

**DURCHFÜHRUNGSVERORDNUNG (EU) Nr. 463/2014 DER KOMMISSION****vom 5. Mai 2014****zur Festlegung der Vorschriften und Anforderungen für das System für den elektronischen Datenaustausch zwischen den Mitgliedstaaten und der Kommission gemäß der Verordnung (EU) Nr. 223/2014 des Europäischen Parlaments und des Rates zum Europäischen Hilfsfonds für die am stärksten benachteiligten Personen**

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) Nr. 223/2014 des Europäischen Parlaments und des Rates vom 11. März 2014 zum Europäischen Hilfsfonds für die am stärksten benachteiligten Personen <sup>(1)</sup>, insbesondere Artikel 30 Absatz 4,

in Erwägung nachstehender Gründe:

- (1) Gemäß Artikel 30 Absatz 4 der Verordnung (EU) Nr. 223/2014 wird der gesamte offizielle Informationsaustausch zwischen den Mitgliedstaaten und der Kommission über ein elektronisches Datenaustauschsystem abgewickelt. Deshalb ist es notwendig, Vorschriften und Anforderungen festzulegen, denen das elektronische Datenaustauschsystem entsprechen muss.
- (2) Um eine hohe Qualität der Informationen über die Durchführung der operationellen Programme zu gewährleisten, den Nutzen des Systems zu optimieren und dessen Handhabung zu vereinfachen, sollten Grundanforderungen zur Form und zum Umfang der auszutauschenden Informationen definiert werden.
- (3) Es sollten Grundsätze sowie für den Betrieb des Systems geltende Vorschriften festgelegt werden, die die Identifizierung der für das Hochladen von Dokumenten bzw. für deren Aktualisierung verantwortlichen Akteure regeln.
- (4) Um den Verwaltungsaufwand für die Mitgliedstaaten und die Kommission zu verringern und zugleich einen wirksamen, effizienten elektronischen Informationsaustausch zu gewährleisten, sollten die technischen Charakteristika des Systems festgelegt werden.
- (5) Die Mitgliedstaaten und die Kommission sollten ferner die Möglichkeit haben, Daten auf zweierlei Weise zu verschlüsseln und zu übermitteln; diese Möglichkeiten sind zu spezifizieren. Zudem sollten Vorschriften für den Fall aufgestellt werden, dass der elektronische Datenaustausch durch höhere Gewalt behindert wird, so dass sowohl die Mitgliedstaaten als auch die Kommission den Informationsaustausch über alternative Wege fortsetzen können.
- (6) Die Mitgliedstaaten und die Kommission sollten dafür sorgen, dass die Datenübertragung über das elektronische Datenaustauschsystem in abgesicherter Form erfolgt, so dass Verfügbarkeit, Vollständigkeit, Authentizität, Vertraulichkeit und Nichtabstreitbarkeit der Informationen gewährleistet sind. Daher sollten Vorschriften über die Sicherheit festgelegt werden.
- (7) Die vorliegende Verordnung sollte im Einklang mit den Grundrechten und Grundsätzen stehen, die mit der Charta der Grundrechte der Europäischen Union anerkannt wurden, insbesondere mit dem Recht auf Schutz personenbezogener Daten. Sie sollte daher entsprechend diesen Rechten und Grundsätzen angewandt werden. Für die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten gilt die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates <sup>(2)</sup>. Für die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Union und den freien Verkehr dieser Daten gilt die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates <sup>(3)</sup>.

<sup>(1)</sup> Verordnung (EU) Nr. 223/2014 des Europäischen Parlaments und des Rates vom 11. März 2014 zum Europäischen Hilfsfonds für die am stärksten benachteiligten Personen (ABl. L 72 vom 12.3.2014, S. 1).

<sup>(2)</sup> Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

<sup>(3)</sup> Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

- (8) Damit die in dieser Verordnung vorgesehenen Maßnahmen zügig angewandt werden können, sollte diese Verordnung am Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft treten.
- (9) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des Ausschusses für den Europäischen Hilfsfonds für die am stärksten benachteiligten Personen —

HAT FOLGENDE VERORDNUNG ERLASSEN:

#### KAPITEL I

### BESTIMMUNGEN ZUR DURCHFÜHRUNG DER VERORDNUNG (EU) NR. 223/2014 ZUM EUROPÄISCHEN HILFSFONDS FÜR DIE AM STÄRKSTEN BENACHTEILIGTEN PERSONEN (FEAD)

#### ELEKTRONISCHES DATENAUSTAUSCHSYSTEM

(Befugnis gemäß Artikel 30 Absatz 4 der Verordnung (EU) Nr. 223/2014)

##### Artikel 1

#### Einrichtung eines elektronischen Datenaustauschsystems

Die Kommission richtet ein elektronisches Datenaustauschsystem für den offiziellen Informationsaustausch zwischen den Mitgliedstaaten und der Kommission ein.

##### Artikel 2

#### Inhalt des elektronischen Datenaustauschsystems

Das elektronische Datenaustauschsystem (im Folgenden „SFC2014“) enthält mindestens die Informationen, die in den Modellen, Formaten und Vorlagen vorgesehen sind, die nach Maßgabe der Verordnung (EU) Nr. 223/2014 festgelegt sind. Die Informationen, die in den in SFC2014 integrierten elektronischen Formularen bereitgestellt werden (im Folgenden „strukturierte Daten“), dürfen nicht durch nichtstrukturierte Daten, einschließlich Hyperlinks und andere Formen nichtstrukturierter Daten, z. B. angehängte Dokumente oder Bilder, ersetzt werden. Übermittelt ein Mitgliedstaat die gleichen Informationen in Form strukturierter Daten und nichtstrukturierter Daten, werden im Falle von Unstimmigkeiten die strukturierten Daten verwendet.

##### Artikel 3

#### Verwendung von SFC2014

(1) Die Kommission, die von den Mitgliedstaaten benannten Behörden gemäß Artikel 59 Absatz 3 der Verordnung (EU, Euratom) Nr. 966/2012 des Europäischen Parlaments und des Rates <sup>(1)</sup> und Artikel 31 der Verordnung (EU) Nr. 223/2014 sowie die Stellen, denen Aufgaben jener Behörden übertragen wurden, geben die Informationen, für deren Übermittlung sie zuständig sind, und gegebenenfalls Aktualisierungen dieser Informationen in SFC2014 ein.

(2) Sämtliche Übermittlungen von Informationen an die Kommission werden von einer Person überprüft und veranlasst, die nicht mit der Person identisch ist, die die zu übermittelnden Daten eingegeben hat. Diese Aufgabentrennung wird von SFC2014 bzw. von den automatisch an SFC2014 angebotenen IT-Systemen der Mitgliedstaaten für Verwaltung und Kontrolle unterstützt.

(3) Die Mitgliedstaaten benennen auf nationaler Ebene Personen, die für die Verwaltung der Zugangsrechte zu SFC2014 zuständig sind und die die folgenden Aufgaben ausführen:

- a) Feststellung der Identität der Benutzer, die einen Zugang beantragen, und Prüfung, ob sie tatsächlich von der betreffenden Organisation beschäftigt werden;
- b) Aufklärung der Benutzer über ihre Pflichten zur Gewährleistung der Sicherheit des Systems;

<sup>(1)</sup> Verordnung (EU, Euratom) Nr. 966/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 über die Haushaltsordnung für den Gesamthaushaltsplan der Union und zur Aufhebung der Verordnung (EG, Euratom) Nr. 1605/2002 des Rates (ABl. L 298 vom 26.10.2012, S. 1).

- c) Überprüfung des Anrechts von Benutzern auf die angeforderte Berechtigungsebene im Hinblick auf ihre Aufgaben und ihre hierarchische Stellung;
- d) Anforderung des Entzugs von Zugriffsrechten, wenn kein Bedarf oder Grund für diese Rechte mehr vorliegt;
- e) unverzügliche Meldung verdächtiger Ereignisse, die die Sicherheit des Systems beeinträchtigen könnten;
- f) Sicherstellung der fortlaufenden Richtigkeit der Identifizierungsdaten der Benutzer durch Meldung von Änderungen;
- g) Ergreifen der erforderlichen Vorsichtsmaßnahmen zum Datenschutz und zur Wahrung des Geschäftsgeheimnisses gemäß den Vorschriften der Union und des betreffenden Mitgliedstaats;
- h) Unterrichtung der Kommission über sämtliche Änderungen, die sich auswirken auf die Fähigkeit der Behörden der Mitgliedstaaten oder der SFC2014-Benutzer, ihre Aufgaben gemäß Absatz 1 zu erfüllen, bzw. auf ihre persönliche Fähigkeit, die unter den Buchstaben a bis g genannten Aufgaben zu erfüllen.

(4) Der Datenaustausch und die Vorgänge werden im Sinne der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates <sup>(1)</sup> obligatorisch elektronisch signiert. Die Mitgliedstaaten und die Kommission erkennen die rechtliche Wirksamkeit und Zulässigkeit der in SFC2014 verwendeten elektronischen Signatur als Beweismittel in Gerichtsverfahren an.

Bei der Verarbeitung von Informationen über SFC2014 wird gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates <sup>(2)</sup>, der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates <sup>(3)</sup>, der Richtlinie 1995/46/EG und der Verordnung (EG) Nr. 45/2001 der Schutz der Privatsphäre und personenbezogener Daten (im Falle natürlicher Personen) bzw. die Wahrung des Geschäftsgeheimnisses (im Falle juristischer Personen) gewährleistet.

#### Artikel 4

##### **Merkmale von SFC2014**

Um einen wirksamen, effizienten elektronischen Informationsaustausch zu gewährleisten, weist SFC2014 folgende Merkmale auf:

- a) interaktive Formulare oder vorab vom System ausgefüllte Formulare, die sich auf die bereits im System erfassten Daten stützen;
- b) automatische Berechnungen, wenn dies den Eingabeaufwand der Benutzer verringert;
- c) eingebettete automatische Kontrollen, um die interne Kohärenz der übermittelten Daten sowie ihre Übereinstimmung mit den geltenden Regeln zu prüfen;
- d) vom System generierte Warnmeldungen, die die SFC2014-Benutzer darüber informieren, dass bestimmte Vorgänge ausgeführt bzw. nicht ausgeführt werden können;
- e) Online-Verfolgung der Verarbeitung von in das System eingegebenen Informationen;
- f) Verfügbarkeit historischer Daten zu sämtlichen Informationen, die für ein operationelles Programm eingegeben wurden.

#### Artikel 5

##### **Übermittlung von Daten über SFC2014**

(1) Die Mitgliedstaaten und die Kommission greifen auf SFC2014 entweder direkt über eine interaktive Benutzeroberfläche (d. h. eine Web-Anwendung) zu oder über eine technische Schnittstelle, die mit vordefinierten Protokollen (d. h. Web-Diensten) arbeitet und die die automatische Synchronisierung und Übertragung von Daten zwischen den Informationssystemen der Mitgliedstaaten und SFC2014 ermöglicht.

<sup>(1)</sup> Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. L 13 vom 19.1.2000, S. 12).

<sup>(2)</sup> Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

<sup>(3)</sup> Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (ABl. L 337 vom 18.12.2009, S. 11).

(2) Das Datum der elektronischen Übermittlung der Informationen vom Mitgliedstaat an die Kommission bzw. in umgekehrter Richtung gilt als Datum der Vorlage des betreffenden Dokuments.

(3) Im Falle höherer Gewalt, einer Funktionsstörung von SFC2014 oder einer gestörten Verbindung zu SFC2014, die vor Ablauf einer vorgeschriebenen Frist für die Einreichung von Informationen oder innerhalb des Zeitraums vom 23. bis zum 31. Dezember länger als einen Arbeitstag andauert oder die in anderen Zeiten länger als fünf Arbeitstage andauert, kann der Informationsaustausch zwischen dem betreffenden Mitgliedstaat und der Kommission auf Papier erfolgen, wobei die in Artikel 2 Absatz 1 der vorliegenden Verordnung genannten Modelle, Formate und Vorlagen zu verwenden sind.

Ist die Störung des elektronischen Datenaustauschsystems behoben, die Verbindung zum System wiederhergestellt oder sind die Gründe der höheren Gewalt nicht mehr gegeben, gibt der betreffende Akteur die bereits auf Papier übermittelten Informationen auch in SFC2014 ein.

(4) In den in Absatz 3 genannten Fällen gilt das Datum des Poststempels als Datum der Vorlage des betreffenden Dokuments.

#### Artikel 6

##### **Sicherheit der über SFC2014 übermittelten Daten**

(1) Die Kommission stellt für SFC2014 eine Strategie für die Informationstechnologiesicherheit (im Folgenden „SFC-Strategie für IT-Sicherheit“) auf, die für sämtliches Personal gilt, das SFC2014 verwendet, und die mit den relevanten Unionsbestimmungen, insbesondere dem Beschluss K(2006) 3602 <sup>(1)</sup> und dessen Durchführungsvorschriften, in Einklang steht. Die Kommission benennt eine Person oder mehrere Personen, die für die Festlegung der Sicherheitsstrategie, ihre Einhaltung und ihre ordnungsgemäße Anwendung in SFC2014 verantwortlich ist bzw. sind.

(2) Die Mitgliedstaaten und andere Europäische Institutionen als die Kommission, die Zugangsrechte zu SFC2014 erhalten haben, kommen den im SFC2014-Portal veröffentlichten Vorschriften und Anforderungen für IT-Sicherheit sowie den Maßnahmen nach, die die Kommission in SFC2014 implementiert, um eine sichere Datenübertragung zu gewährleisten; dies gilt insbesondere für die Verwendung der in Artikel 5 Absatz 1 der vorliegenden Verordnung genannten technischen Schnittstelle.

(3) Die Mitgliedstaaten und die Kommission setzen die für den Schutz der Daten, die sie mittels SFC2014 speichern und übertragen, festgelegten Sicherheitsmaßnahmen um und gewährleisten deren Wirksamkeit.

(4) Die Mitgliedstaaten legen nationale, regionale oder lokale Strategien für IT-Sicherheit fest, die den Zugang zu SFC2014 und die automatische Eingabe von Daten in SFC2014 regeln und die die Einhaltung eines Mindestmaßes an Sicherheitsanforderungen gewährleisten. In diesen nationalen, regionalen oder lokalen Strategien für IT-Sicherheit kann auf andere Sicherheitsdokumente verwiesen werden. Jeder Mitgliedstaat stellt sicher, dass jene Strategien für IT-Sicherheit für alle Behörden gelten, die SFC2014 verwenden.

(5) Diese nationalen, regionalen oder lokalen Strategien für IT-Sicherheit decken Folgendes ab:

- a) im Falle der direkten Nutzung von SFC2014 die für die IT-Sicherheit relevanten Aspekte der Tätigkeiten, die die für die Verwaltung der Zugangsrechte zuständigen Personen gemäß Artikel 3 Absatz 3 der vorliegenden Verordnung ausführen;
- b) in dem Fall, dass nationale, regionale oder lokale IT-Systeme über eine technische Schnittstelle gemäß Artikel 5 Absatz 1 der vorliegenden Verordnung an SFC2014 angebunden werden, die für diese Systeme geltenden Sicherheitsmaßnahmen, mit denen die Einhaltung der Sicherheitsanforderungen für SFC2014 durch diese Systeme sichergestellt wird.

Für die Zwecke von Unterabsatz 1 Buchstabe b sind gegebenenfalls folgende Aspekte zu regeln:

- a) physische Sicherheit;
- b) Kontrolle von Datenträgern und des Zugangs dazu;
- c) Kontrolle der Speicherung;
- d) Zugangs- und Kennwortkontrolle;
- e) Monitoring;
- f) Anbindung an SFC2014;

<sup>(1)</sup> Beschluss K(2006) 3602 der Kommission vom 16. August 2006 betreffend die Sicherheit der von den Dienststellen der Kommission genutzten Informationssysteme.

- g) Kommunikationsinfrastruktur;
- h) Management von Humanressourcen vor der Einstellung, während des Arbeitsverhältnisses und nach Beendigung des Arbeitsverhältnisses;
- i) Störungsmanagement.

(6) Diese nationalen, regionalen oder lokalen Strategien für IT-Sicherheit basieren auf einer Risikobewertung, und die in den Strategien beschriebenen Maßnahmen stehen im Verhältnis zu den identifizierten Risiken.

(7) Die Dokumente zur Spezifizierung der nationalen, regionalen oder lokalen Strategien für IT-Sicherheit werden der Kommission auf Anfrage zur Verfügung gestellt.

(8) Die Mitgliedstaaten benennen auf nationaler Ebene eine Person oder mehrere Personen, die für die Einhaltung und die Anwendung der nationalen, regionalen oder lokalen Strategien für IT-Sicherheit verantwortlich ist bzw. sind. Diese Person dient bzw. diese Personen dienen als Ansprechpartner für die gemäß Artikel 6 Absatz 1 der vorliegenden Verordnung von der Kommission benannte Person bzw. benannten Personen.

(9) Sowohl die SFC-Strategie für IT-Sicherheit als auch die relevanten nationalen, regionalen und lokalen Strategien für IT-Sicherheit werden im Falle technologischer Änderungen, der Feststellung neuer Bedrohungen oder sonstiger relevanter Entwicklungen aktualisiert. In jedem Fall werden die Strategien jährlich überprüft, um ihre fortlaufende Wirksamkeit sicherzustellen.

## KAPITEL II

### SCHLUSSBESTIMMUNG

#### Artikel 7

Diese Verordnung tritt am Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 5. Mai 2014

*Für die Kommission*  
*Der Präsident*  
José Manuel BARROSO