

**ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) NR 463/2014****z dnia 5 maja 2014 r.****ustanawiające, na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 223/2014 w sprawie Europejskiego Funduszu Pomocy Najbardziej Potrzebującym, zasady i warunki mające zastosowanie do systemu elektronicznej wymiany danych między państwami członkowskimi i Komisją**

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 223/2014 z dnia 11 marca 2014 r. w sprawie Europejskiego Funduszu Pomocy Najbardziej Potrzebującym <sup>(1)</sup>, w szczególności jego art. 30 ust. 4,

a także mając na uwadze, co następuje:

- (1) Na podstawie art. 30 ust. 4 rozporządzenia (UE) nr 223/2014 wszelka oficjalna wymiana informacji między państwem członkowskim a Komisją odbywa się z wykorzystaniem systemu elektronicznej wymiany danych. Należy w związku z tym ustanowić warunki, jakie powinien spełniać taki system elektronicznej wymiany danych.
- (2) Aby zapewnić jak najwyższą jakość informacji na temat wdrażania programów operacyjnych, zwiększyć przydatność systemu i uprościć go, konieczne jest określenie podstawowych wymogów co do formy i zakresu wymienianych informacji.
- (3) Należy określić zasady oraz odpowiednie przepisy dotyczące działania systemu, jeśli chodzi o wskazywanie strony odpowiedzialnej za zamieszczanie dokumentów i wszelką ich aktualizację.
- (4) Aby zagwarantować zmniejszenie obciążeń administracyjnych dla państw członkowskich i Komisji, a jednocześnie sprawną i skuteczną elektroniczną wymianę informacji, konieczne jest określenie charakterystyki technicznej systemu.
- (5) Państwa członkowskie i Komisja powinny mieć także możliwość wprowadzania i przesyłania danych na dwa różne sposoby, które należy określić. Należy także przewidzieć przepisy na wypadek działania siły wyższej, uniemożliwiającej korzystanie z systemu elektronicznej wymiany danych, aby zarówno państwa członkowskie, jak i Komisja mogły nadal wymieniać informacje za pomocą alternatywnych środków.
- (6) Państwa członkowskie i Komisja powinny zapewnić, aby przekazywanie danych za pośrednictwem systemu elektronicznej wymiany danych odbywało się w sposób zabezpieczony, gwarantujący dostępność, integralność, wiarygodność, poufność i niezaprzeczalność informacji. Należy w związku z tym określić zasady bezpieczeństwa.
- (7) Niniejsze rozporządzenie nie powinno naruszać praw podstawowych i powinno być zgodne z zasadami uznawanymi w Karcie praw podstawowych Unii Europejskiej, a w szczególności prawem do ochrony danych osobowych. Niniejsze rozporządzenie powinno zatem być stosowane zgodnie z tymi prawami i zasadami. W odniesieniu do danych osobowych przetwarzanych przez państwa członkowskie zastosowanie ma dyrektywa 95/46/WE Parlamentu Europejskiego i Rady <sup>(2)</sup>. W odniesieniu do przetwarzania danych osobowych przez instytucje i podmioty unijne i swobodnego przepływu takich danych zastosowanie ma rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady <sup>(3)</sup>.

<sup>(1)</sup> Dz.U. L 72 z 12.3.2014, s. 1.<sup>(2)</sup> Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).<sup>(3)</sup> Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

- (8) Aby umożliwić szybkie zastosowanie środków przewidzianych w niniejszym rozporządzeniu, powinno ono wejść w życie następnego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.
- (9) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią Komitetu ds. Europejskiego Funduszu Pomocy Najbardziej Potrzebującym,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

#### ROZDZIAŁ I

### PRZEPISY WYKONAWCZE DO ROZPORZĄDZENIA (UE) NR 223/2014 W ODNIESIENIU DO EUROPEJSKIEGO FUNDUSZU POMOCY NAJBARDZIEJ POTRZEBUJĄCYM (FEAD)

#### SYSTEM ELEKTRONICZNEJ WYMIANY DANYCH

(Uprawnienie na mocy art. 30 ust. 4 rozporządzenia (UE) nr 223/2014)

##### Artykuł 1

#### Ustanowienie systemu elektronicznej wymiany danych

Komisja ustanawia system elektronicznej wymiany danych stosowany do wszelkiej oficjalnej wymiany informacji między państwem członkowskim a Komisją.

##### Artykuł 2

#### Zawartość systemu elektronicznej wymiany danych

System elektronicznej wymiany danych (zwany dalej „SFC 2014”) zawiera przynajmniej informacje wyszczególnione w modelach, formatach i wzorach ustanowionych zgodnie z rozporządzeniem (UE) nr 223/2014. Informacji podanych w formularzach elektronicznych należących do systemu SFC2014 (zwanymi dalej „danymi ustrukturyzowanymi”) nie można zastępować danymi nieustrukturyzowanymi, w tym wykorzystując hiperłącza lub inne rodzaje nieustrukturyzowanych danych, takich jak załączone dokumenty lub obrazy. Jeśli państwo członkowskie przekazuje te same informacje w postaci danych ustrukturyzowanych i nieustrukturyzowanych, w przypadku rozbieżności wykorzystuje się dane ustrukturyzowane.

##### Artykuł 3

#### Działanie systemu SFC2014

1. Komisja, instytucje wyznaczone przez państwo członkowskie na mocy art. 59 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 966/2012 <sup>(1)</sup> i art. 31 rozporządzenia (UE) nr 223/2014 oraz organy, którym powierzono wykonanie zadań tych instytucji, wprowadzają do systemu SFC2014 informacje, za których przekazywanie odpowiadają, a także wszelkie ich aktualizacje.
2. Przekazywanie informacji Komisji jest zawsze weryfikowane i dokonywane przez inną osobę niż osoba, która wprowadziła przekazywane dane. Taki podział zadań jest obsługiwany przez system SFC2014 lub systemy informatyczne zarządzania i kontroli państwa członkowskiego automatycznie połączone z systemem SFC2014.
3. Państwa członkowskie wyznaczają — na szczeblu krajowym — osobę lub osoby odpowiedzialne za zarządzanie prawami dostępu do systemu SFC2014, które to osoby wykonują następujące zadania:
  - a) sprawdzanie tożsamości użytkowników wnioskujących o prawa dostępu w celu upewnienia się, czy są oni rzeczywiście pracownikami danej organizacji;
  - b) informowanie użytkowników o spoczywających na nich obowiązkach w zakresie zachowania bezpieczeństwa systemu;

<sup>(1)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 966/2012 z dnia 25 października 2012 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii oraz uchylające rozporządzenie Rady (WE, Euratom) nr 1605/2002 (Dz.U. L 298 z 26.10.2012, s. 1).

- c) weryfikowanie uprawnień użytkowników do wymaganego poziomu uprzywilejowania w stosunku do wykonywanych przez nich zadań i zajmowanych przez nich pozycji w hierarchii;
- d) występowanie o odebranie praw dostępu, gdy nie są już one potrzebne lub uzasadnione;
- e) szybkie zgłaszanie podejrzanych zdarzeń, które mogą naruszyć bezpieczeństwo systemu;
- f) zapewnianie stałej aktualności danych identyfikacyjnych użytkowników poprzez zgłaszanie wszelkich zmian;
- g) podejmowanie niezbędnych środków ostrożności w zakresie ochrony danych i tajemnicy handlowej zgodnie z przepisami unijnymi i krajowymi;
- h) powiadamianie Komisji o wszystkich zmianach wpływających na zdolność instytucji państwa członkowskiego lub użytkowników systemu SFC2014 do wypełniania obowiązków, o których mowa w ust. 1, lub na ich osobistą zdolność do wypełniania zadań, o których mowa w lit. a)–g).

4. Wymiana danych oraz transakcje opatrzone są obowiązkowym podpisem elektronicznym w rozumieniu dyrektywy 1999/93/WE Parlamentu Europejskiego i Rady <sup>(1)</sup>. Państwa członkowskie i Komisja uznają skuteczność prawną i dopuszczalność podpisów elektronicznych używanych w systemie SFC2014 jako dowodów w postępowaniu sądowym.

Przetwarzanie informacji w systemie SFC2014 odbywa się zgodnie z zasadami ochrony prywatności i danych osobowych w przypadku osób fizycznych oraz tajemnicy handlowej w przypadku osób prawnych, zgodnie z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady <sup>(2)</sup>, dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady <sup>(3)</sup>, dyrektywą 1995/46/WE oraz rozporządzeniem (WE) nr 45/2001.

#### Artykuł 4

### Charakterystyka systemu SFC2014

Aby zapewnić sprawną i skuteczną elektroniczną wymianę informacji, system SFC2014 obejmuje następujące elementy:

- a) formularze interaktywne lub formularze uprzednio wypełnione przez system na podstawie danych już zapisanych w systemie;
- b) automatyczne wyliczenia, jeśli ułatwiają one użytkownikom wprowadzanie danych;
- c) automatyczne zintegrowane kontrole służące weryfikacji wewnętrznej spójności przekazywanych danych i spójności tych danych z obowiązującymi przepisami;
- d) generowane przez system ostrzeżenia, informujące użytkowników systemu SFC2014, że niektóre działania mogą lub nie mogą zostać wykonane;
- e) elektroniczny system śledzenia statusu przetwarzania informacji wprowadzonych do systemu;
- f) dostępność danych historycznych w odniesieniu do wszystkich informacji wprowadzonych w zakresie danego programu operacyjnego.

#### Artykuł 5

### Przekazywanie danych w systemie SFC2014

1. System SFC2014 dostępny jest dla państw członkowskich i Komisji bądź bezpośrednio przez interaktywny interfejs użytkownika (tj. stronę internetową), bądź przez interfejs techniczny wykorzystujący predefiniowane protokoły (tj. usługi sieciowe), które umożliwiają automatyczną synchronizację i przekazywanie danych między systemami informatycznymi państw członkowskich a systemem SFC2014.

<sup>(1)</sup> Dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.U. L 13 z 19.1.2000, s. 12).

<sup>(2)</sup> Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

<sup>(3)</sup> Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (Dz.U. L 337 z 18.12.2009, s. 11).

2. Data elektronicznego przekazania informacji Komisji przez państwo członkowskie oraz państwu członkowskiemu przez Komisję uznawana jest za datę przedłożenia danego dokumentu.

3. W przypadku działania siły wyższej, wadliwego działania systemu SFC2014 lub braku łączności z systemem SFC2014 przez okres dłuższy niż jeden dzień roboczy w tygodniu poprzedzającym ustawowy termin przedkładania informacji bądź w okresie od 23 do 31 grudnia, lub pięć dni roboczych w innych okresach, wymiana informacji między państwem członkowskim a Komisją może odbywać się w formie papierowej, przy wykorzystaniu modeli, formatów i wzorów, o których mowa w art. 2 niniejszego rozporządzenia.

Zainteresowana strona wprowadza informacje przesłane już w formie papierowej także do systemu SFC2014 niezwłocznie po tym, jak ustaje wadliwe działanie systemu elektronicznej wymiany, odnowione zostaje połączenie z systemem lub przestaje działać siła wyższa.

4. W przypadkach, o których mowa w ust. 3, za datę przedłożenia danego dokumentu uznaje się datę stempla pocztowego.

## Artykuł 6

### Bezpieczeństwo danych przekazywanych w systemie SFC2014

1. Komisja ustanawia politykę bezpieczeństwa technologii informacyjnych (zwaną dalej „polityką bezpieczeństwa IT dla SFC”) dla systemu SFC2014, obowiązującą pracowników korzystających z systemu SFC2014 zgodnie z odnośnymi przepisami unijnymi, zwłaszcza decyzją Komisji C(2006) 3602 (1) i przepisami wykonawczymi do tej decyzji. Komisja wyznacza osobę lub osoby odpowiedzialne za określanie, aktualizację i zapewnienie odpowiedniego stosowania polityki bezpieczeństwa w odniesieniu do systemu SFC2014.

2. Państwa członkowskie i instytucje europejskie inne niż Komisja, które otrzymały prawa dostępu do systemu SFC2014, przestrzegają zasad i warunków bezpieczeństwa IT opublikowanych na portalu SFC2014 oraz środków, jakie Komisja wdrożyła w systemie SFC2014 w celu zabezpieczenia przekazywania danych, w szczególności zasad dotyczących wykorzystywania interfejsu technicznego, o którym mowa w art. 5 ust. 1 niniejszego rozporządzenia.

3. Państwa członkowskie i Komisja wprowadzają w życie i zapewniają skuteczne stosowanie środków bezpieczeństwa przyjętych w celu ochrony danych, które przechowują i przekazują w systemie SFC2014.

4. Państwa członkowskie przyjmują krajowe, regionalne lub lokalne polityki bezpieczeństwa informacji, obejmujące kwestie dostępu do systemu SFC2014 i automatycznego wprowadzania do niego danych, zapewniając zestaw minimalnych wymogów w zakresie bezpieczeństwa. Te krajowe, regionalne lub lokalne polityki bezpieczeństwa IT mogą zawierać odniesienia do innych dokumentów dotyczących bezpieczeństwa. Każde państwo członkowskie zapewnia, aby wspomniane polityki bezpieczeństwa IT miały zastosowanie do wszystkich instytucji korzystających z systemu SFC2014.

5. Wspomniane krajowe, regionalne lub lokalne polityki bezpieczeństwa IT obejmują:

- a) aspekty bezpieczeństwa IT w pracy osoby lub osób odpowiedzialnych za zarządzanie prawami dostępu, o których mowa w art. 3 ust. 3 niniejszego rozporządzenia, w przypadku aplikacji stosowanych bezpośrednio;
- b) w przypadku krajowych, regionalnych lub lokalnych systemów komputerowych podłączonych do systemu SFC2014 za pomocą interfejsu technicznego, o którym mowa w art. 5 ust. 1 niniejszego rozporządzenia — środki bezpieczeństwa umożliwiające tym systemom dostosowanie się do wymogów bezpieczeństwa systemu SFC2014.

Do celów akapitu pierwszego lit. b) uwzględnia się odpowiednio następujące aspekty:

- a) bezpieczeństwo fizyczne;
- b) kontrolę nośników danych i dostępu;
- c) kontrolę przechowywania danych;
- d) kontrolę dostępu i haseł;
- e) monitorowanie;
- f) połączenie z systemem SFC2014;

(1) Decyzja Komisji C(2006) 3602 z dnia 16 sierpnia 2006 r. dotycząca bezpieczeństwa systemów informacyjnych wykorzystywanych przez Komisję Europejską.

- g) infrastrukturę łączności;
  - h) zarządzanie zasobami ludzkimi przed zatrudnieniem, w jego trakcie i po jego zakończeniu;
  - i) zarządzanie zdarzeniami.
6. Krajowe, regionalne lub lokalne polityki bezpieczeństwa IT opierają się na analizie ryzyka, a wyszczególnione środki są proporcjonalne do zidentyfikowanych zagrożeń.
7. Dokumenty, w których określono krajowe, regionalne lub lokalne polityki bezpieczeństwa IT, udostępniane są Komisji na jej wniosek.
8. Państwa członkowskie wyznaczają — na poziomie krajowym — osobę lub osoby odpowiedzialne za utrzymanie i zapewnianie stosowania krajowych, regionalnych lub lokalnych polityk bezpieczeństwa IT. Ta osoba lub te osoby pełnią funkcję punktu kontaktowego dla osoby lub osób wyznaczonych przez Komisję, o których mowa w art. 6 ust. 1 niniejszego rozporządzenia.
9. Zarówno polityki bezpieczeństwa IT dla SFC, jak i odnośne krajowe, regionalne i lokalne polityki bezpieczeństwa IT uaktualniane są w przypadku zmian technologicznych, identyfikacji nowych zagrożeń lub innych istotnych zmian. Niezależnie od tego są one poddawane co roku przeglądowi, aby zapewnić, że nadal są odpowiednim środkiem.

## ROZDZIAŁ II

### PRZEPISY KOŃCOWE

#### Artykuł 7

Niniejsze rozporządzenie wchodzi w życie następnego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 5 maja 2014 r.

W imieniu Komisji  
José Manuel BARROSO  
Przewodniczący