for in this Regulation and not delay the approval of the national programmes, this Regulation should enter into force on the day following that of its publication in the *Official Journal of the European Union*.

(11) The United Kingdom and Ireland are bound by Regulation (EU) No 514/2014 and are as a consequence bound by this Regulation.

(12) Denmark is not bound by Regulation (EU) No 514/2014 nor by this Regulation.

(13) The measures provided for in this Regulation are in accordance with the opinion of the 'Asylum, Migration and Integration and Internal Security Funds' Committee.

HAS ADOPTED THIS REGULATION:

Article 1

Models for national programmes

The model for national programmes is set out in the Annex.

Article 2

Establishment of electronic data exchange system

The Commission shall establish an electronic data exchange system for all official exchanges of information between Member States and the Commission (hereinafter referred to as 'SFC2014').

Article 3

Content of electronic data exchange system

1 SFC2014 shall contain at least the information specified in the models, formats and templates established in accordance with Article 1 of this Regulation, that are in accordance with the Regulation (EU) No 514/2014 and the Specific Regulations referred to in Article 2(a) of Regulation (EU) No 514/2014.

2 The information provided in the electronic forms embedded in SFC2014 (hereinafter referred to as 'structured data') shall not be replaced by non-structured data, including the use of hyperlinks or other types of non-structured data such as attachment of documents or images. Where a Member State transmits the same information in the form of structured data and non-structured data, the structured data shall be used in case of inconsistencies.

Article 4

Operation of SFC2014

1 The Commission and the competent authorities referred to in Article 25 of Regulation (EU) No 514/2014 shall enter into SFC2014 the information for the transmission of which they are responsible, and any updates thereto.

2 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 the Member State's management and control information systems connected automatically with SFC2014.

3 Member States shall appoint, at national or regional level or at both national and regional levels, one or more persons responsible for managing access rights to SFC2014. Those persons shall fulfil the following tasks:

a identifying users requesting access, making sure those users are employed by the organisation;

b informing users about their obligations to preserve the security of the system;

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

d requesting the termination of access rights when those access rights are no longer needed or justified;

e promptly reporting suspicious events that may undermine the security of the system;

f ensuring the continued accuracy of user identification data by reporting any changes;

g taking the necessary data protection and commercial confidentiality precautions in accordance with applicable Union and national rules; and

h informing the Commission of any changes affecting the capacity of the Member State authorities or users of SFC2014 to carry out the responsibilities referred to in paragraph 1 or their personal capacity to carry out the responsibilities referred to in points (a) to (g).

4 Exchanges of data and transactions shall bear a compulsory electronic signature within the meaning of Directive 1999/93/EC of the European Parliament and of the Council[5]. Member States and the Commission shall recognise the legal effectiveness and admissibility of the electronic signature used in SFC2014 as evidence in legal proceedings.

5 Information processed through SFC2014 shall respect the protection of privacy of personal data for individuals and commercial confidentiality for legal entities in accordance with Directive 2002/58/EC of the European Parliament and of the Council[6], Directive 2009/136/EC of the European Parliament and of the Council[7], Directive 95/46/EC and Regulation (EC) No 45/2001.

Article 5

Characteristics of SFC2014

In order to ensure the electronic exchange of information, SFC2014 shall have the following characteristics:

(a) interactive forms or forms pre-filled by the system on the basis of data already previously recorded in the system;

(b) automatic calculations, where they reduce the encoding effort of users;

(c) automatic embedded controls to verify internal consistency of transmitted data and consistency of this data with applicable rules;

(d) system-generated alerts warning SFC2014 users that certain actions can or cannot be performed;

(e) online status tracking of the treatment of information entered into the system; and

(f) availability of historical data in respect of all information entered for a national programme.

Article 6

Transmission of data through SFC2014

1 SFC2014 shall be accessible to Member States and the Commission either directly through an interactive user interface (that is to say, a Web application) or via a technical interface using predefined protocols (that is to say, Web services) that allows for automatic synchronisation and transmission of data between Member States information systems and SFC2014.

2 The date of electronic transmission of information by the Member State to the Commission and vice versa shall be considered to be the date of submission of the document concerned.

3 In cases of *force majeure*, a malfunctioning of SFC2014 or a lack of a connection with SFC2014 exceeding one working day in the last week before a regulatory deadline for the submission of information or five working days at other times, the information exchange

between Member State and the Commission may take place in paper form using the models, formats and templates referred to in Article 3(1).

When the electronic exchange system ceases to malfunction, the connection with that system is re-established or the cause of *force majeure* ceases, the party concerned shall enter without delay the information already sent in paper form into SFC2014.

4 In cases referred to in paragraph 3 the date stamped by the post shall be considered to be the date of submission of the document concerned.

Article 7

Security of data transmitted through SFC2014

1 The Commission shall establish an information technology security policy (hereinafter referred to as 'SFC IT security policy') for SFC2014 applicable to personnel using SFC2014 in accordance with relevant Union rules, in particular Commission Decision C(2006)3602[8] and its implementing rules. The Commission shall designate one or more persons responsible for defining, maintaining and ensuring the correct application of the security policy for SFC2014.

2 Member States and European institutions other than the Commission, who have received access rights to SFC2014, shall comply with the IT security terms and conditions published in the SFC2014 portal and the measures that are implemented in SFC2014 by the Commission to secure the transmission of data, in particular in relation to the use of the technical interface referred to in Article 6(1) of this Regulation.

3 Member States and the Commission shall implement and ensure effectiveness of security measures adopted to protect the data they have stored and transmitted through SFC2014.

4 Member States shall adopt national, regional or local information technology security policies covering access to SFC2014 and automatic input of data into it, ensuring a minimum set of security requirements. These national, regional or local IT security policies may refer to other security documents. Each Member State shall ensure that these IT security policies apply to all authorities using SFC2014.

5 These national, regional or local IT security policies shall include:

a the IT security aspects of the work performed by the person or persons responsible for managing the access rights referred to in Article 4(3) of this Regulation when working directly in SFC2014; and

b the IT security measures for those national, regional or local computer systems connected to SFC2014 through a technical interface referred to in Article 6(1) of this Regulation.

For the purposes of point (b) of the first subparagraph, the following aspects of IT security shall be covered, as appropriate:

(a) physical security;

(b) data media and access control;

(c) storage control;

(d) access and password control;

(e) monitoring;