►B REGULAMENTUL (UE) 2019/818 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 20 mai 2019

privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE în domeniul cooperării polițienești și judiciare, al azilului și al migrației și de modificare a Regulamentelor (UE) 2018/1726, (UE) 2018/1862 și (UE) 2019/816

(JO L 135, 22.5.2019, p. 85)

Astfel cum a fost modificat prin:

		Jurnalul Oficial		
		NR.	Pagina	Data
►M1	Regulamentul (UE) 2021/1133 al Parlamentului European și al Consiliului din 7 iulie 2021	L 248	1	13.7.2021
►M2	Regulamentul (UE) 2021/1150 al Parlamentului European și al Consiliului din 7 iulie 2021	L 249	1	14.7.2021
►M3	Regulamentul (UE) 2021/1151 al Parlamentului European și al Consiliului din 7 iulie 2021	L 249	7	14.7.2021
►M4	Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024	L 982	1	5.4.2024

rectificat prin:

►C1 Rectificare, JO L 10, 15.1.2020, p. 5 (2019/818)

►C2 Rectificare, JO L 335, 29.12.2022, p. 112 (2019/818)

►C3 Rectificare, JO L 90189, 15.3.2024, p. 1 (2019/818)

▼B

REGULAMENTUL (UE) 2019/818 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 20 mai 2019

privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informaţii ale UE în domeniul cooperării poliţieneşti şi judiciare, al azilului şi al migraţiei şi de modificare a Regulamentelor (UE) 2018/1726, (UE) 2018/1862 şi (UE) 2019/816

CAPITOLUL I

Dispoziţii generale

Articolul 1

Obiect

(1) Prezentul regulament, împreună cu Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului [1], stabilește un cadru pentru a asigura interoperabilitatea dintre Sistemul de intrare/ieșire (EES), Sistemul de informaţii privind vizele (VIS), Sistemul european de informaţii și de autorizare privind călătoriile (ETIAS), Eurodac, Sistemul de informaţii Schengen (SIS) și Sistemul european de informaţii cu privire la cazierele judiciare ale resortisanţilor ţărilor terţe (ECRIS-TCN).

(2) Cadrul include următoarele componente de interoperabilitate:

(a) un portal european de căutare (ESP);

(b) un serviciu comun de comparare a datelor biometrice (BMS comun);

(c) un registru comun de date de identitate (CIR);

(d) un detector de identităţi multiple (MID).

(3) Prezentul regulament cuprinde, de asemenea, dispoziţii privind cerinţele de calitate a datelor, formatul universal pentru mesaje (UMF), registrul central de raportare și statistici (CRRS) și responsabilităţile statelor membre și ale Agenţiei Europene pentru Gestionarea Operaţională a Sistemelor Informatice la Scară Largă în Spaţiul de Libertate, Securitate și Justiţie (eu-LISA) în ceea ce privește conceperea, dezvoltarea și funcţionarea componentelor de interoperabilitate.

(4) Prezentul regulament adaptează totodată procedurile și condiţiile în care autorităţile desemnate și Agenţia Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) au acces la EES, VIS, ETIAS și Eurodac în scopul prevenirii, depistării sau investigării infracţiunilor de terorism sau a altor infracţiuni grave.

[1] Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informaţii ale UE în domeniul frontierelor și al vizelor și de modificare a Regulamentelor (CE) nr. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 și (UE) 2018/1861 ale Parlamentului European și ale Consiliului și a Deciziilor 2004/512/CE și 2008/633/JAI ale Consiliului (a se vedea pagina 27 din prezentul Jurnal Oficial).

▼B

(5) Prezentul regulament stabilește, de asemenea, un cadru pentru verificarea identității persoanelor și pentru identificarea persoanelor.

Articolul 2

Obiective

(1) Prin asigurarea interoperabilității, prezentul regulament are următoarele obiective:

(a) îmbunătățirea eficacității și a eficienței verificărilor la frontierele externe;

(b) contribuirea la prevenirea și combaterea imigrației ilegale;

(c) contribuirea la asigurarea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție al Uniunii, inclusiv menținerea siguranței publice și a ordinii publice și la garantarea securității pe teritoriul statelor membre;

(d) îmbunătățirea punerii în aplicare a politicii comune în materie de vize;

(e) facilitarea examinării cererilor de protecție internațională;

(f) contribuirea la prevenirea, depistarea și investigarea infracțiunilor de terorism sau a altor infracțiuni grave;

(g) facilitarea identificării persoanelor necunoscute care nu pot să se legitimeze sau a rămășițelor umane neidentificate în caz de dezastre naturale, accidente sau atacuri teroriste.

(2) Obiectivele menționate la alineatul (1) sunt realizate prin:

(a) asigurarea identificării corecte a persoanelor;

(b) contribuirea la combaterea fraudelor de identitate;

(c) îmbunătățirea calității datelor și armonizarea cerințelor în materie de calitate a datelor stocate în sistemele de informații ale UE, respectând totodată cerințele privind prelucrarea datelor prevăzute de instrumentele juridice care reglementează sistemele individuale, precum și standardele și principiile în materie de protecție a datelor;

(d) facilitarea și sprijinirea implementării tehnice și operaționale de către statele membre a sistemelor de informații ale UE;

(e) consolidarea și simplificarea condițiilor privind securitatea și protecția datelor care guvernează respectivele sisteme de informații ale UE, precum și sporirea uniformității acestor condiții, fără a afecta protecția și garanțiile speciale de care beneficiază anumite categorii de date;

▼B

(f) raţionalizarea condiţiilor de acces al autorităţilor desemnate la EES, VIS, ETIAS și Eurodac, asigurând totodată condiţii necesare și proporţionale pentru acest acces;

(g) sprijinirea realizării scopurilor pentru care au fost instituite EES, VIS, ETIAS, Eurodac, SIS și ECRIS-TCN.

Articolul 3

Domeniul de aplicare

(1) Prezentul regulament se aplică Eurodac, SIS și ECRIS-TCN.

(2) Prezentul regulament se aplică, de asemenea, datelor Europol, în măsura necesară permiterii unei interogări simultane a acestora și a sistemelor de informaţii ale UE menţionate la alineatul (1).

(3) Prezentul regulament se aplică persoanelor ale căror date cu caracter personal pot fi prelucrate în sistemele de informaţii ale UE la care se face referire la alineatul (1) și în datele Europol la care se face referire la alineatul (2).

Articolul 4

Definiţii

În sensul prezentului regulament:

1. „frontiere externe” înseamnă frontierele externe, astfel cum sunt definite la articolul 2 punctul 2 din Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului ([2]);

2. „verificări la frontiere” înseamnă verificările la frontiere, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (UE) 2016/399;

3. „autoritate de frontieră” înseamnă poliţistul de frontieră desemnat în conformitate cu dreptul intern să efectueze verificări la frontiere;

4. „autorităţi de supraveghere” înseamnă autoritatea de supraveghere menţionată la articolul 51 alineatul (1) din Regulamentul (UE) 2016/679 și autoritatea de supraveghere menţionată la articolul 41 alineatul (1) din Directiva (UE) 2016/680;

5. „verificare” înseamnă procesul de comparare a unor serii de date în vederea stabilirii autenticităţii unei identităţi declarate (controlul realizat prin compararea a două serii de date);

6. „identificare” înseamnă procesul de determinare a identităţii unei persoane prin efectuarea unei căutări într-o bază de date după mai multe serii de date (controlul realizat prin compararea mai multor serii de date);

([2]) Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2016 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen) (JO L 77, 23.3.2016, p. 1).

▼B

7. „date alfanumerice” înseamnă date constând în litere, cifre, caractere speciale, spaţii și semne de punctuaţie;

▼C1

8. „date de identitate” înseamnă datele prevăzute la articolul 27 alineatul (3) literele (a) și (b);

▼B

9. „date dactiloscopice” înseamnă imagini de amprente digitale și imagini de amprente digitale latente care, datorită unicităţii lor și punctelor de referinţă pe care le conţin, permit comparaţii fiabile și concludente referitoare la identitatea unei persoane;

10. „imagine facială” înseamnă imagini digitale ale feţei;

11. „date biometrice” înseamnă datele dactiloscopice sau imaginea facială sau ambele;

12. „șablon biometric” înseamnă o reprezentare matematică obţinută prin extragerea de caracteristici din datele biometrice limitată la parametrii necesari pentru efectuarea de identificări și verificări;

13. „document de călătorie” înseamnă pașaportul sau un alt document echivalent care îi dă titularului dreptul de trecere a frontierelor externe și pe care se poate aplica o viză;

14. „date din documentul de călătorie” înseamnă tipul și numărul documentului de călătorie, ţara care l-a eliberat, data expirării perioadei de valabilitate a documentului de călătorie și codul din trei litere al ţării care a eliberat documentul de călătorie;

15. „sisteme de informaţii ale UE” înseamnă sistemele EES, VIS, ETIAS, Eurodac, SIS și ECRIS-TCN;

16. „date Europol” înseamnă datele cu caracter personal prelucrate de Europol în scopurile menţionate la articolul 18 alineatul (2) literele (a), (b) și (c) din Regulamentul (UE) 2016/794;

17. „baze de date ale Interpol” înseamnă baza de date a Interpol privind documentele de călătorie furate și pierdute (baza de date SLTD) și baza de date a Interpol privind documentele de călătorie asociate unor notiţe (baza de date TDAWN);

18. „concordanţă” înseamnă existenţa unei corespondenţe care reiese din compararea automatizată a unor date cu caracter personal care sunt înregistrate sau sunt în curs de a fi înregistrate într-un sistem de informaţii sau într-o bază de date;

19. „autoritate poliţienească” înseamnă „autoritate competentă”, astfel cum este definită la articolul 3 punctul 7 din Directiva (UE) 2016/680;

▼M1

20. „autorități desemnate” înseamnă autoritățile desemnate de statele membre, astfel cum sunt definite la articolul 4 punctul 3a din Regulamentul (CE) nr. 767/2008, la articolul 3 alineatul (1) punctul 26 din Regulamentul (UE) 2017/2226 și la articolul 3 alineatul (1) punctul 21 din Regulamentul (UE) 2018/1240;

▼B

21. „infracțiune de terorism” înseamnă o infracțiune prevăzută în dreptul intern care corespunde unei infracțiuni menționate în Directiva (UE) 2017/541 a Parlamentului European și a Consiliului ([3]) sau este echivalentă cu una dintre acestea;

22. „infracțiune gravă” corespunde unei infracțiuni prevăzute la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI a Consiliului ([4]) sau care este echivalentă cu una dintre acestea, dacă este pasibilă de pedeapsă cu închisoarea sau cu o măsură de siguranță privativă de libertate pe o perioadă maximă de cel puțin trei ani în temeiul dreptului intern;

23. „Sistemul de intrare/ieșire” sau „EES” înseamnă Sistemul de intrare/ieșire, instituit de Regulamentul (UE) 2017/2226;

24. „Sistemul de informații privind vizele” („VIS”) înseamnă Sistemul de informații privind vizele, instituit de Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului ([5]);

25. „Sistemul european de informații și de autorizare privind călătoriile” („ETIAS”) înseamnă Sistemul european de informații și de autorizare privind călătoriile, instituit de Regulamentul (UE) 2018/1240;

26. „Eurodac” înseamnă Eurodac, instituit de Regulamentul (UE) nr. 603/2013 al Parlamentului European și al Consiliului ([6]);

27. „Sistemul de informații Schengen” („SIS”) înseamnă Sistemul de informații Schengen, instituit de Regulamentele (UE) 2018/1860, (UE) 2018/1861 și (UE) 2018/1862;

28. „ECRIS-TCN” înseamnă sistemul centralizat de identificare a statelor membre în care există informații privind condamnările resortisanților țărilor terțe și ale apatrizilor, instituit de Regulamentul (UE) 2019/816.

([3]) Directiva (UE) 2017/541 a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO L 88, 31.3.2017, p. 6).

([4]) Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO L 190, 18.7.2002, p. 1).

([5]) Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS) (JO L 218, 13.8.2008, p. 60).

([6]) Regulamentul (UE) nr. 603/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid și privind cererile autorităților de aplicare a legii din statele membre și a Europol de comparare a datelor Eurodac în scopul asigurării respectării aplicării legii și de modificare a Regulamentului (UE) nr. 1077/2011 de instituire a Agenției europene pentru gestionarea operațională a sistemelor informatice la scară largă, în spațiul de libertate, securitate și justiție (JO L 180, 29.6.2013, p. 1).

▼B

Articolul 5

Nediscriminarea și drepturile fundamentale

Prelucrarea datelor cu caracter personal în sensul prezentului regulament nu poate să conducă la discriminarea persoanelor pe motive de gen, rasă, culoare, origine etnică sau socială, caracteristici genetice, limbă, religie sau convingeri, opinii politice sau de orice altă natură, apartenenţă la o minoritate naţională, situaţie materială, statut la naștere, handicap, vârstă sau orientare sexuală. Pe parcursul prelucrării datelor cu caracter personal se respectă pe deplin demnitatea și integritatea umană, precum și drepturile fundamentale, inclusiv dreptul la respectarea vieţii private și la protecţia datelor cu caracter personal. Se acordă o atenţie specială copiilor, persoanelor în vârstă, persoanelor cu handicap și persoanelor care au nevoie de protecţie internaţională. Interesul superior al copilului este considerat primordial.

CAPITOLUL II

Portalul european de căutare

Articolul 6

Portalul european de căutare

(1) Se instituie un portal european de căutare (ESP) cu scopul de a facilita accesul rapid, neîntrerupt, eficient, sistematic și controlat al autorităţilor statelor membre și al agenţiilor Uniunii la sistemele de informaţii ale UE, la datele Europol și la bazele de date ale Interpol pentru îndeplinirea sarcinilor care le revin și în conformitate cu drepturile de acces de care beneficiază și cu obiectivele și scopurile EES, VIS, ETIAS, Eurodac, SIS și ECRIS-TCN.

(2) ESP este alcătuit din următoarele componente:

(a) o infrastructură centrală, care include un portal de căutare ce permite lansarea de interogări simultane în EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN, precum și în datele Europol și în bazele de date ale Interpol;

(b) un canal securizat de comunicaţii între ESP, statele membre și agenţiile Uniunii care au dreptul să utilizeze ESP;

(c) o infrastructură de comunicaţii securizată între ESP și EES, VIS, ETIAS, Eurodac, SIS central, ECRIS-TCN, datele Europol și bazele de date ale Interpol, precum și între ESP și infrastructurile centrale ale CIR și ale MID;

▼M4

(d) o infrastructură de comunicaţii securizată între ESP și routerul instituit prin Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului ([7]).

([7]) Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul automatizat de date în scopul cooperării poliţieneşti, și de modificare a Deciziilor 2008/615/JAI și 2008/616/JAI ale Consiliului și a Regulamentelor (UE) 2018/1726, (UE) 2019/817 și (UE) 2019/818 ale Parlamentului European și ale Consiliului (Regulamentul Prüm II) (JO L, 2024/982, 5.4.2024, ELI: http://data.europa.eu/eli/reg/2024/982/oj).

▼B

(3) eu-LISA dezvoltă ESP și asigură gestionarea tehnică a acestuia.

Articolul 7

Utilizarea portalului european de căutare

(1) Utilizarea ESP este rezervată autorităţilor statelor membre și agenţiilor Uniunii care au acces la cel puţin unul dintre sistemele de informaţii ale UE, în conformitate cu instrumentele juridice care reglementează aceste sisteme de informaţii ale UE, la CIR și la MID, în conformitate cu prezentul regulament, la datele Europol, în conformitate cu Regulamentul (UE) 2016/794, sau la bazele de date ale Interpol, în conformitate cu dreptul Uniunii sau cu dreptul intern care reglementează un astfel de acces.

Respectivele autorităţi ale statelor membre și agenţii ale Uniunii pot utiliza ESP și datele furnizate de acesta exclusiv pentru obiectivele și scopurile prevăzute de instrumentele juridice care reglementează respectivele sisteme de informaţii ale UE, de Regulamentul (UE) 2016/794 și de prezentul regulament.

(2) Autorităţile statelor membre și agenţiile Uniunii menţionate la alineatul (1) utilizează ESP pentru a căuta date referitoare la persoane sau la documentele de călătorie ale acestora în sistemele centrale ale Eurodac și ECRIS-TCN, în conformitate cu drepturile de acces de care beneficiază în temeiul instrumentelor juridice care reglementează aceste sisteme de informaţii ale UE și în temeiul dreptului intern.. De asemenea, acestea utilizează ESP pentru a lansa interogări în CIR în conformitate cu drepturile de acces de care beneficiază în temeiul prezentului regulament, în scopurile menţionate la articolele 20, 21 și 22.

▼C2

(3) Autorităţile statelor membre menţionate la alineatul (1) pot utiliza ESP pentru a căuta date referitoare la persoane sau la documentele de călătorie ale acestora în SIS central menţionat în Regulamentul (UE) 2018/1862.

▼B

(4) Atunci când dreptul Uniunii prevede acest lucru, agenţiile Uniunii menţionate la alineatul (1) utilizează ESP pentru a căuta date referitoare la persoane sau la documentele de călătorie ale acestora în SIS central.

(5) Autorităţile statelor membre și agenţiile Uniunii menţionate la alineatul (1) pot utiliza ESP pentru a căuta date referitoare la persoane sau la documentele de călătorie ale acestora în datele Europol, în conformitate cu drepturile de acces de care beneficiază în temeiul dreptului intern și al Uniunii.

Articolul 8

Profiluri pentru utilizatorii portalului european de căutare

(1) Pentru a facilita utilizarea ESP, în cooperare cu statele membre, eu-LISA creează un profil bazat pe fiecare categorie de utilizator ESP și pe scopul interogărilor, în conformitate cu detaliile tehnice și cu drepturile de acces menţionate la alineatul (2). Fiecare profil cuprinde, în conformitate cu dreptul Uniunii și dreptul intern următoarele informaţii:

(a) câmpurile de date ce urmează a fi utilizate pentru lansarea interogărilor;

▼B

(b) sistemele de informaţii ale UE, date Europol și bazele de date ale Interpol care urmează să fie interogate, cele care pot fi interogate și cele care urmează să furnizeze un răspuns utilizatorului;

(c) datele specifice din sistemele de informaţii ale UE, date Europol și bazele de date ale Interpol care pot fi interogate;

(d) categoriile de date care pot fi furnizate în fiecare răspuns.

(2) Comisia adoptă acte de punere în aplicare pentru a specifica detaliile tehnice ale profilurilor menţionate la alineatul (1), în conformitate cu drepturile de acces ale utilizatorilor ESP în temeiul instrumentelor juridice care reglementează sistemele de informaţii ale UE și în temeiul dreptului intern. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 70 alineatul (2).

(3) Profilurile menţionate la alineatul (1) sunt revizuite cu regularitate de către eu-LISA în cooperare cu statele membre, cel puţin o dată pe an, și, dacă este necesar, sunt actualizate.

Articolul 9

Interogări

(1) Utilizatorii ESP lansează o interogare prin transmiterea de date alfanumerice sau biometrice către ESP. În cazul în care a fost lansată o interogare, ESP va interoga EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN și CIR, datele Europol și bazele de date ale Interpol, simultan, folosind datele transmise de utilizatorul ESP și în funcţie de profilul de utilizator.

(2) Categoriile de date folosite pentru a lansa o interogare prin intermediul ESP corespund categoriilor de date referitoare la persoane sau documente de călătorie care pot fi utilizate pentru a interoga diferitele sisteme de informaţii ale UE, datele Europol și bazele de date ale Interpol în conformitate cu instrumentele juridice care le reglementează.

(3) În cooperare cu statele membre, eu-LISA implementează pentru ESP un document de control al interfeţei pe baza UMF menţionat la articolul 38.

(4) Atunci când un utilizator ESP lansează o interogare, EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, CIR și MID, datele Europol și bazele de date ale Interpol furnizează în răspunsul la interogare datele pe care le conţin.

Fără a aduce atingere articolului 20, răspunsul furnizat de ESP indică sistemul de informaţii al UE sau baza de date de unde provin datele.

ESP nu furnizează nicio informaţie referitoare la datele din sistemele de informaţii ale UE, datele Europol și bazele de date ale Interpol la care utilizatorul nu are acces în temeiul dreptului Uniunii și al dreptului intern aplicabil.

▼B

(5) Toate interogările în bazele de date ale Interpol lansate prin intermediul ESP se efectuează în așa mod încât nicio informație să nu fie dezvăluită proprietarului semnalării Interpol.

(6) ESP furnizează răspunsuri utilizatorului de îndată ce sunt disponibile date din unul dintre sistemele de informații ale UE, din datele Europol și din bazele de date ale Interpol. Răspunsurile respective conțin numai informațiile la care acesta are acces în temeiul dreptului Uniunii și al dreptului intern.

(7) Comisia adoptă un act de punere în aplicare pentru a preciza procedura tehnică pentru interogarea de către ESP a sistemelor de informații ale UE, a datelor Europol și a bazelor de date ale Interpol și formatul răspunsurilor ESP. Actul respectiv de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 70 alineatul (2).

Articolul 10

Păstrarea înregistrărilor

(1) Fără a aduce atingere articolelor 12 și 18 din Regulamentul (UE) 2018/1862, articolului 29 din Regulamentul (UE) 2019/816 și articolului 40 din Regulamentul (UE) 2016/794, eu-LISA păstrează înregistrări ale tuturor operațiunilor de prelucrare a datelor din cadrul ESP. În aceste înregistrări sunt incluse următoarele informații:

(a) statul membru sau agenția Uniunii care lansează interogarea și profilul ESP utilizat;

(b) data și ora efectuării interogării;

(c) sistemele de informații ale UE și datele Europol care au fost interogate;

(2) Fiecare stat membru păstrează înregistrări ale interogărilor efectuate de autoritățile sale și de personalul acestora autorizat în mod corespunzător să utilizeze ESP. Fiecare agenție a Uniunii păstrează înregistrări ale interogărilor efectuate de personalul său autorizat în mod corespunzător.

(3) Înregistrările menționate la alineatele (1) și (2) pot fi folosite numai pentru a se monitoriza protecția datelor, inclusiv pentru a se verifica admisibilitatea unei interogări și legalitatea prelucrării datelor, precum și pentru a se asigura securitatea și integritatea datelor. Aceste înregistrări sunt protejate prin măsuri corespunzătoare împotriva accesului neautorizat și sunt șterse după o perioadă de un an de la data la care au fost create. Dacă, cu toate acestea, înregistrările sunt necesare pentru desfășurarea unor proceduri de monitorizare aflate în curs, acestea se șterg odată ce nu mai este nevoie de aceste înregistrări pentru procedurile de monitorizare.

Articolul 11

Proceduri alternative în cazul imposibilității tehnice de a utiliza portalul european de căutare

(1) În cazul în care, din cauza unei disfuncționalități a ESP, este imposibil din punct de vedere tehnic să se utilizeze ESP pentru a lansa o interogare în unul sau mai multe dintre sistemele de informații ale UE sau în CIR, utilizatorii ESP primesc în mod automat o notificare în acest sens din partea eu-LISA.

▼B

(2) În cazul în care, din cauza unei disfuncţionalităţi a infrastructurii naţionale dintr-un stat membru, este imposibil din punct de vedere tehnic să se utilizeze ESP pentru a lansa o interogare în unul sau mai multe dintre sistemele de informaţii ale UE sau în CIR, statul membru respectiv notifică eu-LISA și Comisia în mod automat.

(3) În cazurile menţionate la alineatele (1) și (2) din prezentul articol și până la remedierea problemei tehnice, obligaţia menţionată la articolul 7 alineatele (2) și (4) nu se aplică, iar statele membre au acces la sistemele de informaţii ale UE sau direct la CIR atunci când acest lucru este impus în temeiul dreptului Uniunii sau dreptului intern.

(4) În cazul în care, din cauza unei disfuncţionalităţi a infrastructurii unei agenţii a Uniunii, este imposibil din punct de vedere tehnic să se utilizeze ESP pentru a lansa o interogare într-unul sau mai multe dintre sistemele de informaţii ale Uniunii sau în CIR, agenţia respectivă notifică eu-LISA și Comisia în mod automat.

CAPITOLUL III

Serviciul comun de comparare a datelor biometrice

Articolul 12

Serviciul comun de comparare a datelor biometrice

(1) Pentru a sprijini CIR și MID și obiectivele EES, VIS, Eurodac, SIS și ECRIS-TCN, se instituie un serviciu comun de comparare a datelor biometrice (BMS comun), care stochează șabloane biometrice obţinute pe baza datelor biometrice menţionate la articolul 13 care sunt stocate în CIR și în SIS și permite efectuarea de interogări folosind date biometrice în mai multe sisteme de informaţii ale UE.

(2). BMS comun este alcătuit din următoarele componente:

(a) o infrastructură centrală, care înlocuiește sistemele centrale ale EES, VIS, SIS, Eurodac și, respectiv, ECRIS-TCN, în măsura în care aceasta stochează șabloane biometrice și permite efectuarea de căutări cu ajutorul datelor biometrice;

(b) o infrastructură de comunicaţii securizată între BMS comun, SIS central și CIR.

(3) eu-LISA dezvoltă BMS comun și asigură gestionarea tehnică a acestuia.

Articolul 13

Stocarea șabloanelor biometrice în serviciul comun de comparare a datelor biometrice

(1) În BMS comun se stochează șabloane biometrice pe care acesta le obţine din următoarele date biometrice:

(a) datele menţionate la articolul 20 alineatul (3) literele (w) și (y) din Regulamentul (UE) 2018/1862, cu excepţia datelor privind amprentele palmare;

▼C3

(b) datele menţionate la articolul 5 alineatul (1) litera (b) și alineatul (3) din Regulamentul (UE) 2019/816.

▼B

Șabloanele biometrice se stochează în BMS comun într-o formă separată în mod logic în funcţie de sistemul de informaţii din care provin datele.

(2) Pentru fiecare set de date menţionate la alineatul (1), BMS comun include în fiecare șablon biometric o trimitere la sistemele de informaţii ale UE în care sunt stocate datele biometrice corespondente și o trimitere la înregistrările efective din sistemele de informaţii ale UE.

(3) Șabloanele biometrice se introduc în BMS comun numai în urma unei verificări automatizate a calităţii datelor biometrice adăugate într-unul din sistemele de informaţii ale UE, efectuate de BMS comun pentru a se asigura îndeplinirea unui standard minim de calitate a datelor.

(4) Stocarea datelor menţionate la alineatul (1) respectă standardele de calitate prevăzute la articolul 37 alineatul (2).

(5) Prin intermediul unui act de punere în aplicare, Comisia stabilește cerinţele de performanţă pentru BMS comun și modalităţile practice de monitorizare a performanţei acestuia, pentru a se asigura că eficacitatea căutărilor biometrice respectă procedurile urgente, cum ar fi verificările la frontiere și identificările. Respectivul act de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 70 alineatul (2).

Articolul 14

Căutarea de date biometrice prin intermediul serviciului comun de comparare a datelor biometrice

Pentru a căuta date biometrice stocate în CIR și SIS, CIR și SIS utilizează șabloanele biometrice stocate în BMS comun. Interogările efectuate folosind date biometrice se lansează în conformitate cu scopurile prevăzute în prezentul regulament și în Regulamentele (CE) nr. 767/2008, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2018/1862 și (UE) 2019/816.

Articolul 15

Păstrarea datelor în serviciul comun de comparare a datelor biometrice

Datele menţionate la articolul 13 alineatele (1) și (2) sunt stocate în BMS comun numai atât timp cât sunt stocate în CIR sau SIS datele biometrice corespondente. Datele respective se șterg din BMS comun într-un mod automatizat.

▼B

Articolul 16

Păstrarea înregistrărilor

(1) Fără a aduce atingere articolelor 12 și 18 din Regulamentul (UE) 2018/1862 și articolului 29 din Regulamentul (UE) 2019/816, eu-LISA păstrează înregistrări ale tuturor operațiunilor de prelucrare a datelor din cadrul BMS comun. În aceste înregistrări sunt incluse următoarele informații:

(a) statul membru sau agenția Uniunii care lansează interogarea;

(b) istoricul creării și stocării șabloanelor biometrice;

(c) sistemele de informații ale UE în care s-au efectuat interogările folosind șabloanele biometrice stocate în BMS comun;

(d) data și ora efectuării interogării;

(e) tipul de date biometrice utilizate pentru lansarea interogării;

(f) rezultatele interogării și data și ora obținerii rezultatului.

(2) Fiecare stat membru păstrează înregistrări ale interogărilor efectuate de autoritățile sale și de personalul acestora autorizat în mod corespunzător să utilizeze BMS comun. Fiecare agenție a Uniunii păstrează înregistrări ale înregistrărilor efectuate de personalul său autorizat în mod corespunzător.

(3) Înregistrările menționate la alineatele (1) și (2) pot fi folosite numai pentru a se monitoriza protecția datelor, inclusiv pentru a se verifica admisibilitatea unei interogări și legalitatea prelucrării datelor, precum și pentru a se asigura securitatea și integritatea datelor. Aceste înregistrări sunt protejate prin măsuri corespunzătoare împotriva accesului neautorizat și sunt șterse după o perioadă de un an de la data la care au fost create. Totuși, dacă înregistrările sunt necesare pentru desfășurarea unor proceduri de monitorizare aflate în curs, acestea se șterg odată ce nu mai este nevoie de aceste înregistrări pentru procedurile de monitorizare.

CAPITOLUL IV

Registrul comun de date de identitate

Articolul 17

Registrul comun de date de identitate

(1) Se instituie un registru comun de date de identitate (CIR), în care se creează un dosar individual pentru fiecare persoană care este înregistrată în EES, VIS, ETIAS, Eurodac sau ECRIS-TCN, ce conține datele menționate la articolul 18, în scopul de a facilita și a asista procesul de identificare corectă a persoanelor înregistrate în EES, VIS, ETIAS, Eurodac și [ECRIS-TCN], în conformitate cu articolul 20, de a sprijini funcționarea MID, în conformitate cu articolul 21, și de a facilita și simplifica accesul autorităților desemnate și al Europol la EES, VIS, ETIAS și Eurodac, atunci când acest lucru este necesar pentru prevenirea, depistarea sau investigarea infracțiunilor de terorism sau a altor infracțiuni grave în conformitate cu articolul 22.

▼B

(2) CIR este alcătuit din următoarele componente:

(a) o infrastructură centrală care înlocuiește sistemele centrale ale EES, VIS, ETIAS, Eurodac și, respectiv, ECRIS-TCN, în măsura în care aceasta stochează datele menţionate la articolul 18;

(b) un canal securizat de comunicaţii între CIR, statele membre și agenţiile Uniunii care au dreptul să utilizeze CIR în conformitate cu dreptul Uniunii și cu dreptul intern;

(c) o infrastructură de comunicaţii securizată între CIR și EES, VIS, ETIAS, Eurodac și ECRIS-TCN, precum și cu infrastructurile centrale ale ESP, BMS comun și MID.

(3) eu-LISA dezvoltă CIR și asigură gestionarea tehnică a acestuia.

(4) În cazul în care, din cauza unei disfuncţionalităţi a CIR, este imposibil din punct de vedere tehnic să se interogheze CIR în scopul identificării unei persoane în temeiul articolului 20, al detectării unor identităţi multiple în temeiul articolului 21 sau al prevenirii, depistării ori investigării infracţiunilor de terorism sau a altor infracţiuni grave în temeiul articolului 22, utilizatorii CIR sunt notificaţi în mod automat de către eu-LISA.

(5) În cooperare cu statele membre, eu-LISA implementează pentru CIR un document de control al interfeţei pe baza UMF menţionat la articolul 38.

Articolul 18

Datele din registrul comun de date de identitate

▼C3

(1) CIR stochează următoarele date, separate în mod logic în funcţie de sistemul de informaţii din care provin: datele menţionate la articolul 5 alineatul (1) litera (b) și alineatul (3) din Regulamentul (UE) 2019/816, precum și următoarele date enumerate la articolul 5 alineatul (1) litera (a) din regulamentul respectiv: numele (de familie), prenumele, data naşterii, locul naşterii (localitatea și ţara), cetăţenia sau cetăţeniile, genul, numele anterioare, dacă este cazul, pseudonimele sau numele de împrumut, dacă sunt disponibile, precum și, dacă sunt disponibile, informaţiile privind documentele de călătorie.

▼M1

(1a) În scopul articolelor 9a și 22b din Regulamentul (CE) nr. 767/2008, CIR stochează, de asemenea, separate în mod logic de datele menţionate la alineatul (1) din prezentul articol, datele menţionate la articolul 5 alineatul (1) litera (c) din Regulamentul (UE) 2019/816. Datele menţionate la articolul 5 alineatul (1) litera (c) din Regulamentul (UE) 2019/816 sunt accesibile numai în modul menţionat la articolul 5 alineatul (7) din regulamentul respectiv.

▼M3

(1b) În scopul articolului 20 din Regulamentul (UE) 2018/1240, CIR stochează, de asemenea, într-o formă separată în mod logic de datele menţionate la alineatul (1) din prezentul articol, datele menţionate la articolul 5 alineatul (1) litera (c) din Regulamentul (UE) 2019/816. Datele menţionate la articolul 5 alineatul (1) litera (c) din Regulamentul (UE) 2019/816 sunt accesibile exclusiv în modul menţionat la articolul 5 alineatul (7) din respectivul regulament.

▼B

(2) Pentru fiecare set de date menţionate la alineatul (1), CIR include o trimitere la sistemele de informaţii ale UE din care provin datele.

(3) Autorităţile care accesează CIR fac acest lucru în conformitate cu drepturile de acces de care beneficiază în temeiul instrumentelor juridice care reglementează sistemele de informaţii ale UE și în temeiul dreptului intern și în conformitate cu drepturile de acces de care beneficiază în temeiul prezentului regulament în scopurile menţionate la articolele 20, 21 și 22.

(4) Pentru fiecare set de date menţionate la alineatul (1), CIR include o trimitere la înregistrarea efectivă în sistemele de informaţii ale UE din care provin datele.

(5) Stocarea datelor menţionate la alineatul (1) respectă standardele de calitate prevăzute la articolul 37 alineatul (2).

Articolul 19

Adăugarea, modificarea și ștergerea datelor din registrul comun de date de identitate

(1) În cazul în care se adaugă, se modifică sau se elimină date din Eurodac sau ECRIS-TCN, datele menţionate la articolul 18 stocate în dosarul individual din CIR se adăugă, se modifică sau se elimină în mod automat.

(2) În cazul în care se creează o conexiune albă sau roșie în MID, în conformitate cu articolul 32 sau 33, între datele provenite din două sau mai multe dintre sistemele de informaţii ale UE care alcătuiesc CIR, în loc să se creeze un nou dosar individual, CIR adaugă datele noi în dosarul individual al datelor conexate.

Articolul 20

Accesul la registrul comun de date de identitate în scopul identificării

(1) Interogările CIR se efectuează de către o autoritate de poliţie, în conformitate cu alineatele (2) și (5), numai în următoarele circumstanţe:

(a) în cazul în care o autoritate de poliţie nu este în măsură să identifice o persoană din cauza lipsei unui document de călătorie sau a unui alt document credibil care să ateste identitatea persoanei respective;

(b) în cazul în care există îndoieli cu privire la datele de identitate furnizate de o persoană;

(c) în cazul în care există îndoieli cu privire la autenticitatea documentului de călătorie sau a unui alt document credibil furnizat de o persoană;

(d) în cazul în care există îndoieli cu privire la identitatea unui titular al unui document de călătorie sau al unui alt document credibil; sau

(e) în cazul în care o persoană nu poate ori refuză să coopereze.

▼B

Astfel de interogări nu sunt permise în cazul minorilor cu vârsta mai mică de 12 ani, cu excepţia cazului în care interogarea este în interesul superior al copilului.

(2) În cazul în care survine una dintre circumstanţele enumerate la alineatul (1) și o autoritate de poliţie are competenţe în acest sens în temeiul unor măsuri legislative naţionale, astfel cum se menţionează la alineatul (5), aceasta poate, exclusiv în scopul identificării unei persoane, să lanseze o interogare în CIR folosind datele biometrice ale persoanei respective, preluate în timp real în cursul unui control de identitate, cu condiţia ca această procedură să fie iniţiată în prezenţa persoanei respective.

(3) În cazul în care, în urma interogării, reiese că în CIR sunt stocate date referitoare la persoana respectivă, autoritatea de poliţie are acces să consulte datele menţionate la articolul 18 alineatul (1).

În cazul în care datele biometrice ale persoanei respective nu pot fi utilizate sau interogarea lansată folosind acele date nu a dat rezultate, se lansează o interogare cu datele de identitate ale persoanei, în combinaţie cu datele din documentul de călătorie sau cu datele de identitate pe care le furnizează persoana respectivă.

(4) În cazul în care o autoritate de poliţie are competenţe în acest sens în temeiul unor măsuri legislative naţionale, astfel cum se prevede la alineatul (6), aceasta poate, în cazul unei catastrofe naturale, al unui accident sau al unui atentat terorist și exclusiv în scopul identificării persoanelor necunoscute care nu sunt în măsură să se legitimeze sau a rămășiţelor umane neidentificate, să lanseze o interogare în CIR folosind datele biometrice ale persoanelor respective.

(5) Statele membre care doresc să facă uz de posibilitatea prevăzută la alineatul (2) adoptă în acest sens măsuri legislative naţionale. Cu această ocazie, statele membre iau în considerare necesitatea de a evita orice discriminare împotriva resortisanţilor ţărilor terţe. Aceste măsuri legislative precizează scopurile precise ale identificării din cele menţionate la articolul 2 alineatul (1) literele (b) și (c). Statele membre desemnează autorităţile de poliţie competente și stabilesc procedurile, condiţiile și criteriile aferente acestor controale.

(6) Statele membre care doresc să facă uz de posibilitatea prevăzută la alineatul (4) adoptă măsuri legislative naţionale de stabilire a procedurilor, condiţiilor și criteriilor.

Articolul 21

Accesul la registrul comun de date de identitate în scopul detectării de identităţi multiple

(1) În cazul în care o interogare în CIR are ca rezultat o conexiune galbenă, în conformitate cu articolul 28 alineatul (4), autoritatea responsabilă de verificarea manuală a identităţilor diferite în conformitate cu articolul 29 are acces, exclusiv în scopul verificării respective, la datele menţionate la articolul 18 alineatele (1) și (2) stocate în CIR conexate printr-o conexiune galbenă.

▼B

(2) În cazul în care o interogare în CIR are ca rezultat o conexiune roșie, în conformitate cu articolul 32, autoritățile menționate la articolul 26 alineatul (2) au acces, exclusiv în scopul combaterii fraudei de identitate, la datele menționate la articolul 18 alineatele (1) și (2) stocate în CIR conexate printr-o conexiune roșie.

Articolul 22

Efectuarea de interogări în registrul comun de date de identitate în scopul prevenirii, depistării sau anchetării infracțiunilor de terorism sau a altor infracțiuni grave

(1) În cazuri specifice, când există motive întemeiate să se creadă că o consultare a sistemelor de informații ale UE va contribui la prevenirea, depistarea sau anchetarea infracțiunilor de terorism sau a altor infracțiuni grave, în special în cazul în care există o suspiciune întemeiată că suspectul, făptuitorul sau victima unei infracțiuni de terorism sau a altei infracțiuni grave este o persoană ale cărei date sunt stocate în Eurodac, autoritățile desemnate și Europol pot consulta CIR pentru a afla dacă datele unei anumite persoane sunt prezente în Eurodac.

(2) În cazul în care, ca răspuns la o interogare, CIR indică faptul că există date privind persoana respectivă în Eurodac, CIR pune la dispoziția autorităților desemnate și a Europol un răspuns sub forma unei trimiteri, astfel cum se menționează la articolul 18 alineatul (2), indicând că Eurodac conține date între care s-a stabilit o concordanță. CIR răspunde de așa manieră încât securitatea datelor să nu fie compromisă.

Răspunsul care indică faptul că există date referitoare la persoana respectivă în Eurodac poate fi utilizat numai în scopul de a depune o cerere de acces integral, conform condițiilor și procedurilor prevăzute de instrumentul juridic care reglementează un astfel de acces.

În cazul unei concordanțe sau al concordanțelor multiple, autoritatea desemnată sau Europol solicită accesul integral la cel puțin unul dintre sistemele informatice la care a fost generată o concordanță.

În cazul în care, în mod excepțional, nu se solicită acest acces complet, autoritățile desemnate înregistrează motivele pentru nesolicitare, care trebuie să fie ușor de identificat în dosarul național. Europol înregistrează motivele în dosarul corespunzător.

(3) Accesul deplin la datele conținute în Eurodac în scopul prevenirii, depistării sau investigării infracțiunilor cu caracter terorist sau a altor infracțiuni grave rămâne supus condițiilor și procedurilor prevăzute în instrumentul juridic care reglementează acest acces.

Articolul 23

Păstrarea datelor în registrul comun de date de identitate

(1) Datele menționate la articolul 18 alineatele (1), (2) și (4) se elimină din CIR în mod automat, în conformitate cu dispozițiile privind păstrarea datelor din Regulamentul (UE) 2019/816.

▼B

(2) Dosarul individual este stocat în CIR numai atât timp cât datele corespondente sunt stocate cel puţin într-unul din sistemele de informaţii ale UE ale căror date sunt incluse în CIR. Crearea unei conexiuni nu afectează durata de păstrare a fiecărui element al datelor conexate.

Articolul 24

Păstrarea înregistrărilor

(1) Fără a aduce atingere articolului 29 din Regulamentul (UE) 2019/816, eu-LISA păstrează înregistrări ale tuturor operaţiunilor de prelucrare a datelor efectuate în CIR, în conformitate cu alineatele (2), (3) și (4) din prezentul articol.

(2) eu-LISA păstrează înregistrările tuturor operaţiunilor de prelucrare a datelor efectuate în CIR în temeiul articolului 20. În aceste înregistrări sunt incluse următoarele informaţii:

(a) statul membru sau agenţia Uniunii care lansează interogarea;

(b) scopul accesului utilizatorului care a lansat interogarea în CIR;

(c) data și ora efectuării interogării;

(d) tipul de date utilizate pentru lansarea interogării;

(e) rezultatele interogării.

(3) eu-LISA păstrează înregistrările tuturor operaţiunilor de prelucrare a datelor efectuate în CIR în temeiul articolului 21. În aceste înregistrări sunt incluse următoarele informaţii:

(a) statul membru sau agenţia Uniunii care lansează interogarea;

(b) scopul accesului utilizatorului care a lansat interogarea în CIR;

(c) data și ora efectuării interogării;

(d) atunci când se creează o conexiune, datele utilizate pentru lansarea interogării și rezultatele interogării care indică sistemul de informaţii al UE de la care s-au primit datele.

(4) eu-LISA păstrează înregistrările tuturor operaţiunilor de prelucrare a datelor efectuate în CIR în temeiul articolului 22. În aceste înregistrări sunt incluse următoarele informaţii:

(a) data și ora efectuării interogării;

(b) datele utilizate pentru lansarea interogării;

(c) rezultatele interogării;

(d) statul membru sau agenţia Uniunii care lansează interogarea în CIR.

Înregistrările acestor accesări sunt verificate periodic de către autoritatea de supraveghere competentă, în conformitate cu articolul 41 din Directiva (UE) 2016/680 sau de către Autoritatea Europeană pentru Protecţia Datelor, în conformitate cu articolul 43 din Regulamentul (UE) 2016/794, la intervale de cel mult șase luni, pentru a verifica dacă sunt îndeplinite procedurile și condiţiile prevăzute la articolul 22 alineatele (1) și (2) din prezentul regulament.

▼B

(5) Fiecare stat membru păstrează înregistrările interogărilor efectuate de autorităţile sale și de personalul acestora autorizat în mod corespunzător să utilizeze CIR în temeiul articolelor 20, 21 și 22. Fiecare agenţie a Uniunii păstrează înregistrările interogărilor efectuate în temeiul articolelor 21 și 22 de personalul său autorizat în mod corespunzător.

În plus, pentru orice acces la CIR în temeiul articolului 22, fiecare stat membru păstrează următoarele înregistrări:

(a) referinţa dosarului naţional;

(b) scopul accesării;

(c) în conformitate cu normele naţionale, identitatea de utilizator unică a funcţionarului care a efectuat interogarea și a funcţionarului care a dispus interogarea.

(6) În conformitate cu Regulamentul (UE) 2016/794, pentru orice acces la CIR în temeiul articolului 22 din prezentul regulament, Europol păstrează înregistrările privind identitatea de utilizator unică a funcţionarului care a efectuat interogarea și a funcţionarului care a dispus interogarea.

(7) Înregistrările menţionate la alineatele (2)-(6) pot fi folosite numai pentru a se monitoriza protecţia datelor, inclusiv pentru a se verifica admisibilitatea unei interogări și legalitatea prelucrării datelor, precum și pentru a se asigura securitatea și integritatea datelor. Aceste înregistrări sunt protejate prin măsuri corespunzătoare împotriva accesului neautorizat și sunt șterse după o perioadă de un an de la data la care au fost create. Totuși, dacă înregistrările sunt necesare pentru desfășurarea unor proceduri de monitorizare aflate în curs, acestea se șterg odată ce nu mai este nevoie de aceste înregistrări pentru procedurile de monitorizare.

(8) eu-LISA stochează înregistrările referitoare la istoricul datelor în dosare individuale. eu-LISA șterge astfel de înregistrări într-un mod automatizat, odată ce sunt șterse datele.

CAPITOLUL V

Detectorul de identităţi multiple

Articolul 25

Detectorul de identităţi multiple

(1) Pentru a susţine funcţionarea CIR și a sprijini realizarea obiectivelor EES, VIS, ETIAS, Eurodac, SIS și ECRIS-TCN, se instituie un detector de identităţi multiple (MID), care creează și stochează dosare de confirmare a identităţii, astfel cum se menţionează la articolul 34, și

▼B

care conține conexiuni între datele din sistemele de informații ale UE incluse în CIR și SIS, permițând astfel detectarea identităților multiple, cu scopul dublu de a facilita controalele de identitate și de a combate frauda de identitate.

(2) MID este alcătuit din următoarele componente:

(a) o infrastructură centrală, care stochează conexiuni și trimiteri la sistemele de informații ale UE;

(b) o infrastructură de comunicații securizată, care conectează MID cu SIS, cu infrastructurile centrale ale ESP și cu CIR.

(3) eu-LISA dezvoltă MID și asigură gestionarea tehnică a acestuia.

Articolul 26

Accesul la detectorul de identități multiple

(1) În scopul verificării manuale a identităților diferite, menționate la articolul 29, se acordă acces la datele menționate la articolul 34 stocate în MID:

(a) biroului SIRENE din statul membru atunci când creează sau actualizează o semnalare în conformitate cu Regulamentul (UE) 2018/1862;

(b) autorităților centrale ale statului membru de condamnare, atunci când înregistrează sau modifică date în ECRIS-TCN în conformitate cu articolul 5 sau cu articolul 9 din Regulamentul (UE) 2019/816.

(2) Autoritățile statelor membre și agențiile Uniunii care au acces la cel puțin un sistem de informații al UE inclus în CIR sau la SIS au acces la datele menționate la articolul 34 literele (a) și (b) cu privire la orice conexiune roșie, astfel cum se menționează la articolul 32.

(3) Autoritățile statelor membre și agențiile Uniunii au acces la conexiunile albe menționate la articolul 33 în cazul în care au acces la cele două sisteme de informații ale UE care conțin datele între care a fost creată conexiunea albă.

(4) Autoritățile statelor membre și agențiile Uniunii au acces la conexiunile verzi menționate la articolul 31 în cazul în care au acces la cele două sisteme de informații ale UE care conțin datele între care a fost creată conexiunea verde și dacă o interogare în sistemele de informații respective a evidențiat o concordanță între cele două seturi de date conexate.

Articolul 27

Detectarea de identități multiple

(1) Se lansează o detectare de identități multiple în CIR și în SIS atunci când:

(a) se creează sau se actualizează o semnalare în SIS privind o persoană, în conformitate cu capitolele VI-IX din Regulamentul (UE) 2018/1862;

(b) se creează sau se modifică un fișier de date în ECRIS-TCN în conformitate cu articolul 5 sau cu articolul 9 din Regulamentul (UE) 2019/816.

(2) În cazul în care datele conținute într-unul dintre sistemele de informații ale UE menționate la alineatul (1) includ date biometrice, CIR și SIS central utilizează BMS comun pentru a detecta identitățile

▼B

multiple. BMS comun compară șabloanele biometrice obținute din eventualele date biometrice noi cu șabloanele biometrice existente în BMS comun pentru a verifica dacă sunt deja stocate în CIR sau în SIS central date care aparțin aceleiași persoane.

(3) În plus față de procesul menționat la alineatul (2), CIR și SIS central utilizează EPS pentru a căuta datele stocate în SIS central, respectiv în CIR, utilizând următoarele date:

(a) numele (de familie), prenumele, numele la naștere, numele folosite anterior și numele de împrumut, locul nașterii, data nașterii, genul și orice cetățenii deținute, astfel cum se menționează la articolul 20 alineatul (3) din Regulamentul (UE) 2018/1862;

(b) numele (de familie), prenumele, data nașterii, locul nașterii (localitatea și țara), cetățenia sau cetățeniile și genul, astfel cum se menționează la articolul 5 alineatul (1) litera (a) din Regulamentul (UE) 2019/816.

(4) În plus față de procesul menționat la alineatele (2) și (3), CIR și SIS central utilizează EPS pentru a căuta datele stocate în SIS central, respectiv în CIR, utilizând datele din documentele de călătorie.

(5) Detectarea de identități multiple este lansată doar pentru a compara datele disponibile într-un sistem de informații al UE cu datele disponibile în alte sisteme de informații ale UE.

Articolul 28

Rezultatele detectării de identități multiple

(1) În cazul în care, în urma interogărilor menționate la articolul 27 alineatele (2), (3) și (4), nu se obține nicio concordanță, procedurile menționate la articolul 27 alineatul (1) continuă în conformitate cu instrumentele juridice care le reglementează.

(2) În cazul în care, în urma interogării menționate la articolul 27 alineatele (2), (3) și (4), se obțin(e) una sau mai multe concordanțe, CIR și, dacă este relevant, SIS creează o conexiune între datele utilizate pentru lansarea interogării și datele care au generat concordanța.

În cazul în care se obțin mai multe concordanțe, se creează o conexiune între toate datele care au generat concordanța. În cazul în care datele erau deja conexate, conexiunea existentă se extinde la datele utilizate pentru lansarea interogării.

(3) În cazul în care, în urma interogării menționate la articolul 27 alineatele (2), (3) și (4), se obțin una sau mai multe concordanțe și datele de identitate din dosarele conexate sunt aceleași sau similare, se creează o conexiune albă în conformitate cu articolul 33.

▼B

(4) În cazul în care, în urma interogării menţionate la articolul 27 alineatele (2), (3) și (4), se obţin una sau mai multe concordanţe și datele de identitate din dosarele legate nu pot fi considerate ca fiind similare, se creează o conexiune galbenă în conformitate cu articolul 30 și se aplică procedura prevăzută la articolul 29.

(5) Comisia adoptă acte delegate în conformitate cu articolul 69 prin care stabilește proceduri pentru a determina cazurile în care datele de identitate pot fi considerate aceleași sau similare.

(6) Conexiunile sunt stocate în dosarul de confirmare a identităţii menţionat la articolul 34.

(7) Comisia stabilește, în cooperare cu eu-LISA, prin acte de punere în aplicare, normele tehnice de creare a conexiunilor între datele provenite de la diferitele sisteme de informaţii ale UE. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 70 alineatul (2).

Articolul 29

Verificarea manuală a identităţilor diferite și autorităţile responsabile

(1) Fără a aduce atingere alineatului (2), autoritatea responsabilă de verificarea manuală a identităţilor diferite este:

(a) biroul SIRENE din statul membru pentru concordanţe obţinute la crearea sau actualizarea unei semnalări în SIS în conformitate cu Regulamentul (UE) 2018/1862;

(b) autorităţile centrale ale statului membru de condamnare în cazul concordanţelor obţinute la înregistrarea sau modificarea de date în ECRIS-TCN în conformitate cu articolul 5 sau articolul 9 din Regulamentul (UE) 2019/816.

MID indică autoritatea responsabilă de verificarea manuală a identităţilor diferite în dosarul de confirmare a identităţii.

(2) Autoritatea responsabilă de verificarea manuală a identităţilor diferite în dosarul de confirmare a identităţii este biroul SIRENE din statul membru care a creat semnalarea, în cazul în care se stabilește o conexiune între datele conţinute într-o semnalare:

(a) cu privire la persoanele căutate în vederea arestării în scopul predării sau al extrădării, menţionată la articolul 26 din Regulamentul (UE) 2018/1862;

(b) cu privire la persoane dispărute sau vulnerabile, menţionată la articolul 32 din Regulamentul (UE) 2018/1862;

(c) cu privire la persoane căutate în vederea participării la o procedură judiciară, astfel cum se prevede la articolul 34 din Regulamentul (UE) 2018/1862;

(d) cu privire la persoane în scopul efectuării de controale discrete, de controale prin interviu sau de controale specifice, astfel cum se prevede la articolul 36 din Regulamentul (UE) 2018/1862.

▼B

(3) Autoritatea responsabilă de verificarea manuală a identităţilor diferite are acces la datele conexate conţinute în dosarul relevant de confirmare a identității și la datele de identitate conexate din CIR și, în cazul în care este relevant, din SIS. Aceasta evaluează fără întârziere identităţile diferite. După finalizarea evaluării, actualizează conexiunea, în conformitate cu articolele 31, 32 și 33, și o adaugă fără întârziere la dosarul de confirmare a identității.

(4) În cazul în care se creează mai multe conexiuni, autoritatea responsabilă de verificarea manuală a identităţilor diferite evaluează fiecare conexiune separat.

(5) În cazul în care datele care au generat concordanţa erau deja conexate, autoritatea responsabilă de verificarea manuală a identităţilor diferite ţine seama de conexiunile existente atunci când evaluează crearea de noi conexiuni.

Articolul 30

Conexiunea galbenă

(1) În cazul în care nu s-a efectuat încă o verificare manuală a identităţilor diferite, o conexiune între datele din două sau mai multe sisteme de informaţii ale UE este clasificată ca galbenă în oricare dintre următoarele cazuri:

(a) datele conexate au în comun aceleași date biometrice, însă au date de identitate similare sau diferite;

(b) datele conexate au date de identitate diferite, dar au în comun aceleași date din documentul de călătorie și cel puţin unul dintre sistemele de informaţii ale UE nu conţine date biometrice privind persoana în cauză;

(c) datele conexate au în comun aceleași date de identitate, însă au date biometrice diferite;

(d) datele conexate au date de identitate similare sau diferite și au în comun aceleași date din documentul de călătorie, însă au date biometrice diferite.

(2) În cazul în care o conexiune este clasificată ca galbenă în conformitate cu alineatul (1), se aplică procedura prevăzută la articolul 29.

Articolul 31

Conexiune verde

(1) O conexiune între datele din două sau mai multe sisteme de informaţii ale UE este clasificată ca verde în cazul în care:

(a) datele conexate au date biometrice diferite, însă au în comun aceleași date de identitate, iar autoritatea responsabilă de verificarea manuală a identităţilor diferite a ajuns la concluzia că datele conexate se referă la două persoane diferite;

(b) datele conexate au date biometrice diferite, au date de identitate similare sau diferite și au în comun aceleași date din documentul de călătorie, iar autoritatea responsabilă de verificarea manuală a identităţilor diferite a ajuns la concluzia că datele conexate se referă la două persoane diferite;

▼B

(c) datele conexate au date de identitate diferite, dar au în comun aceleași date privind documentele de călătorie, cel puţin unul dintre sistemele de informaţii ale UE nu conţine date biometrice privind persoana în cauză, iar autoritatea responsabilă de verificarea manuală a identităţilor diferite a ajuns la concluzia că datele conexate se referă la două persoane diferite.

(2) În cazul în care se lansează o interogare în CIR sau în SIS și există o conexiune verde între datele din două sau mai multe dintre sistemele de informaţii ale UE, MID indică faptul că datele de identitate ale datelor conexate nu corespund aceleiași persoane.

(3) În cazul în care o autoritate dintr-un stat membru deţine dovezi care sugerează că o conexiune verde a fost înregistrată incorect în MID, că o conexiune verde nu este actualizată sau că datele au fost prelucrate în MID sau în sistemele de informaţii ale UE cu încălcarea prezentului regulament, aceasta verifică datele relevante stocate în CIR și în SIS și, dacă este necesar, rectifică sau șterge conexiunea din MID fără întârziere. Autoritatea în cauză din statul membru informează fără întârziere statul membru responsabil de verificarea manuală a identităţilor diferite.

Articolul 32

Conexiune roșie

(1) O conexiune între datele din două sau mai multe sisteme de informaţii ale UE este clasificată ca roșie în oricare dintre următoarele cazuri:

(a) datele conexate au în comun aceleași date biometrice, însă au date de identitate similare sau diferite, iar autoritatea responsabilă de verificarea manuală a identităţilor diferite a ajuns la concluzia că datele conexate se referă în mod nejustificat la aceeași persoană;

(b) datele conexate au aceleași date de identitate sau date de identitate similare sau diferite și aceleași date din documentul de călătorie, însă au date biometrice diferite, iar autoritatea responsabilă de verificarea manuală a identităţilor diferite a ajuns la concluzia că datele conexate se referă la două persoane diferite dintre care cel puţin una utilizează același document de călătorie în mod nejustificat;

(c) datele conexate au în comun aceleași date de identitate, însă au date biometrice diferite, iar datele din documentul de călătorie sunt diferite sau lipsesc, iar autoritatea responsabilă de verificarea manuală a identităţilor diferite a ajuns la concluzia că datele conexate se referă în mod nejustificat la două persoane diferite;

(d) datele conexate au date de identitate diferite, dar au în comun aceleași date din documentul de călătorie, cel puţin unul dintre sistemele de informaţii ale UE nu conţine date biometrice privind persoana în cauză, iar autoritatea responsabilă de verificarea manuală a identităţilor diferite a ajuns la concluzia că datele conexate se referă în mod nejustificat la aceeași persoană.

▼B

(2) În cazul în care se lansează o interogare în CIR sau în SIS și există o conexiune roșie între datele din două sau mai multe dintre sistemele de informaţii ale UE, MID indică datele menţionate la articolul 34. Măsurile subsecvente creării unei conexiuni roșii se iau în conformitate cu dreptul Uniunii și cu dreptul intern, orice consecinţă juridică pentru persoana în cauză bazându-se exclusiv pe datele relevante privind persoana respectivă. Din simpla existenţă a unei conexiuni roșii nu derivă nicio consecinţă juridică pentru persoana în cauză.

(3) În cazul în care este creată o conexiune roșie între datele din EES, VIS, ETIAS, Eurodac sau ECRIS-TCN, dosarul individual stocat în CIR se actualizează în conformitate cu articolul 19 alineatul (2).

(4) Fără a aduce atingere dispoziţiilor referitoare la gestionarea semnalărilor în SIS din Regulamentele (UE) 2018/1860, (UE) 2018/1861 și (UE) 2018/1862 și fără a aduce atingere restricţiilor necesare pentru protejarea securităţii și a ordinii publice, pentru prevenirea infracţiunilor și pentru garantarea faptului că nicio anchetă naţională nu va fi pusă în pericol, în cazul în care se creează o conexiune roșie, autoritatea responsabilă de verificarea manuală a identităţilor diferite informează persoana în cauză cu privire la prezenţa unor date de identitate multiple ilegale și pune la dispoziţia persoanei în cauză un număr de identificare unic, astfel cum este menţionat la articolul 34 litera (c) din prezentul regulament, o trimitere la autoritatea responsabilă de verificarea manuală a identităţilor diferite, astfel cum este menţionată la articolul 34 litera (d) din prezentul regulament, precum și adresa site-ului de internet de pe portalul web creat în conformitate cu articolul 49 din prezentul regulament.

(5) Informaţiile menţionate la alineatul (4) sunt furnizate în scris sub forma unui formular standard de către autoritatea responsabilă cu verificarea manuală a identităţilor diferite. Comisia stabilește conţinutul și prezentarea acestui formular prin intermediul unor acte de punere în aplicare. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 70 alineatul (2).

(6) În cazul în care se creează o conexiune roșie, MID notifică într-un mod automatizat autorităţile responsabile de datele conexate.

(7) În cazul în care o autoritate a unui stat membru sau o agenţie a Uniunii care are acces la CIR sau la SIS are dovezi care sugerează că o conexiune roșie a fost înregistrată incorect în MID sau că datele au fost prelucrate în MID, CIR sau SIS cu încălcarea dispoziţiilor prezentului regulament, autoritatea sau agenţia respectivă verifică datele relevante stocate în CIR și SIS și:

(a) în cazul în care conexiunea se referă la una dintre semnalările SIS menţionate la articolul 29 alineatul (2), informează imediat biroul SIRENE relevant din statul membru care a creat semnalarea SIS;

(b) în toate celelalte cazuri, fie rectifică, fie șterge conexiunea din MID imediat.

Dacă un birou SIRENE este contactat în temeiul literei (a) de la primul paragraf, acesta verifică probele furnizate de către autoritatea din statul membru sau agenţia Uniunii și, dacă este cazul, rectifică sau șterge conexiunea din MID imediat.

▼B

Autoritatea competentă a statului membru care obţine dovezile informează fără întârziere autoritatea statului membru responsabil de verificarea manuală a identităţilor diferite cu privire la orice rectificare sau ștergere relevantă a unei conexiuni roșii.

Articolul 33

Conexiune albă

(1) O conexiune între datele din două sau mai multe sisteme de informaţii ale UE este clasificată ca albă în oricare dintre următoarele cazuri:

(a) datele conexate au în comun aceleași date biometrice și date de identitate identice sau similare;

(b) datele conexate au în comun date de identitate identice sau similare, aceleași date din documentul de călătorie și cel puţin unul dintre sistemele de informaţii ale UE nu dispune de datele biometrice ale persoanei în cauză;

(c) datele conexate au aceleași date biometrice, aceleași date din documentul de călătorie și date de identitate similare;

(d) datele conexate au în comun aceleași date biometrice, însă au date de identitate similare sau diferite, iar autoritatea responsabilă de verificarea manuală a identităţilor diferite a ajuns la concluzia că datele conexate se referă în mod justificat la aceeași persoană.

(2) În cazul în care se lansează o interogare în CIR sau în SIS și există o conexiune albă între datele din două sau mai multe dintre sistemele de informaţii ale UE, MID indică faptul că datele de identitate ale datelor conexe corespund aceleiași persoane. Sistemele de informaţii ale UE în care s-a lansat interogarea răspund indicând, după caz, toate datele conexate referitoare la persoana respectivă și generând, prin urmare, o concordanţă în raport cu datele conexate de conexiunea albă, dacă autoritatea care a lansat interogarea are acces la datele conexate în temeiul dreptului Uniunii sau al dreptului intern.

(3) În cazul în care se creează o conexiune albă între datele din EES, VIS, ETIAS, Eurodac sau ECRIS-TCN, dosarul individual stocat în CIR se actualizează în conformitate cu articolul 19 alineatul (2).

(4) Fără a aduce atingere dispoziţiilor referitoare la gestionarea semnalărilor în SIS din Regulamentele (UE) 2018/1860, (UE) 2018/1861 și (UE) 2018/1862 și fără a aduce atingere restricţiilor necesare pentru protejarea securităţii și a ordinii publice, pentru prevenirea infracţiunilor și pentru garantarea faptului că nicio anchetă naţională nu va fi pusă în pericol, în cazul în care este creată o conexiune albă în urma unei verificări manuale a unor identităţi diferite, autoritatea responsabilă de verificarea manuală a identităţilor diferite informează persoana în cauză cu privire la prezenţa unor date de identitate similare sau diferite și furnizează persoanei în cauză un număr de identificare unic, astfel cum este menţionat la articolul 34 litera (c) din prezentul regulament, o trimitere către la autoritatea responsabilă de verificarea manuală a identităţilor diferite, astfel cum este menţionată la articolul 34 litera (d) din prezentul regulament, precum și adresa site-ului de internet de pe portalul web creat în conformitate cu articolul 49 din prezentul regulament.

▼B

(5) În cazul în care o autoritate dintr-un stat membru deține dovezi care sugerează că o conexiune albă a fost înregistrată incorect în MID, că o conexiune albă nu este actualizată sau că datele au fost prelucrate în MID sau în sistemele de informații ale UE cu încălcarea prezentului regulament, aceasta verifică datele relevante stocate în CIR și în SIS și, dacă este necesar, rectifică sau șterge conexiunea din MID, fără întârziere. Autoritatea în cauză din statul membru informează fără întârziere statul membru responsabil de verificarea manuală a identităților diferite.

(6) Informațiile din alineatul (4) sunt furnizate în scris sub forma unui formular standard de către autoritatea responsabilă cu verificarea manuală a identităților diferite. Comisia stabilește conținutul și prezentarea acestui formular prin intermediul unor acte de punere în aplicare. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 70 alineatul (2).

Articolul 34

Dosarul de confirmare a identității

Dosarul de confirmare a identității conține următoarele date:

(a) conexiunile menționate la articolele 30-33;

(b) o trimitere la sistemele de informații ale UE în care sunt ținute datele conexate;

(c) un număr de identificare unic care permite extragerea datelor conexate din sistemele de informații ale UE corespondente;

(d) autoritatea responsabilă de verificarea manuală a identităților diferite;

(e) data creării conexiunii sau a oricărei actualizări a acesteia.

Articolul 35

Păstrarea datelor în detectorul de identități multiple

Dosarele de confirmare a identității și datele din aceste dosare, inclusiv conexiunile, se stochează în MID numai atât timp cât datele conexate sunt stocate în două sau mai multe dintre sistemele de informații ale UE. Dosarele se șterg din MID în mod automat.

Articolul 36

Păstrarea înregistrărilor

(1) eu-LISA păstrează înregistrări ale tuturor operațiunilor de prelucrare a datelor efectuate în MID. În aceste înregistrări sunt incluse următoarele informații:

(a) statul membru care lansează interogarea;

(b) scopul în care utilizatorul a avut acces;

(c) data și ora efectuării interogării;

(d) tipul de date utilizate pentru lansarea interogării;

▼B

(e) trimiterea la datele conexate;

(f) istoricul dosarului de confirmare a identității.

(2) Fiecare stat membru păstrează înregistrări ale interogărilor efectuate de autoritățile sale și de personalul acestora autorizat în mod corespunzător să utilizeze MID. Fiecare agenție a Uniunii păstrează înregistrări ale interogărilor efectuate de personalul său autorizat în mod corespunzător.

(3) Înregistrările menționate la alineatele (1) și (2) pot fi folosite numai pentru a se monitoriza protecția datelor, inclusiv pentru a se verifica admisibilitatea unei interogări și legalitatea prelucrării datelor, precum și pentru a se asigura securitatea și integritatea datelor. Aceste înregistrări sunt protejate prin măsuri corespunzătoare împotriva accesului neautorizat și sunt șterse după o perioadă de un an de la data la care au fost create. Dacă cu toate acestea, înregistrările sunt necesare pentru desfășurarea unor proceduri de monitorizare aflate în curs, acestea se șterg odată ce nu mai este nevoie de aceste înregistrări pentru procedurile de monitorizare.

CAPITOLUL VI

Măsuri de asistare a interoperabilității

Articolul 37

Calitatea datelor

(1) Fără a aduce atingere responsabilităților statelor membre cu privire la calitatea datelor introduse în sisteme, eu-LISA instituie mecanisme și proceduri automatizate de control al calității datelor în ceea ce privește datele stocate în SIS, Eurodac, ECRIS-TCN, BMS comun și CIR.

(2) eu-LISA implementează mecanisme de evaluare a fiabilității BMS comun, indicatori comuni de calitate a datelor și standarde minime de calitate pentru stocarea datelor în SIS, Eurodac, ECRIS-TCN, BMS comun și CIR.

Numai datele care respectă standardele minime de calitate pot fi introduse în SIS, Eurodac, ECRIS-TCN, BMS comun, CIR și MID.

(3) eu-LISA furnizează statelor membre rapoarte periodice privind mecanismele și procedurile automatizate de control al calității datelor și privind indicatorii comuni de calitate a datelor. De asemenea, agenția furnizează Comisiei rapoarte periodice privind problemele întâmpinate și statele membre vizate. La cerere, eu-LISA pune raportul și la dispoziția Parlamentului European și a Consiliului. Niciun raport prezentat în temeiul prezentului alineat nu conține date cu caracter personal.

(4) Detaliile privind mecanismele și procedurile automatizate de control al calității datelor, indicatorii comuni de calitate a datelor și standardele minime de calitate pentru stocarea datelor în SIS, Eurodac, ECRIS-TCN, BMS comun și CIR, în special în ceea ce privește datele biometrice, sunt stabilite prin acte de punere în aplicare. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 70 alineatul (2).

▼B

(5) La un an de la instituirea mecanismelor și procedurilor automatizate de control al calităţii datelor și a indicatorilor comuni de calitate a datelor și a standardelor minime de calitate a datelor și, ulterior, în fiecare an, Comisia evaluează modul în care statele membre asigură calitatea datelor și formulează eventuale recomandări. Statele membre pun la dispoziţia Comisiei un plan de acţiune pentru remedierea deficienţelor identificate în raportul de evaluare și, în special, a problemelor de calitate a datelor cauzate de datele eronate din sistemele de informaţii ale UE. Statele membre raportează regulat Comisiei cu privire la progresele înregistrate în funcţie de acest plan de acţiune până în momentul în care acesta este pus în aplicare pe deplin.

Comisia transmite raportul de evaluare Parlamentului European, Consiliului, Autorităţii Europene pentru Protecţia Datelor, Comitetului european pentru protecţia datelor și Agenţiei pentru Drepturi Fundamentale a Uniunii Europene instituită prin Regulamentul (CE) nr. 168/2007 al Consiliului ([8]).

Articolul 38

Formatul universal pentru mesaje

(1) Se instituie un format universal pentru mesaje (UMF). UMF definește standardele pentru anumite elemente de conţinut ale schimbului transfrontalier de informaţii între sistemele de informaţii, autorităţile sau organizaţiile participante din domeniul justiţiei și afacerilor interne.

(2) Standardul UMF se utilizează în dezvoltarea Eurodac, a ECRIS-TCN, a ESP, a CIR, a MID și, dacă este necesar, în dezvoltarea de către eu-LISA sau de către orice altă agenţie a Uniunii a unor noi modele de schimb de informaţii și sisteme de informaţii în domeniul justiţiei și afacerilor interne.

(3) Comisia adoptă un act de punere în aplicare pentru a stabili și dezvolta standardul UMF menţionat la alineatul (1) din prezentul articol. Respectivul act de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 70 alineatul (2).

Articolul 39

Registrul central de raportare și statistici

▼M4

(1) Se instituie un registru central de raportare și statistici (CRRS) în scopul de a susţine obiectivele SIS, Eurodac și ECRIS-TCN, în conformitate cu instrumentele juridice respective care reglementează sistemele menţionate, și de a furniza date statistice utilizabile între sisteme și rapoarte analitice în scopuri de elaborare a politicilor, operaţionale și de asigurare a calităţii datelor. CRRS sprijină, de asemenea, obiectivele Regulamentului (UE) 2024/982.

(2) eu-LISA creează, implementează și găzduiește în amplasamentele sale tehnice CRRS care conţine datele și statisticile menţionate

([8]) Regulamentul (CE) nr. 168/2007 al Consiliului din 15 februarie 2007 privind înfiinţarea Agenţiei pentru Drepturi Fundamentale a Uniunii Europene (JO L 53, 22.2.2007, p. 1).

▼M4

la articolul 74 din Regulamentul (UE) 2018/1862 și la articolul 32 din Regulamentul (UE) 2019/816 separate în mod logic pe sisteme de informaţii ale UE. De asemenea, eu-LISA colectează datele și statisticile de la routerul menţionat la articolul 72 alineatul (1) din Regulamentul (UE) 2024/982. Accesul la CRRS se acordă printr-un acces controlat și securizat și cu profiluri de utilizator specifice, exclusiv în scopul întocmirii de rapoarte și statistici, autorităţilor menţionate la articolul 74 din Regulamentul (UE) 2018/1862, la articolul 32 din Regulamentul (UE) 2019/816 și la articolul 72 alineatul (1) din Regulamentul (UE) 2024/982.

▼B

(3) eu-LISA anonimizează datele și înregistrează aceste date anonimizate în CRRS. Procesul de anonimizare a datelor este automatizat.

Datele conţinute în CRRS trebuie să nu permită identificarea persoanelor fizice.

(4) CRRS este alcătuit din următoarele componente:

(a) instrumentele necesare anonimizării datelor;

(b) o infrastructură centrală, constând într-un registru de date anonime;

(c) o infrastructură de comunicaţii securizată pentru a conecta CRRS la SIS, Eurodac și ECRIS-TCN, precum și la infrastructurile centrale ale BMS comun, CIR și MID.

(5) Comisia adoptă un act delegat în conformitate cu articolul 69 prin care stabilește norme detaliate privind funcţionarea CRRS, inclusiv garanţii specifice pentru prelucrarea datelor cu caracter personal în temeiul alineatelor (2) și (3) din prezentul articol și norme de securitate aplicabile registrului.

CAPITOLUL VII

Protecţia datelor

Articolul 40

Operatorul de date

(1) În ceea ce privește prelucrarea datelor în BMS comun, autorităţile statelor membre care sunt operatori pentru Eurodac, SIS și, respectiv, ECRIS-TCN sunt operatori în conformitate cu articolul 4 punctul 7 din Regulamentul (UE) 2016/679 sau cu articolul 3 punctul 8 din Directiva (UE) 2016/680 în ceea ce privește șabloanele biometrice obţinute din datele menţionate la articolul 13 din prezentul regulament pe care acestea le introduc în sistemele de bază și sunt responsabile de prelucrarea șabloanelor biometrice în BMS comun.

(2) În ceea ce privește prelucrarea datelor în CIR, autorităţile statelor membre care sunt operatori pentru Eurodac și, respectiv, ECRIS-TCN sunt operatori în conformitate cu articolul 4 punctul 7 din Regulamentul (UE) 2016/679 sau articolul 3 punctul 8 din Directiva (UE) 2016/680 în ceea ce privește datele menţionate la articolul 18 din prezentul regulament pe care le introduc în sistemele de bază și sunt responsabile de prelucrarea respectivelor date cu caracter personal în CIR.

▼B

(3) În ceea ce privește prelucrarea datelor în MID:

(a) Agenţia Europeană pentru Poliţia de Frontieră și Garda de Coastă este operator de date în înţelesul articolului 3 punctul 8 din Regulamentul (UE) 2018/1725 în ceea ce privește prelucrarea datelor cu caracter personal de către unitatea centrală a ETIAS;

(b) autorităţile statelor membre care introduc sau modifică date în dosarul de confirmare a identităţii sunt operatori în conformitate cu articolul 4 punctul 7 din Regulamentul (UE) 2016/679 sau cu articolul 3 punctul 8 din Directiva (UE) 2016/680 și sunt responsabile de prelucrarea datelor cu caracter personal în MID.

(4) În scopul monitorizării protecţiei datelor, inclusiv pentru verificarea admisibilităţii unei interogări și a legalităţii prelucrării datelor, operatorii de date au acces la înregistrările menţionate la articolele 10, 16, 24 și 36 pentru automonitorizarea menţionată la articolul 44.

Articolul 41

Persoana împuternicită de către operatorul de date

În ceea ce privește prelucrarea datelor cu caracter personal în BMS comun, CIR și MID, eu-LISA este persoană împuternicită de operatorul de date în înţelesul articolului 3 punctul 12 litera (a) din Regulamentul (UE) 2018/1725.

Articolul 42

Securitatea prelucrărilor de date

(1) eu-LISA, unitatea centrală a ETIAS, Europol și autorităţile din statele membre asigură securitatea prelucrărilor de date cu caracter personal efectuate în temeiul prezentului regulament. eu-LISA, unitatea centrală a ETIAS, Europol și autorităţile din statele membre cooperează în ceea ce privește sarcinile legate de securitate.

(2) Fără a aduce atingere articolului 33 din Regulamentul (UE) 2018/1725, eu-LISA ia măsurile necesare pentru a asigura securitatea componentelor de interoperabilitate și a infrastructurii de comunicaţii aferente.

(3) Mai precis, eu-LISA adoptă măsurile necesare, în special un plan de securitate, un plan de asigurare a continuităţii activităţii și un plan de recuperare în caz de dezastru, pentru:

(a) a proteja fizic datele, inclusiv prin elaborarea de planuri de urgenţă în scopul protejării infrastructurii critice;

(b) a interzice accesul persoanelor neautorizate la echipamentele și instalaţiile de prelucrare a datelor;

(c) a împiedica citirea, copierea, modificarea sau ștergerea neautorizate a suporturilor de date;

(d) a împiedica introducerea neautorizată de date, precum și orice inspectare, modificare sau ștergere neautorizată a datelor cu caracter personal înregistrate;

▼B

(e) a împiedica prelucrarea neautorizată de date, precum și orice copiere, modificare sau ștergere neautorizată a datelor;

(f) a împiedica utilizarea sistemelor de prelucrare automată a datelor de către persoane neautorizate care utilizează echipamente de comunicare a datelor;

(g) a asigura faptul că persoanele autorizate să acceseze componentele de interoperabilitate au acces numai la datele care fac obiectul autorizației lor de acces, prin utilizarea exclusivă a unor nume de utilizator individuale și a unor moduri de acces confidențiale;

(h) a asigura posibilitatea de a verifica și de a stabili care sunt organismele cărora le pot fi transmise datele cu caracter personal prin utilizarea echipamentelor de comunicare a datelor;

(i) a asigura faptul că se poate verifica și stabili ce date au fost prelucrate în componentele de interoperabilitate, în ce moment, de către cine și cu ce scop;

(j) a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transmiterii datelor cu caracter personal către sau din componentele de interoperabilitate sau în timpul transportului suporturilor de date, în special prin intermediul unor tehnici de criptare corespunzătoare;

(k) a asigura că, în cazul unei întreruperi, sistemele instalate pot fi readuse la operarea normală;

(l) a asigura fiabilitatea prin garantarea faptului că orice eroare de funcționare a componentelor de interoperabilitate este semnalată în mod adecvat;

(m) a monitoriza eficacitatea măsurilor de securitate prevăzute la prezentul alineat și a se lua măsurile de organizare necesare referitoare la supravegherea internă, astfel încât să se asigure respectarea dispozițiilor prezentului regulament și să se evalueze aceste măsuri de securitate în contextul noilor evoluții tehnologice.

(4) Statele membre, Europol și unitatea centrală a ETIAS iau măsuri echivalente celor menționate la alineatul (3) în materie de securitate în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile care au drept de acces la oricare dintre componentele de interoperabilitate.

Articolul 43

Incidente de securitate

(1) Orice eveniment care are sau poate avea un impact asupra securității componentelor de interoperabilitate și care poate cauza daune sau pierderi ale datelor stocate în acestea se consideră a fi un incident de securitate, în special în cazul în care este posibil să se fi accesat în mod neautorizat datele sau în cazul în care disponibilitatea, integritatea și confidențialitatea datelor a fost sau este posibil să fi fost compromisă.

(2) Incidentele de securitate sunt gestionate astfel încât să se asigure un răspuns rapid, eficace și corespunzător.

▼B

(3) Fără a aduce atingere notificării și comunicării unei încălcări a securității datelor cu caracter personal în temeiul articolului 33 din Regulamentul (UE) 2016/679, al articolului 30 din Directiva (UE) 2016/680 sau al ambelor articole, statele membre notifică fără întârziere orice incident de securitate Comisiei, eu-LISA, autorităților competente de supraveghere și Autorității Europene pentru Protecția Datelor.

Fără a aduce atingere articolelor 34 și 35 din Regulamentul (UE) 2018/1725 și articolului 34 din Regulamentul (UE) 2016/794, unitatea centrală a ETIAS și Europol notifică fără întârziere orice incident de securitate Comisiei, eu-LISA și Autorității Europene pentru Protecția Datelor.

În cazul unui incident de securitate legat de infrastructura centrală a componentelor de interoperabilitate, eu-LISA notifică fără întârziere Comisia și Autoritatea Europeană pentru Protecția Datelor.

(4) Informațiile privind un incident de securitate care are sau poate avea un impact asupra funcționării componentelor de interoperabilitate sau asupra disponibilității, integrității și confidențialității datelor sunt puse fără întârziere la dispoziția statelor membre, a unității centrale a ETIAS și Europol și se raportează în conformitate cu planul de gestionare a incidentelor întocmit de eu-LISA.

(5) Statele membre în cauză, unitatea centrală a ETIAS, Europol și eu-LISA colaborează în cazul unui incident de securitate. Comisia stabilește detaliile acestei cooperări prin intermediul unor acte de punere în aplicare. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 70 alineatul (2).

Articolul 44

Automonitorizarea

Statele membre și agențiile relevante ale Uniunii se asigură că fiecare autoritate care are acces la componentele de interoperabilitate ia măsurile necesare pentru a monitoriza respectarea prezentului regulament și cooperează, dacă este cazul, cu autoritatea națională de supraveghere.

Operatorii de date menționați la articolul 40 iau măsurile necesare pentru a monitoriza respectarea dispozițiilor prezentului regulament pe parcursul prelucrării datelor, inclusiv prin verificarea frecventă a înregistrărilor menționate la articolele 10, 16, 24 și 36 și cooperează, după caz, cu autoritățile de supraveghere și cu Autoritatea Europeană pentru Protecția Datelor.

Articolul 45

Sancțiuni

Statele membre se asigură că orice utilizare abuzivă a datelor și orice prelucrare sau schimb de date care încalcă prezentul regulament sunt sancționate în conformitate cu dreptul intern. Sancțiunile prevăzute trebuie să fie eficace, proporționale și cu efect de descurajare.

Articolul 46

Răspunderea

(1) Fără a aduce atingere dreptului la despăgubiri și răspunderii din partea operatorului sau a persoanei împuternicite de către operator în conformitate cu Regulamentul (UE) 2016/679, Directiva (UE) 2016/680 și Regulamentul (UE) 2018/1725:

▼B

(a) orice persoană sau stat membru care a suferit prejudicii materiale sau morale ca urmare a unei operaţiuni ilegale de prelucrare a datelor cu caracter personal sau a oricărei alte acţiuni incompatibile cu prezentul regulament realizate de către un stat membru are dreptul de a primi despăgubiri din partea statului membru respectiv;

(b) orice persoană sau stat membru care a suferit prejudicii materiale sau morale ca urmare a oricărei acţiuni realizate de către Europol, Agenţia Europeană pentru Poliţia de Frontieră și Garda de Coastă sau eu-LISA care este incompatibilă cu prezentul regulament are dreptul de a primi despăgubiri din partea agenţiei respective.

Respectivul stat membru, Europol, Agenţia Europeană pentru Poliţia de Frontieră și Garda de Coastă sau eu-LISA sunt exonerate de răspunderea care le revine în temeiul primului paragraf, integral sau parţial, dacă dovedesc că fapta care a cauzat prejudiciul nu le este imputabilă.

(2) Dacă orice nerespectare de către un stat membru a obligaţiilor în temeiul prezentului regulament provoacă prejudicii componentelor de interoperabilitate, răspunderea aparţine statului membru respectiv, cu excepţia cazului în care eu-LISA sau un alt stat membru care are obligaţii în temeiul prezentului regulament nu a luat măsuri rezonabile pentru a preveni producerea prejudiciului sau pentru a reduce la minimum impactul acestuia.

(3) Cererile de despăgubiri introduse împotriva unui stat membru pentru prejudiciile menţionate la alineatele (1) și (2) sunt reglementate de dreptul intern al statului membru pârât. Cererile de despăgubiri împotriva operatorului sau a eu-LISA pentru prejudiciile menţionate la alineatele (1) și (2) fac obiectul condiţiilor prevăzute în tratate.

Articolul 47

Dreptul la informare

(1) Autoritatea care colectează date cu caracter personal care urmează a fi stocate în BMS comun, în CIR sau în MID pun la dispoziţia persoanelor ale căror date sunt colectate informaţiile cerute în temeiul articolelor 13 și 14 din Regulamentul (UE) 2016/679, al articolelor 12 și 13 din Directiva (UE) 2016/680 și al articolelor 15 și 16 din Regulamentul (UE) 2018/1725. Autoritatea furnizează informaţiile la momentul colectării acestor date.

(2) Informaţiile sunt furnizate într-un limbaj clar și simplu, într-o limbă pe care persoana în cauză o înţelege sau despre care se poate presupune în mod rezonabil că o înţelege. Aceasta trebuie să includă furnizarea de informaţii într-un mod adecvat vârstei persoanelor vizate care sunt minore.

(3) Normele privind dreptul la informare din cadrul normelor aplicabile ale Uniunii în materie de protecţie a datelor se aplică datelor cu caracter personal înregistrate în ECRIS-TCN și prelucrate în scopurile prezentului regulament.

Articolul 48

Dreptul de acces, de rectificare și de ștergere a datelor cu caracter personal stocate în MID și dreptul la restricţionarea prelucrării acestora

(1) Pentru a-și exercita drepturile prevăzute la articolele 15-18 din Regulamentul (UE) 2016/679, la articolele 17-20 din Regulamentul (UE) 2018/1725 și la articolele 14, 15 și 16 din Directiva

▼B

(UE) 2016/680, orice persoană are dreptul de a se adresa autorității competente din oricare stat membru, care trebuie să examineze cererea și să răspundă.

(2) Statul membru care examinează o astfel de cerere răspunde fără întârzieri nejustificate și, în orice caz, în termen de 45 de zile de la primirea cererii. Această perioadă poate fi prelungită cu încă 15 zile atunci când este necesar, ținându-se seama de complexitatea și de numărul cererilor. Statul membru care examinează cererea respectivă informează persoana vizată cu privire la orice astfel de prelungire în termen de 45 de zile de la primirea cererii, prezentându-i acesteia și motivele întârzierii. Statele membre pot decide ca răspunsurile să fie oferite de birourile centrale.

(3) În cazul în care o cerere de rectificare sau de ștergere a datelor cu caracter personal este adresată unui alt stat membru decât cel responsabil de verificarea manuală a identităților diferite, statul membru căruia i s-a adresat cererea contactează autoritățile statului membru responsabil de verificarea manuală a identităților diferite în termen de șapte zile. Statul membru responsabil de verificarea manuală a identităților diferite verifică exactitatea datelor și legalitatea prelucrării acestora fără întârzieri nejustificate și, în orice caz, în termen de 30 zile de la data la care a fost contactat. Această perioadă poate fi prelungită cu încă 15 zile atunci când este necesar, ținându-se seama de complexitatea și de numărul cererilor. Statul membru responsabil de verificarea manuală a identităților diferite informează statul membru care l-a contactat în ceea ce privește orice astfel de prelungire și motivele întârzierii. Persoana în cauză este informată de statul membru care a contactat autoritatea statului membru responsabil de verificarea manuală a identităților diferite în legătură cu procedura ulterioară.

(4) În cazul în care o cerere de rectificare sau de ștergere a datelor cu caracter personal este adresată unui stat membru în care unitatea centrală ETIAS a fost responsabilă cu verificarea manuală a identităților diferite, statul membru căruia i s-a adresat cererea contactează unitatea centrală ETIAS în termen de șapte zile pentru a-i cere acesteia avizul. Unitatea centrală a ETIAS își prezintă avizul fără întârzieri nejustificate și, în orice caz, în termen de 30 de zile de la contactare. Această perioadă poate fi prelungită cu încă 15 zile atunci când este necesar, ținându-se seama de complexitatea și de numărul cererilor. Persoana vizată este informată de către statul membru care a contactat unitatea centrală ETIAS în legătură cu procedura ulterioară.

(5) În cazul în care, în urma examinării, se constată că datele stocate în MID conțin erori sau au fost înregistrate în mod ilegal, statul membru responsabil cu verificarea manuală a identităților diferite sau, în cazul în care niciun stat membru nu a fost responsabil de verificarea manuală a identităților diferite sau dacă unitatea centrală ETIAS a fost responsabilă de verificarea manuală a identităților diferite, statul membru căruia i s-a adresat cererea rectifică sau șterge datele respective fără întârzieri nejustificate. Persoana în cauză este informată în scris că datele sale au fost rectificate sau șterse.

(6) În cazul în care datele stocate în MID se modifică de către un stat membru responsabil în timpul perioadei lor de păstrare, acel stat membru responsabil desfășoară activitățile de prelucrare prevăzute la articolul 27 și, după caz, la articolul 29 pentru a stabili dacă datele modificate trebuie

▼B

conexate. În cazul în care, în urma prelucrării, nu se obține o concordanță, statul membru respectiv șterge datele din dosarul de confirmare a identității. În cazul în care, în urma prelucrării automate, se obțin una sau mai multe concordanțe, statul membru respectiv creează sau actualizează conexiunea aferentă în conformitate cu dispozițiile relevante din prezentul regulament.

(7) În cazul în care statul membru responsabil cu verificarea manuală a identităților diferite sau, după caz, statul membru căruia i s-a adresat cererea nu este de acord că datele înregistrate în MID conțin erori sau că au fost înregistrate în mod ilegal, acesta adoptă o decizie administrativă prin care persoanei interesate i se explică în scris și fără întârziere motivele pentru care statul membru respectiv nu este dispus să rectifice sau să șteargă datele care o privesc.

(8) În decizia menționată la alineatul (7) i se furnizează persoanei vizate și informații privind posibilitatea de a contesta decizia luată în privința cererii de acces, de rectificare, de ștergere sau de restricționare a prelucrării datelor cu caracter personal și, dacă este cazul, informații cu privire la modalitatea de a depune o plângere sau de a introduce o acțiune la autoritățile sau instanțele judecătorești competente și cu privire la orice asistență de care poate beneficia, inclusiv din partea autorităților de supraveghere.

(9) Cererile de acces, de rectificare, de ștergere sau de restricționare a prelucrării datelor cu caracter personal conțin informațiile necesare pentru a identifica persoana vizată. Aceste informații se utilizează exclusiv pentru a permite exercitarea drepturilor menționate la prezentul articol și apoi se șterg imediat.

(10) Statul membru responsabil cu verificarea manuală a identităților diferite sau, după caz, statul membru căruia i s-a adresat cererea ține o evidență scrisă care să ateste că s-a depus o cerere de acces, de rectificare, de ștergere sau de restricționare a prelucrării datelor cu caracter personal și modul în care a fost soluționată aceasta și pune evidența respectivă, fără întârziere, la dispoziția autorităților de supraveghere.

(11) Prezentul articol nu aduce atingere oricărei limitări și restrângeri a drepturilor prevăzute în prezentul articol în temeiul Regulamentului (UE) 2016/679 și Directivei (UE) 2016/680.

Articolul 49

Portalul web

(1) Se creează un portal web cu scopul de a facilita exercitarea dreptului de acces, de rectificare, de ștergere sau de restricționare a prelucrării datelor cu caracter personal.

(2) Portalul web conține informații privind drepturile și procedurile menționate la articolele 47 și 48 și o interfață cu utilizatorul care permite persoanelor ale căror date sunt prelucrate în MID și care au fost informate cu privire la existența unei legături roșii în conformitate cu articolul 32 alineatul (4) să primească informațiile de contact ale autorității competente a statului membru responsabil de verificarea manuală a identităților diferite.

(3) Pentru a obține datele de contact ale autorității competente a statului membru responsabil de verificarea manuală a identităților diferite, persoana ale cărei date sunt prelucrate în MID ar trebui să introducă o referință la autoritatea responsabilă de verificarea manuală a identităților diferite menționată la articolul 34 litera (d). Portalul web utilizează această referință pentru a obține informațiile de contact ale autorității competente a statului membru responsabil de verificarea manuală a identităților diferite. Portalul web conține, de asemenea, un

▼B

model de e-mail pentru a facilita comunicarea între utilizatorul portalului și autoritatea competentă a statului membru responsabil de verificarea manuală a identităţilor diferite. Acest e-mail trebuie să includă un spaţiu dedicat numărului de identificare unic menţionat la articolul 34 litera (c) pentru a permite autorităţii competente a statului membru responsabil de verificarea manuală a identităţilor diferite să identifice datele în cauză.

(4) Statele membre comunică eu-LISA datele de contact ale tuturor autorităţilor care sunt competente să examineze și să răspundă oricărei cereri menţionate la articolele 47 și 48 și examinează periodic dacă aceste date de contact sunt actualizate.

(5) eu-LISA dezvoltă portalul web și asigură gestionarea tehnică a acestuia.

(6) Comisia adoptă un act delegat în conformitate cu articolul 69 prin care adoptă norme detaliate privind funcţionarea portalului web, inclusiv a interfeţei pentru utilizatori, limbile în care acesta este disponibil și modelul de e-mail.

Articolul 50

Comunicarea datelor cu caracter personal către ţări terţe, organizaţii internaţionale și părţi private

Fără a aduce atingere articolului 31 din Regulamentul (CE) nr. 767/2008, articolelor 25 și 26 din Regulamentul (UE) 2016/794, articolului 41 din Regulamentul (UE) 2017/2226, articolului 65 din Regulamentul (UE) 2018/1240 și efectuării de interogări în bazele de date ale Interpolului prin intermediul ESP în conformitate cu articolul 9 alineatul (5) din prezentul regulament care respectă prevederile de la capitolul V din Regulamentul (UE) 2018/1725 și de la capitolul V din Regulamentul (UE) 2016/679, datele cu caracter personal stocate în componentele de interoperabilitate, prelucrate sau accesate prin intermediul acestora nu se transferă și nu se pun la dispoziţia unei ţări terţe, a unei organizaţii internaţionale sau a unei părţi private.

Articolul 51

Supravegherea de către autorităţile de supraveghere

(1) Fiecare stat membru se asigură că autorităţile de supraveghere monitorizează în mod independent legalitatea prelucrării datelor cu caracter personal în temeiul prezentului regulament de către statul membru în cauză, inclusiv a transmiterii acestora către și de la componentele de interoperabilitate.

(2) Fiecare stat membru se asigură că actele cu putere de lege, reglementările și actele administrative naţionale adoptate în temeiul Directivei (UE) 2016/680 sunt aplicabile, dacă este relevant, accesului autorităţilor poliţienești și autorităţilor desemnate la componentele de interoperabilitate, inclusiv în ceea ce privește drepturile persoanelor ale căror date sunt accesate în acest mod.

▼B

(3) Autorităţile de supraveghere garantează că, cel puţin la fiecare patru ani, se realizează un audit al operaţiunilor de prelucrare a datelor cu caracter personal de către autorităţile naţionale responsabile, în sensul prezentului regulament, în conformitate cu standardele internaţionale de audit relevante.

Autorităţile de supraveghere publică anual numărul solicitărilor de rectificare sau ștergere a datelor cu caracter personal sau de restricţionare a prelucrării datelor cu caracter personal, acţiunile întreprinse ulterior și numărul rectificărilor, ștergerilor și restricţionărilor prelucrării efectuate în urma solicitărilor depuse de persoanele în cauză.

(4) Statele membre se asigură că autorităţile lor de supraveghere au resurse și cunoștinţe suficiente pentru a îndeplini sarcinile care le-au fost încredinţate în temeiul prezentului regulament

(5) Statele membre oferă toate informaţiile solicitate de autoritatea de supraveghere menţionată la articolul 51 alineatul (1) din Regulamentul (UE) 2016/679 și, în special, îi comunică informaţii privind activităţile desfășurate în conformitate cu responsabilităţile lor, în temeiul prezentului regulament. Statele membre acordă autorităţilor de supraveghere menţionate la articolul 51 alineatul (1) din Regulamentul (UE) 2016/679 acces la înregistrările lor menţionate la articolele 10, 16, 24 și 36 din prezentul regulament, la motivele menţionate la articolul 22 alineatul (2) din prezentul regulament și le permit în orice moment accesul în toate localurile proprii utilizate pentru asigurarea interoperabilităţii.

Articolul 52

Auditurile efectuate de Autoritatea Europeană pentru Protecţia Datelor

Autoritatea Europeană pentru Protecţia Datelor garantează că cel puţin o dată la patru ani se realizează un audit al operaţiunilor de prelucrare a datelor cu caracter personal desfășurate de eu-LISA, de unitatea centrală ETIAS și de Europol, în sensul prezentului regulament, în conformitate cu standardele internaţionale de audit relevante. Un raport al acestui audit se trimite Parlamentului European, Consiliului, eu-LISA, Comisiei, statelor membre și agenţiei Uniunii în cauză. eu-LISA, unităţii centrale ETIAS și Europol li se oferă posibilitatea de a face observaţii înainte de adoptarea rapoartelor.

eu-LISA, unitatea centrală a ETIAS și Europol pun la dispoziţia Autorităţii Europene pentru Protecţia Datelor informaţiile solicitate de aceasta, oferă Autorităţii Europene pentru Protecţia Datelor acces la toate documentele solicitate de aceasta și la înregistrările lor menţionate la articolele 10, 16, 24 și 36, precum și la toate localurile proprii, în orice moment.

Articolul 53

Cooperarea dintre autorităţile de supraveghere și Autoritatea Europeană pentru Protecţia Datelor

(1) Autorităţile de supraveghere și Autoritatea Europeană pentru Protecţia Datelor, fiecare acţionând în limitele competenţelor sale, cooperează activ în cadrul responsabilităţilor lor și asigură o supraveghere coordonată a utilizării componentelor de interoperabilitate și

▼B

aplicarea celorlalte dispoziţii ale prezentului regulament, în special dacă Autoritatea Europeană pentru Protecţia Datelor sau o autoritate de supraveghere identifică discrepanţe majore între practicile statelor membre sau transferuri potenţial ilegale efectuate prin canalele de comunicare ale componentelor de interoperabilitate.

(2) În cazurile menţionate la alineatul (1) din prezentul articol, se asigură o supraveghere coordonată în conformitate cu articolul 62 din Regulamentul (UE) 2018/1725.

(3) Comitetul european pentru protecţia datelor transmite Parlamentului European, Consiliului, Comisiei, Europol, Agenţiei Europene pentru Poliţia de Frontieră și Garda de Coastă și eu-LISA un raport comun privind activităţile sale în temeiul prezentului articol, până la 12 iunie 2021 și ulterior din doi în doi ani. Raportul respectiv include un capitol despre fiecare stat membru, elaborat de autoritatea de supraveghere a statului membru în cauză.

CAPITOLUL VIII

Responsabilităţi

Articolul 54

Responsabilităţile eu-LISA în timpul etapei de concepere și dezvoltare

(1) eu-LISA se asigură că infrastructurile centrale ale componentelor de interoperabilitate sunt exploatate în conformitate cu prezentul regulament.

(2) Componentele de interoperabilitate sunt găzduite de eu-LISA în amplasamentele sale tehnice și asigură funcţionalităţile prevăzute în prezentul regulament, în conformitate cu condiţiile de securitate, disponibilitate, calitate și performanţă prevăzute la articolul 55 alineatul (1).

(3) eu-LISA este responsabilă de dezvoltarea componentelor de interoperabilitate, de orice adaptare necesară pentru asigurarea interoperabilităţii între sistemele centrale ale EES, VIS, ETIAS, SIS, Eurodac, ECRIS-TCN și ESP, BMS comun, CIR, MID și CRRS.

Fără a aduce atingere articolului 62, eu-LISA nu are acces la niciuna dintre datele cu caracter personal prelucrate prin intermediul ESP, BMS comun, CIR sau MID.

eu-LISA definește modul în care este concepută arhitectura fizică a componentelor de interoperabilitate, inclusiv infrastructurile acestora de comunicaţii, precum și specificaţiile tehnice și evoluţia acestora în ceea ce privește infrastructura centrală și infrastructura de comunicaţii securizată, care sunt adoptate de către Consiliul de administraţie, sub rezerva unui aviz favorabil din partea Comisiei. De asemenea, eu-LISA pune în aplicare orice adaptare necesară a SIS, Eurodac sau ECRIS-TCN care rezultă din stabilirea interoperabilităţii și este prevăzută de prezentul regulament.

eu-LISA dezvoltă și implementează componentele de interoperabilitate cât mai curând posibil după intrarea în vigoare a prezentului regulament și adoptarea de către Comisie a măsurilor prevăzute la articolul 8 alineatul (2), articolul 9 alineatul (7), articolul 28 alineatele (5) și (7), articolul 37 alineatul (4), articolul 38 alineatul (3), articolul 39 alineatul (5) articolul 43 alineatul (5) și articolul 74 alineatul (10).

Dezvoltarea constă în elaborarea și implementarea specificaţiilor tehnice, efectuarea de teste și gestionarea și coordonarea generală a proiectului.

▼B

(4) În cursul fazei de concepere și dezvoltare se instituie un consiliu de administrație al programului, alcătuit din maximum 10 membri. Acesta este compus din șapte membri numiți de Consiliul de administrație al eu-LISA din rândul membrilor săi sau al membrilor săi supleanți, președintele Grupului consultativ privind interoperabilitatea menționat la articolul 71, un membru care reprezintă eu-LISA numit de directorul executiv al acesteia și un membru numit de Comisie. Membrii numiți de către Consiliul de administrație al eu-LISA sunt aleși numai din statele membre pentru care instrumentele juridice ce reglementează dezvoltarea, instituirea, operarea și utilizarea tuturor sistemelor de informații ale UE prevăd obligații depline în temeiul dreptului Uniunii și care vor participa la componentele de interoperabilitate.

(5) Consiliul de administrație al programului se întrunește periodic și cel puțin de trei ori pe trimestru. Acesta asigură gestionarea adecvată a etapei de concepere și dezvoltare a componentelor de interoperabilitate.

Consiliul de administrație al programului prezintă lunar Consiliului de administrație al eu-LISA rapoarte scrise privind evoluția proiectului. Consiliul de administrație al programului nu are competențe decizionale și nu dispune de un mandat de reprezentare a membrilor Consiliului de administrație al eu-LISA.

(6) Consiliul de administrație al eu-LISA stabilește regulamentul de procedură al Consiliului de administrație al programului, care include în special norme privind:

(a) președinția;

(b) locul reuniunilor;

(c) pregătirea reuniunilor;

(d) accesul experților la reuniuni;

(e) planuri de comunicare care să asigure informarea permanentă și pe deplin a membrilor neparticipanți din cadrul Consiliului de administrație.

Președinția este asigurată de un stat membru pentru care instrumentele juridice care reglementează dezvoltarea, instituirea, operarea și utilizarea tuturor sistemelor de informații ale UE prevăd obligații depline în temeiul dreptului Uniunii și care va participa la componentele de interoperabilitate.

Toate cheltuielile de deplasare și de ședere suportate de membrii Consiliului de administrație al programului sunt plătite de eu-LISA, iar articolul 10 din regulamentul intern al eu-LISA se aplică *mutatis mutandis*. eu-LISA asigură secretariatul Consiliului de administrație al programului.

Grupul consultativ privind interoperabilitatea menționat la articolul 71 se reunește periodic până la punerea în funcțiune a componentelor de interoperabilitate. După fiecare reuniune, grupul consultativ prezintă un raport Consiliului de administrație al programului. Grupul consultativ furnizează expertiză tehnică pentru a asista Consiliul de administrație al programului în îndeplinirea sarcinilor sale și monitorizează stadiul de pregătire a statelor membre.

▼B

Articolul 55

Responsabilităţile eu-LISA după punerea în funcţiune

(1) După punerea în funcţiune a fiecărei componente de interoperabilitate, eu-LISA este responsabilă de gestionarea tehnică a infrastructurii centrale a componentelor de interoperabilitate, inclusiv de întreţinerea acestora și de evoluţiile tehnologice. În cooperare cu statele membre, eu-LISA asigură utilizarea celor mai bune tehnologii disponibile, sub rezerva unei analize costuri-beneficii. eu-LISA este, de asemenea, responsabilă de gestionarea tehnică a infrastructurii de comunicaţii menţionate la articolele 6, 12, 17, 25 și 39.

Gestionarea tehnică a componentelor de interoperabilitate cuprinde toate sarcinile și soluţiile tehnice necesare pentru a menţine în funcţiune componentele de interoperabilitate și asigurând servicii neîntrerupte statelor membre și agenţiilor Uniunii 24 de ore pe zi, 7 zile pe săptămână, în conformitate cu prezentul regulament. Gestionarea tehnică trebuie să includă lucrările de întreţinere și dezvoltările tehnice necesare pentru a se asigura funcţionarea componentelor la un nivel satisfăcător de calitate tehnică, mai ales în ceea ce privește timpul de răspuns pentru efectuarea de căutări în infrastructurile centrale în conformitate cu specificaţiile tehnice.

Toate componentele de interoperabilitate sunt dezvoltate și gestionate astfel încât să se asigure un acces rapid, neîntrerupt, eficient și controlat și o disponibilitate totală și neîntreruptă a componentelor și a datelor stocate în MID, BMS comun și CIR, precum și un timp de răspuns adecvat nevoilor operaţionale ale autorităţilor statelor membre și ale agenţiilor Uniunii.

(2) Fără a aduce atingere articolului 17 din Statutul funcţionarilor Uniunii Europene, eu-LISA aplică norme corespunzătoare privind secretul profesional sau alte obligaţii echivalente de confidenţialitate membrilor personalului său care lucrează cu date stocate în componentele de interoperabilitate. Această obligaţie se aplică și după ce persoanele respective au încetat să mai ocupe o anumită funcţie sau după ce și-au încetat activitatea.

Fără a aduce atingere articolului 62, eu-LISA nu are acces la niciuna dintre datele cu caracter personal prelucrate prin intermediul ESP, BMS comun, CIR și MID.

(3) eu-LISA dezvoltă și întreţine un mecanism și proceduri de verificare a calităţii datelor stocate în BMS comun și în CIR, în conformitate cu articolul 37.

(4) eu-LISA îndeplinește, de asemenea, sarcini legate de asigurarea formării privind utilizarea tehnică a componentelor de interoperabilitate.

Articolul 56

Responsabilităţile statelor membre

(1) Fiecare stat membru este responsabil de:

(a) conectarea la infrastructura de comunicare a ESP și a CIR;

(b) integrarea sistemelor și a infrastructurilor naţionale existente cu ESP, CIR și MID.

▼B

(c) organizarea, gestionarea, operarea și întreținerea infrastructurii naționale existente și de conectarea acesteia la componentele de interoperabilitate;

(d) gestionarea accesului și modalitățile de acces al personalului autorizat din cadrul autorităților naționale competente la ESP, CIR și MID în conformitate cu dispozițiile prezentului regulament, precum și de crearea și actualizarea periodică a unei liste a personalului menționat și a profilurilor acestora;

(e) adoptarea măsurilor legislative menționate la articolul 20 alineatul (5) și (6) pentru a avea acces la CIR în scopuri de identificare;

(f) verificarea manuală a identităților diferite, menționată la articolul 29;

(g) conformitatea cu cerințele de calitate a datelor stabilite în temeiul legislației Uniunii;

(h) respectarea normelor fiecărui sistem de informații al UE privind securitatea și integritatea datelor cu caracter personal;

(i) remedierea oricăror deficiențe identificate în raportul de evaluare privind calitatea datelor efectuat de Comisie și menționat la articolul 37 alineatul (5).

(2) Fiecare stat membru își conectează la CIR autoritățile desemnate.

Articolul 57

Responsabilitățile Europol

(1) Europol asigură prelucrarea interogărilor efectuate prin intermediul ESP în datele Europol. Europol își adaptează interfața sa *Querying Europol Systems* (QUEST) pentru datele cu un nivel de protecție de bază (BPL) în mod corespunzător.

(2) Europol este responsabil de gestionarea utilizării și a accesului și de modalitățile de utilizare și de acces al personalului său autorizat în mod corespunzător la ESP și CIR în temeiul prezentului regulament, precum și de crearea și actualizarea periodică a unei liste a personalului menționat și a profilurilor acestora.

Articolul 58

Responsabilitățile unității centrale a ETIAS

Unitatea centrală a ETIAS este responsabilă de:

(a) verificarea manuală a identităților diferite, în conformitate cu articolul 29;

(b) efectuarea de detectări de identități multiple în datele stocate în EES, VIS, Eurodac și SIS, menționată la articolul 65.

CAPITOLUL IX

Modificarea altor instrumente ale Uniunii

Articolul 59

Modificarea Regulamentului (UE) 2018/1726

Regulamentul (UE) 2018/1726 se modifică după cum urmează:

▼B

1. Articolul 12 se înlocuiește cu următorul text:

„*Articolul 12*

Calitatea datelor

(1) Fără a aduce atingere responsabilităţilor statelor membre în ceea ce privește datele introduse în sisteme sub răspunderea operativă a agenţiei, agenţia, cu implicarea strânsă a grupurilor sale consultative, stabilește, pentru toate sistemele sub răspundere operativă a acesteia, mecanisme și proceduri automatizate de control al calităţii datelor, indicatori comuni de calitate și standardele minime de calitate pentru stocarea datelor, în conformitate cu dispoziţiile relevante ale instrumentelor juridice care guvernează respectivele sisteme de informaţii și cu articolul 37 din Regulamentele (UE) 2019/817 (*) și (UE) 2019/818 (**) ale Parlamentului European și ale Consiliului.

(2) Agenţia instituie un registru central care conţine numai date anonimizate pentru raportare și statistici, în conformitate cu articolul 39 din Regulamentele (UE) 2019/817 și (UE) 2019/818, sub rezerva dispoziţiilor specifice din instrumentele juridice care reglementează dezvoltarea, instituirea, funcţionarea și utilizarea sistemelor informatice la scară largă gestionate de agenţie.

(*) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informaţii ale UE în domeniul frontierelor și al vizelor și de modificare a Regulamentelor (CE) nr. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 și (UE) 2018/1861 ale Parlamentului European și ale Consiliului și a Deciziilor 2004/512/CE și 2008/633/JAI ale Consiliului (JO L 135, 22.5.2019, p. 27).

(**) Regulamentul (UE) 2019/818 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informaţii ale UE în domeniul cooperării poliţienești și judiciare, al azilului și al migraţiei și de modificare a Regulamentelor (UE) 2018/1726, (UE) 2018/1862 și (UE) 2019/816 (JO L 135, 22.5.2019, p. 85).”;

2. La articolul 19, alineatul (1) se modifică după cum urmează:

(a) se introduce următoarea literă:

„(eea) adoptă rapoarte privind stadiul dezvoltării componentelor de interoperabilitate în temeiul articolului 78 alineatul (2) din Regulamentul (UE) 2019/817 și al articolului 74 alineatul (2) din Regulamentul (UE) 2019/818;”;

(b) litera (ff) se înlocuiește cu următorul text:

„(ff) adoptă rapoartele privind funcţionarea tehnică a SIS în temeiul articolului 60 alineatul (7) din Regulamentul (UE) 2018/1861 al Parlamentului European și al Consiliului (*) și al articolului 74 alineatul (8) din Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului (**), a VIS în temeiul articolului 50 alineatul (3) din Regulamentul (CE) nr. 767/2008 și al articolului 17 alineatul (3) din Decizia 2008/633/JHA, a SEE în temeiul articolului 72 alineatul (4) din Regulamentul (UE) 2017/2226, a ETIAS în temeiul articolului 92 alineatul (4) din Regulamentul (UE) 2018/1240, a ECRIS-TCN și a aplicaţiei de referinţă a ECRIS în temeiul articolului 36 alineatul (8) din Regulamentul

▼B

(UE) 2019/816 al Parlamentului European și al Consiliului (***) și a componentelor de interoperabilitate în temeiul articolului 78 alineatul (3) din Regulamentul (UE) 2019/817 și al articolului 74 alineatul (3) din Regulamentul (UE) 2019/818;

(*) Regulamentul (UE) 2018/1861 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcţionarea și utilizarea Sistemului de informaţii Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Convenţiei de punere în aplicare a Acordului Schengen și de modificare și abrogare a Regulamentului (CE) nr. 1987/2006 (JO L 312, 7.12.2018, p. 14).

(**) Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcţionarea și utilizarea Sistemului de informaţii Schengen (SIS) în domeniul cooperării poliţienești și al cooperării judiciare în materie penală, de modificare și abrogare a Deciziei 2007/533/JAI a Consiliului și de abrogare a Regulamentului (CE) nr. 1986/2006 al Parlamentului European și al Consiliului și a Deciziei 2010/261/UE a Comisiei (JO L 312, 7.12.2018, p. 56).

(***) Regulamentul (UE) 2019/816 al Parlamentului European și al Consiliului din 17 aprilie 2019 de stabilire a unui sistem centralizat pentru determinarea statelor membre care deţin informaţii privind condamnările resortisanţilor ţărilor terţe și ale apatrizilor (ECRIS-TCN), destinat să completeze sistemul european de informaţii cu privire la cazierele judiciare și de modificare a Regulamentului (UE) 2018/1726 (JO L 135, 22.5.2019, p. 1).”;

(c) litera (hh) se înlocuiește cu următorul text:

„(hh) adoptă observaţii formale referitoare la rapoartele Autorităţii Europene pentru Protecţia Datelor privind auditurile în temeiul articolului 56 alineatul (2) din Regulamentul (UE) 2018/1861, al articolului 42 alineatul (2) din Regulamentul (CE) nr. 767/2008, al articolului 31 alineatul (2) din Regulamentul (UE) nr. 603/2013, al articolului 56 alineatul (2) din Regulamentul (UE) 2017/2226, al articolului 67 din Regulamentul (UE) 2018/1240, al articolului 29 alineatul (2) din Regulamentul (UE) 2019/816 și al articolului 52 din Regulamentele (UE) 2019/817 și (UE) 2019/818 și asigură luarea de măsuri corespunzătoare prin care să se dea curs recomandărilor formulate în cadrul auditurilor respective;”;

(d) litera (mm) se înlocuiește cu următorul text:

„(mm) asigură publicarea anuală a listei autorităţilor competente autorizate să consulte direct datele introduse în SIS în temeiul articolului 41 alineatul (8) din Regulamentul (UE) 2018/1861 și al articolului 56 alineatul (7) din Regulamentul (UE) 2018/1862, împreună cu lista oficiilor sistemelor naţionale ale SIS (N.SIS) și a birourilor SIRENE în temeiul articolului 7 alineatul (3) din Regulamentul (UE) 2018/1861 și, respectiv, al articolului 7 alineatul (3) din Regulamentul (UE) 2018/1862, precum și lista autorităţilor competente în temeiul articolului 65 alineatul (2) din Regulamentul (UE) 2017/2226, lista autorităţilor competente în temeiul articolului 87 alineatul (2) din Regulamentul (UE) 2018/1240, lista autorităţilor

▼B

centrale în temeiul articolului 34 alineatul (2) din Regulamentul (UE) 2019/816, precum și lista autorităților în temeiul articolului 71 alineatul (1) din Regulamentul (UE) 2019/817 și al articolului 67 alineatul (1) din Regulamentul (UE) 2019/818.”;

3. La articolul 22, alineatul (4) se înlocuiește cu următorul text:

„(4) Europol și Eurojust pot participa la reuniunile consiliului de administrație, în calitate de observatori, atunci când pe ordinea de zi se află o chestiune referitoare la SIS II în legătură cu aplicarea Deciziei 2007/533/JAI.

Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă poate participa la reuniunile Consiliului de administrație, în calitate de observatori, atunci când pe ordinea de zi se află o chestiune referitoare la SIS II în legătură cu punerea în aplicare a Regulamentului (UE) 2016/1624.

Europol poate participa la reuniunile consiliului de administrație, în calitate de observator, atunci când pe ordinea de zi se află o chestiune referitoare la VIS, în legătură cu aplicarea Deciziei 2008/633/JAI sau o chestiune referitoare la Eurodac în legătură cu aplicarea Regulamentului (UE) nr. 603/2013.

Europol poate participa la reuniunile Consiliului de administrație, în calitate de observator, atunci când pe ordinea de zi se află o chestiune referitoare la EES, în legătură cu aplicarea Regulamentului (UE) 2017/2226, sau atunci când pe ordinea de zi se află o chestiune privind ETIAS, în legătură cu Regulamentul (UE) 2018/1240.

Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă poate, participa la reuniunile Consiliului de administrație, în calitate de observator, atunci când pe ordinea de zi se află o chestiune referitoare la ETIAS în legătură cu punerea în aplicare a Regulamentul (UE) 2018/1240.

Eurojust, Europol și Parchetul European pot participa la reuniunile consiliului de administrație, în calitate de observatori, atunci când pe ordinea de zi se află o chestiune referitoare la Regulamentul (UE) 2019/816.

Eurojust, Europol și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă pot participa la reuniunile consiliului de administrație, în calitate de observatori, atunci când pe ordinea de zi se află o chestiune referitoare la Regulamentele (UE) 2019/817 și (UE) 2019/818.

Consiliul de administrație poate invita să participe la reuniuni în calitate de observator orice altă persoană ale cărei opinii pot fi de interes.”;

4. La articolul 24 alineatul (3), litera (p) se înlocuiește cu următorul text:

„(p) fără a aduce atingere articolului 17 din Statutul funcționarilor, stabilirea cerințelor de confidențialitate pentru respectarea articolului 17 din Regulamentul (CE) nr. 1987/2006, a articolului 17 din Decizia 2007/533/JAI, a articolului 26 alineatul (9) din Regulamentul (CE) nr. 767/2008, a articolului 4 alineatul (4) din Regulamentul (UE) nr. 603/2013, a articolului 37 alineatul (4) din Regulamentul (UE) 2017/2226, a articolului 74 alineatul (2) din Regulamentul (UE) 2018/1240, a articolului 11 alineatul (16) din Regulamentul (UE) 2019/816 și a articolului 55 alineatul (2) din Regulamentele (UE) 2019/817 și (UE) 2019/818;”;

5. Articolul 27 se modifică după cum urmează:

▼C1

(a) la alineatul (1), se introduce următoarea literă:

„(db) Grupul consultativ privind interoperabilitatea;”

▼B

(b) alineatul (3) se înlocuiește cu următorul text:

„(3) Europol, Eurojust și Agenţia Europeană pentru Poliţia de Frontieră și Garda de Coastă pot numi fiecare câte un reprezentat în cadrul grupului consultativ privind SIS II.

Europol poate numi, de asemenea, un reprezentant în grupurile consultative privind VIS, Eurodac și EES-ETIAS.

Agenţia Europeană pentru Poliţia de Frontieră și Garda de Coastă poate, de asemenea, să numească un reprezentant în cadrul grupului consultativ EES-ETIAS.

Eurojust, Europol și Parchetul European pot numi fiecare câte un reprezentant în cadrul grupului consultativ ECRIS-TCN.

Europol, Eurojust și Agenţia Europeană pentru Poliţia de Frontieră și Garda de Coastă pot numi fiecare câte un reprezentat în cadrul grupului consultativ privind interoperabilitatea.”

Articolul 60

Modificarea Regulamentului (UE) 2018/1862

Regulamentul (UE) 2018/1862 se modifică după cum urmează:

1. La articolul 3 se adaugă următoarele puncte:

„18. «ESP» înseamnă portalul european de căutare, instituit prin articolul 6 alineatul (1) din Regulamentul (UE) 2019/818 al Parlamentului European și al Consiliului (*);

19. «BMS comun» înseamnă serviciul comun de comparare a datelor biometrice instituit prin articolul 12 alineatul (1) din Regulamentul (UE) 2019/818;

20. «CIR» înseamnă registrul comun de date de identitate instituit prin articolul 17 alineatul (1) din Regulamentul (UE) 2019/818;

21. «MID» înseamnă detectorul de identităţi multiple instituit prin articolul 25 alineatul (1) din Regulamentul (UE) 2019/818;

(*) Regulamentul (UE) 2019/818 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informaţii ale UE în domeniul cooperării polițienești și judiciare, al azilului și al migraţiei și de modificare a Regulamentelor (UE) 2018/1726, (UE) 2018/1862 și (UE) 2019/816 (JO L 135, 22.5.2019, p. 85).”

2. Articolul 4 se modifică după cum urmează:

(a) la alineatul (1), literele (b) și (c) se înlocuiesc cu următorul text:

„(b) un sistem naţional (N.SIS) în fiecare stat membru, care constă în sisteme naţionale de date care comunică cu SIS central, inclusiv cel puţin un N.SIS de rezervă naţional sau comun;

(c) o infrastructură de comunicaţii între CS-SIS, CS-SIS de rezervă și NI-SIS (denumită în continuare „infrastructura de comunicaţii”) care furnizează o reţea virtuală criptată dedicată datelor din SIS și schimbului de date între birourile SIRENE, astfel cum sunt menţionate la articolul 7 alineatul (2); și

(d) o infrastructură de comunicaţii securizată între CS-SIS și infrastructurile centrale ale ESP, BMS comun și MID.”;

▼B

(b) se adaugă următoarele alineate:

„(8) Fără a se aduce atingere alineatelor (1)-(5), datele SIS privind persoanele și documentele de identitate pot fi consultate și prin intermediul ESP.

(9) Fără a se aduce atingere alineatelor (1)-(5), datele SIS privind persoanele și documentele de identitate pot fi transmise și prin intermediul infrastructurii de comunicare securizate menţionate la alineatul (1) litera (d). Aceste transmisii se efectuează numai în măsura în care datele sunt necesare în scopul Regulamentului (UE) 2019/818.”;

3. La articolul 7 se introduce următorul alineat:

„(2a) Birourile SIRENE asigură, de asemenea, verificarea manuală a identităţilor diferite în conformitate cu articolul 29 din Regulamentul (UE) 2019/818. În măsura în care este necesar pentru a îndeplini această sarcină, birourile SIRENE au acces la datele stocate în CIR și în MID în scopurile prevăzute la articolele 21 și 26 din Regulamentul (UE) 2019/818.”;

4. La articolul 12 alineatul (1) se adaugă următorul paragraf:

„Statele membre se asigură că fiecare accesare a datelor cu caracter personal prin intermediul ESP este, de asemenea, înregistrată în scopul verificării legalităţii căutării, al monitorizării legalităţii prelucrării datelor, al automonitorizării și al asigurării integrităţii și securităţii datelor.”;

5. La articolul 44 alineatul (1) se adaugă următoarea literă:

„(f) verificarea identităţilor diferite și combaterea fraudei de identitate în conformitate cu capitolul V din Regulamentul (UE) 2019/818.”;

6. La articolul 74, alineatul (7) se înlocuiește cu următorul text:

„(7) În sensul articolului 15 alineatul (4) și al alineatelor (3), (4) și (6) din prezentul articol, eu-LISA stochează datele menţionate la articolul 15 alineatul (4) și la alineatul (3) din prezentul articol care trebuie să nu permită identificarea persoanelor fizice în registrul central de raportare și statistici menţionat la articolul 39 din Regulamentul (UE) 2019/818.

eu-LISA permite Comisiei și organismelor menţionate la alineatul (6) din prezentul articol să obţină rapoarte și statistici personalizate. La cerere, eu-LISA acordă acces statelor membre, Comisiei, Europol și Agenţiei Europene pentru Poliţia de Frontieră și Garda de Coastă la registrul central de raportare și statistici în conformitate cu articolul 39 din Regulamentul (UE) 2019/818.”

Articolul 61

Modificarea Regulamentului (UE) 2019/816

Regulamentul (UE) 2019/816 se modifică după cum urmează:

1. La articolul 1 se adaugă următoarea literă:

„(c) condiţiile în care ECRIS-TCN contribuie la facilitarea și acordarea de asistenţă în vederea identificării corecte a persoanelor înregistrate în ECRIS-TCN în condiţiile și în

▼B

scopurile de la articolul 20 din Regulamentul (UE) 2019/818 al Parlamentului European și al Consiliului (*), prin stocarea datelor de identitate, a datelor privind documentele de călătorie și a datelor biometrice în CIR.

(*) Regulamentul (UE) 2019/818 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE în domeniul cooperării polițienești și judiciare, al azilului și al migrației și de modificare a Regulamentelor (UE) 2018/1726, (UE) 2018/1862 și (UE) 2019/816 (JO L 135, 22.5.2019, p. 85).”

2. Articolul 2 se înlocuiește cu următorul text:

„*Articolul 2*

Domeniul de aplicare

Prezentul regulament se aplică prelucrării informațiilor privind identitatea resortisanților țărilor terțe care au făcut obiectul unor condamnări în statele membre, cu scopul de a identifica statele membre în care au fost pronunțate aceste condamnări. Cu excepția articolului 5 alineatul (1) litera (b) punctul (ii), dispozițiile prezentului regulament aplicabile resortisanților țărilor terțe se aplică și cetățenilor Uniunii care dețin și cetățenia unei țări terțe și care au făcut obiectul unor condamnări în statele membre. De asemenea, prezentul regulament facilitează și sprijină identificarea corectă a persoanelor în conformitate cu prezentul regulament și cu Regulamentul (UE) 2019/818.”;

3. Articolul 3 se modifică după cum urmează:

(a) punctul 8 se elimină;

(b) se adaugă următoarele puncte:

„19. «CIR» înseamnă registrul comun de date de identitate instituit prin articolul 17 alineatul (1) din Regulamentul (UE) 2019/818;

20. «date din ECRIS-TCN» înseamnă toate datele stocate în sistemul central și în CIR în conformitate cu articolul 5;

21. «ESP» înseamnă portalul european de căutare instituit prin articolul 6 alineatul (1) din Regulamentul (UE) 2019/818.”;

4. La articolul 4, alineatul (1) se modifică după cum urmează:

(a) litera (a) se înlocuiește cu următorul text:

„(a) un sistem central;”;

(b) se introduce următoarea literă:

„(aa) CIR;”;

(c) se adaugă următoarea literă:

„(e) o infrastructură de comunicații între sistemul central și infrastructurile centrale ale ESP și CIR”;

5. Articolul 5 se modifică după cum urmează:

(a) la alineatul (1), teza introductivă se înlocuiește cu următorul text:

▼B

„(1) Pentru fiecare resortisant al unei ţări terţe condamnat, autoritatea centrală a statului membru de condamnare creează un fișier de date în ECRIS-TCN. Fișierul de date include:”;

(b) se introduce următorul alineat:

„1a. CIR conţine datele menţionate la alineatul (1) litera (b) și următoarele date de la alineatul (1) litera (a): numele (de familie), prenumele, data nașterii, locul nașterii (localitatea și ţara), cetăţenia sau cetăţeniile, genul, numele anterioare, dacă este cazul, pseudonimele sau numele de împrumut, dacă sunt disponibile, tipul și numărul documentelor de călătorie ale persoanei și denumirea autorităţii emitente, dacă sunt disponibile. CIR poate conţine și datele menţionate la alineatul (3). Celelalte date ECRIS-TCN sunt stocate în sistemul central.”;

6. Articolul 8 se modifică după cum urmează:

(a) alineatul (1) se înlocuiește cu următorul text:

„(1) Fiecare fișier de date este stocat în sistemul central și în CIR atât timp cât datele referitoare la condamnările persoanei în cauză sunt stocate în cazierele judiciare.”;

(b) alineatul (2) se înlocuiește cu următorul text:

„(2) La expirarea perioadei de păstrare menţionate la alineatul (1), autoritatea centrală din statul membru de condamnare șterge fișierul de date, inclusiv datele dactiloscopice și imaginile faciale din sistemul central al ECRIS-TCN și din CIR. Ștergerea se realizează automat, dacă este posibil, și în orice caz în termen de cel mult o lună de la expirarea perioadei de păstrare.”;

7. Articolul 9 se modifică după cum urmează:

(a) la alineatul (1), cuvântul „ECRIS-TCN” se înlocuiește cu cuvintele „sistemul central și în CIR”;

(b) la alineatele (2), (3) și (4), cuvintele „sistemul central” se înlocuiesc cu cuvintele „sistemul central și în CIR”.

8. La articolul 10 alineatul (1), litera (j) se elimină;

9. La articolul 12 alineatul (2), cuvintele „sistemul central” se înlocuiesc cu cuvintele „sistemul central și în CIR”;

10. La articolul 13 alineatul (2), cuvintele „sistemului central” se înlocuiesc cu cuvintele „sistemului central, a CIR”;

11. La articolul 23 alineatul (2), cuvintele „sistemul central” se înlocuiesc cu cuvintele „sistemul central și în CIR”;

12. Articolul 24 se modifică după cum urmează:

(a) alineatul (1) se înlocuiește cu următorul text:

„(1) Datele introduse în sistemul central și în CIR sunt prelucrate exclusiv în scopul identificării statelor membre care deţin informaţii privind cazierele judiciare ale resortisanţilor ţărilor terţe. Datele introduse în CIR se prelucrează, de asemenea, în conformitate cu Regulamentul (UE) 2019/818 în scopul facilitării și sprijinirii identificării corecte a persoanelor înregistrate în ECRIS-TCN în conformitate cu prezentul regulament.”;

▼B

(b) se adaugă următorul alineat:

„(3) Fără a aduce atingere alineatului (2), accesul în vederea consultării datelor stocate în CIR este rezervat, de asemenea, personalului autorizat în mod corespunzător din cadrul autorităţilor naţionale din fiecare stat membru și personalului autorizat în mod corespunzător din cadrul agenţiilor Uniunii cu competenţe în scopurile prevăzute la articolele 20 și 21 din Regulamentul (UE) 2019/818. Acest acces este limitat la măsura în care datele sunt necesare pentru îndeplinirea sarcinilor lor în scopurile menţionate și este proporţional cu obiectivele urmărite.”;

13. La articolul 32, alineatul (2) se înlocuiește cu următorul text:

„(2) În sensul alineatului (1) din prezentul articol, eu-LISA stochează datele menţionate la alineatul respectiv în registrul central de raportare și statistici menţionat la articolul 39 din Regulamentul (UE) 2019/818.”;

14. La articolul 33 alineatul (1), cuvintele „sistemului central” se înlocuiesc cu cuvintele „sistemului central, CIR și”.

15. La articolul 41, alineatul (2) se înlocuiește cu următorul text:

„(2) Pentru condamnări pronunţate înainte de data începerii introducerii datelor în conformitate cu articolul 35 alineatul (1), autorităţile centrale creează fișiere individuale de date în sistemul central și în CIR după cum urmează:

(a) datele alfanumerice sunt introduse în sistemul central și în CIR până la sfârșitul perioadei menţionate la articolul 35 alineatul (2);

(b) datele dactiloscopice sunt introduse în sistemul central și în CIR în termen de doi ani de la punerea în funcţiune în conformitate cu articolul 35 alineatul (4).”

CAPITOLUL IX

Dispoziţii finale

Articolul 62

Întocmirea de rapoarte și de statistici

(1) Personalul autorizat în mod corespunzător din cadrul autorităţilor competente ale statelor membre, din cadrul Comisiei și al eu-LISA are acces pentru a consulta, exclusiv în scopul întocmirii de rapoarte și statistici, numărul de interogări per profil de utilizator ESP.

Datele trebuie să nu permită identificarea persoanelor fizice.

(2) Personalul autorizat în mod corespunzător din cadrul autorităţilor competente ale statelor membre, din cadrul Comisiei și al eu-LISA are acces pentru a consulta următoarele date referitoare la CIR, exclusiv în scopul întocmirii de rapoarte și statistici:

(a) numărul de interogări lansate în sensul articolelor 20, 21 și 22;

▼B

(b) cetățenia, genul și anul nașterii persoanei;

(c) tipul documentului de călătorie, inclusiv codul din trei litere al țării emitente;

(d) numărul de căutări efectuate cu și fără date biometrice.

Datele trebuie să nu permită identificarea persoanelor fizice.

(3) Personalul autorizat în mod corespunzător din cadrul autorităţilor competente ale statelor membre, din cadrul Comisiei și al eu-LISA are acces pentru a consulta următoarele date referitoare la MID, exclusiv în scopul întocmirii de rapoarte și statistici:

(a) numărul de căutări efectuate cu și fără date biometrice.

(b) numărul de conexiuni stabilite, în funcţie de tip, și sistemele de informaţii ale UE care conţin datele conexate;

(c) cât timp a rămas în sistem o conexiune galbenă sau roșie.

Datele trebuie să nu permită identificarea persoanelor fizice.

(4) Personalul autorizat în mod corespunzător din cadrul Agenţiei Europene pentru Poliţia de Frontieră și Garda de Coastă are acces pentru a consulta datele menţionate la alineatele (1), (2) și (3) din prezentul articol în scopul de a efectua analize de risc și evaluări ale vulnerabilităţii, astfel cum se menţionează la articolele 11 și 13 din Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului ([9]).

(5) Personalul autorizat în mod corespunzător al Europol are acces pentru a consulta datele menţionate la alineatele (2) și (3) din prezentul articol în scopul de a efectua analize strategice, tematice și operaţionale, astfel cum se menţionează la articolul 18 alineatul (2) literele (b) și (c) din Regulamentul (UE) 2016/794.

(6) În sensul alineatelor (1), (2) și (3), eu-LISA stochează datele menţionate la alineatele respective în CRRS. Datele incluse în CRRS trebuie să nu permită identificarea persoanelor fizice, dar permit autorităţilor enumerate la alineatele (1), (2) și (3) să obţină rapoarte și statistici adaptabile pentru a spori eficienţa verificărilor la frontieră, a sprijini autorităţile să prelucreze cererile de viză și a sprijini elaborarea de politici bazate pe date concrete în materie de migraţie și de securitate în Uniune.

(7) La cerere, Comisia îi pune la dispoziţie Agenţiei pentru Drepturi Fundamentale a Uniunii Europene informaţii relevante pentru a evalua impactul prezentului regulament asupra drepturilor fundamentale.

Articolul 63

Perioada de tranziţie pentru utilizarea portalului european de căutare

(1) Pentru o perioadă de doi ani de la data punerii în funcţiune a ESP, obligaţiile menţionate la articolul 7 alineatele (2) și (4) nu se aplică, iar utilizarea ESP este opţională.

([9]) Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului din 14 septembrie 2016 privind Poliția de frontieră și garda de coastă la nivel european și de modificare a Regulamentului (UE) 2016/399 al Parlamentului European și al Consiliului și de abrogare a Regulamentului (CE) nr. 863/2007 al Parlamentului European și al Consiliului, a Regulamentului (CE) nr. 2007/2004 al Consiliului și a Deciziei 2005/267/CE a Consiliului (JO L 251, 16.9.2016, p. 1).

▼B

(2) Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 69 pentru a modifica prezentul regulament prin prelungirea, o singură dată, a perioadei menţionate la alineatul (1) din prezentul articol, cu maximum un an, atunci când o evaluare a punerii în aplicare a ESP a arătat că o astfel de prelungire este necesară, în special având în vedere impactul pe care l-ar avea punerea în funcţiune a ESP asupra organizării și duratei verificărilor la frontiere.

Articolul 64

Perioada de tranziţie aplicabilă dispoziţiilor privind accesul la registrul comun de date de identitate în scopul prevenirii, depistării sau anchetării infracţiunilor de terorism sau a altor infracţiuni grave

Articolul 22 se aplică de la data punerii în funcţiune a CIR menţionată la articolul 68 alineatul (3).

Articolul 65

Perioada de tranziţie aplicabilă detectorului de identităţi multiple

(1) Pentru o perioadă de un an de la notificarea de către eu-LISA a încheierii perioadei de testare a MID menţionate la articolul 68 alineatul (4) litera (b) și înainte de punerea în funcţiune a MID, unitatea centrală a ETIAS este responsabilă de efectuarea unei detectări de identităţi multiple utilizând datele stocate în EES, VIS, Eurodac și SIS. Detectarea identităţilor multiple se efectuează folosind exclusiv date biometrice.

(2) În cazul în care, în urma interogărilor, se obţin una sau mai multe concordanţe și datele de identitate din dosarele conexate sunt aceleași sau similare, se stabilește o conexiune albă în conformitate cu articolul 33.

În cazul în care, în urma interogărilor, se obţin una sau mai multe concordanţe și datele de identitate ale dosarelor astfel conexate nu pot fi considerate similare, se stabilește o conexiune galbenă în conformitate cu articolul 30 și se aplică procedura prevăzută la articolul 29.

În cazul în care se obţin mai multe concordanţe, se stabilește o conexiune între fiecare componentă a datelor care a generat corespondenţa.

(3) În cazul în care se stabilește o conexiune galbenă, MID acordă acces unităţii centrale a ETIAS la datele de identitate existente în diferitele sisteme de informaţii ale UE.

(4) În cazul în care se stabilește o conexiune cu o semnalare din SIS, alta decât o semnalare creată în temeiul articolului 3 din Regulamentul (UE) 2018/1860, al articolelor 24 și 25 din Regulamentul (UE) 2018/1861 sau al articolului 38 din Regulamentul (UE) 2018/1862, MID acordă acces biroului SIRENE din statul membru care a creat semnalarea la datele de identitate existente în diferitele sisteme de informaţii.

(5) Unitatea centrală a ETIAS sau, în cazurile menţionate la alineatul (4) din prezentul articol, biroul SIRENE din statul membru care a creat semnalarea are acces la datele conţinute în dosarul de confirmare a identităţii, analizează identităţile diferite și actualizează conexiunea în conformitate cu articolele 31, 32 și 33, adăugând-o la dosarul de confirmare a identităţii.

▼B

(6) Unitatea centrală a ETIAS informează Comisia în conformitate cu articolul 67 alineatul (3) numai după ce toate conexiunile galbene au fost verificate manual, iar statutul lor a fost actualizat în conexiuni verzi, albe sau roșii.

(7) În cazul în care este necesar, statele membre acordă asistență unității centrale a ETIAS în vederea detectării identităților multiple în temeiul prezentului articol.

(8) Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 69 pentru a modifica prezentul regulament prin extinderea cu șase luni a perioadei menționate la alineatul (1) din prezentul articol, care poate fi prelungită de două ori cu câte șase luni. O astfel de prelungire se acordă numai în urma unei evaluări a timpului estimat pentru finalizarea detectării identităților multiple în temeiul prezentului articol, care demonstrează că, din motive independente de unitatea centrală a ETIAS, detectarea identităților multiple nu se poate finaliza înainte de expirarea perioadei rămase în temeiul alineatului (1) din prezentul articol sau al unei prelungiri în curs și că nu se pot aplica măsuri corective. Evaluarea se efectuează cel târziu cu trei luni înainte de expirarea acestei perioade sau a prelungirii în curs.

Articolul 66

Costuri

(1) Costurile aferente instituirii și funcționării ESP, a BMS comun, a CIR și a MID sunt suportate din bugetul general al Uniunii.

(2) Costurile aferente integrării infrastructurilor naționale existente și conectării lor la interfețele uniforme naționale, precum și cele aferente găzduirii interfețelor uniforme naționale sunt suportate din bugetul general al Uniunii.

Sunt excluse următoarele costuri:

(a) costurile aferente biroului de gestionare a proiectelor de către statele membre (reuniuni, misiuni, spații de lucru);

(b) costurile aferente găzduirii sistemelor IT naționale (spații, implementare, electricitate, răcire);

(c) costurile aferente operării sistemelor IT naționale (operatori și contracte de sprijin);

(d) costurile aferente conceperii, dezvoltării, implementării, funcționării și întreținerii rețelelor naționale de comunicații.

(3) Fără a exclude finanțarea suplimentară în acest scop din alte surse ale bugetului general al Uniunii Europene, se mobilizează o sumă de 32 077 000 EUR din pachetul financiar de 791 000 000 EUR prevăzut în temeiul articolului 5 alineatul (5) litera (b) din Regulamentul (UE) nr. 515/2014 pentru a acoperi costurile de punere în aplicare a prezentului regulament, astfel cum se prevede la alineatele (1) și (2) din prezentul articol.

(4) Din pachetul menționat la alineatul (3), 22 861 000 EUR se alocă eu-LISA, 9 072 000 EUR se alocă Europol, iar 144 000 EUR se alocă Agenției Uniunii Europene pentru Formare în Materie de Aplicare a Legii (CEPOL), pentru a sprijini aceste agenții să își îndeplinească sarcinile în temeiul prezentului regulament. Această finanțare este mobilizată în gestiune indirectă.

▼B

(5) Costurile aferente autorităţilor desemnate sunt suportate în mod corespunzător de către fiecare stat membru de desemnare. Costurile aferente conectării fiecărei autorităţi desemnate la CIR sunt suportate de către fiecare stat membru.

Costurile aferente Europol, inclusiv cele aferente conectării la CIR, sunt suportate de Europol.

Articolul 67

Notificări

(1) Statele membre notifică eu-LISA autorităţile menţionate la articolele 7, 20, 21 și 26 care pot utiliza sau avea acces la ESP, CIR și, respectiv, MID.

O listă consolidată a acestor autorităţi se publică în *Jurnalul Oficial al Uniunii Europene* în termen de trei luni de la data punerii în funcţiune a fiecărei componente de interoperabilitate în conformitate cu articolul 68. În cazul în care lista este modificată, eu-LISA publică o actualizare consolidată a acesteia o dată pe an.

(2) eu-LISA notifică Comisiei finalizarea cu succes a testării menţionate la articolul 68 alineatul (1) litera (b), alineatul (2) litera (b), alineatul (3) litera (b), alineatul (4) litera (b), alineatul (5) litera (b) și alineatul (6) litera (b).

(3) Unitatea centrală a ETIAS notifică Comisiei încheierea cu succes a perioadei de tranziţie prevăzute la articolul 65.

(4) Comisia pune la dispoziţia statelor membre și a publicului, prin intermediul unui site web public actualizat în permanenţă, informaţiile notificate în temeiul alineatului (1).

Articolul 68

Punerea în funcţiune

(1) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care ESP trebuie să fie pus în funcţiune, odată ce sunt îndeplinite următoarele condiţii:

(a) au fost adoptate măsurile menţionate la articolul 8 alineatul (2), articolul 9 alineatul (7) și articolul 43 alineatul (5);

(b) eu-LISA a notificat finalizarea cu succes a unei testări complete a ESP, pe care a efectuat-o în cooperare cu autorităţile statelor membre și cu agenţiile Uniunii care pot folosi ESP;

(c) eu-LISA a validat modalităţile tehnice și juridice de colectare și transmitere a datelor menţionate la articolul 8 alineatul (1) și a notificat aceste modalităţi Comisiei.

ESP efectuează interogări în bazele de date ale Interpol numai odată ce condiţiile tehnice permit respectarea articolului 9 alineatul (5). Dacă nu se poate asigura respectarea articolului 9 alineatul (5), ESP nu efectuează interogări în bazele de date ale Interpol, însă acest lucru nu întârzie punerea în funcţiune a ESP.

Comisia stabilește data menţionată la primul paragraf ca fiind o dată din intervalul de 30 de zile de la data adoptării actului de punere în aplicare.

▼M1

(1a) Fără a aduce atingere alineatului (1) din prezentul articol, ESP își începe funcţionarea, în scopul prelucrării automate în temeiul articolelor 9a și 22b din Regulamentul (CE) nr. 767/2008, doar de la data

▼M1

începerii activității VIS în temeiul articolului 11 din Regulamentul (UE) 2021/1134 al Parlamentului European și al Consiliului ([10]).

▼M3

(1b) Fără a aduce atingere alineatului (1) de la prezentul articol, ESP este pus în funcțiune, în scopurile efectuării de verificări automate doar în temeiul articolului 20, al articolului 23, al articolului 24 alineatul (6) litera (c) punctul (ii), al articolului 41 și al articolului 54 alineatul (1) litera (b) din Regulamentul (UE) 2018/1240, după ce sunt îndeplinite condițiile prevăzute la articolul 88 din regulamentul menționat.

▼B

(2) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care începe să funcționeze BMS comun, odată ce sunt îndeplinite următoarele condiții:

(a) au fost adoptate măsurile menționate la articolul 13 alineatul (5) și articolul 43 alineatul (5);

(b) eu-LISA a notificat finalizarea cu succes a unei testări complete a BMS comun, pe care a efectuat-o în cooperare cu autoritățile statelor membre;

(c) eu-LISA a validat modalitățile tehnice și juridice de colectare și transmitere a datelor menționate la articolul 13 și le-a notificat Comisiei;

(d) eu-LISA a notificat finalizarea cu succes a testării menționate la alineatul (5) litera (b).

Comisia stabilește data menționată la primul paragraf ca fiind o dată din intervalul de 30 de zile de la data adoptării actului de punere în aplicare.

(3) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care începe să funcționeze CIR, odată ce sunt îndeplinite următoarele condiții:

(a) au fost adoptate măsurile menționate la articolul 43 alineatul (5) și la articolul 74 alineatul (10);

(b) eu-LISA a notificat finalizarea cu succes a unei testări complete a CIR, pe care a efectuat-o în cooperare cu autoritățile statelor membre;

(c) eu-LISA a validat modalitățile tehnice și juridice de colectare și transmitere a datelor menționate la articolul 18 și le-a notificat Comisiei;

(d) eu-LISA a notificat finalizarea cu succes a testării menționate la alineatul (5) litera (b).

Comisia stabilește data menționată la primul paragraf ca fiind o dată din intervalul de 30 de zile de la data adoptării actului de punere în aplicare.

(4) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care începe să funcționeze MID, odată ce sunt îndeplinite următoarele condiții:

(a) au fost adoptate măsurile menționate la articolul 28 alineatele (5) și (7), articolul 32 alineatul (5), articolul 33 alineatul (6), articolul 43 alineatul (5) și articolul 49 alineatul (6);

(b) eu-LISA a notificat finalizarea cu succes a unei testări complete a MID, pe care a efectuat-o în cooperare cu autoritățile statelor membre și cu unitatea centrală a ETIAS;

(c) eu-LISA a validat modalitățile tehnice și juridice de colectare și transmitere a datelor menționate la articolul 34 și a notificat aceste modalități Comisiei;

([10]) Regulamentul (UE) 2021/1134 al Parlamentului European și al Consiliului din 7 iulie 2021 de modificare a Regulamentelor (CE) nr. 767/2008, (CE) nr. 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 și (UE) 2019/1896 ale Parlamentului European și ale Consiliului și de abrogare a Deciziilor 2004/512/CE și 2008/633/JAI ale Consiliului, în scopul reformării Sistemului de informații privind vizele (JO L 248, 13.7.2021, p. 11).

▼B

(d) unitatea centrală a ETIAS a trimis Comisiei notificarea în conformitate cu articolul 67 alineatul (3);

(e) eu-LISA a notificat finalizarea cu succes a testării menţionate la alineatul (1) litera (b), alineatul (2) litera (b), alineatul (3) litera (b) și alineatul (4) litera (b).

Comisia stabilește data menţionată la primul paragraf ca fiind o dată din intervalul de 30 de zile de la data adoptării actului de punere în aplicare.

(5) Comisia stabilește, prin intermediul unor acte de punere în aplicare, data de la care urmează să fie utilizate mecanismele și procedurile automatizate de control al calităţii datelor, indicatorii comuni de calitate a datelor și standardele minime de calitate a datelor, odată ce sunt îndeplinite următoarele condiţii:

(a) au fost adoptate măsurile menţionate la articolul 37 alineatul (4);

(b) eu-LISA a notificat finalizarea cu succes a unei testări complete a mecanismelor și procedurilor automatizate de control al calităţii datelor, a indicatorilor comuni de calitate a datelor și a standardelor minime de calitate a datelor, pe care a efectuat-o în cooperare cu autorităţile statelor membre.

Comisia stabilește data menţionată la primul paragraf se stabilește ca fiind o dată din intervalul de 30 de zile de la data adoptării actului de punere în aplicare.

(6) Comisia stabilește, prin intermediul unui act de punere în aplicare, data de la care începe să funcţioneze CRRS, odată ce sunt îndeplinite următoarele condiţii:

(a) au fost adoptate măsurile menţionate la articolul 39 alineatul (5) și articolul 43 alineatul (5);

(b) eu-LISA a notificat finalizarea cu succes a unei testări complete a CRRS, pe care a efectuat-o în cooperare cu autorităţile statelor membre;

(c) eu-LISA a validat modalităţile tehnice și juridice de colectare și transmitere a datelor menţionate la articolul 39 și a notificat aceste modalităţi Comisiei.

Comisia stabilește data menţionată la primul paragraf ca fiind o dată din intervalul de 30 de zile de la data adoptării actului de punere în aplicare.

(7) Comisia informează Parlamentul European și Consiliul cu privire la rezultatele testelor realizate în temeiul alineatului (1) litera (b), al alineatului (2) litera (b), al alineatului (3) litera (b), al alineatului (4) litera (b), al alineatului (5) litera (b), și al alineatului (6) litera (b).

(8) Statele membre, unitatea centrală a ETIAS și Europol încep să utilizeze fiecare dintre componentele de interoperabilitate de la data stabilită de Comisie în conformitate cu alineatele (1), (2), (3) și, respectiv, (4).

Articolul 69

Exercitarea delegării de competenţe

(1) Competenţa de a adopta acte delegate este conferită Comisiei în condiţiile prevăzute la prezentul articol.

(2) Competenţa de a adopta acte delegate menţionată la articolul 28 alineatul (5), articolul 39 alineatul (5), articolul 49 alineatul (6), articolul 63 alineatul (2) și articolul 65 alineatul (8) se conferă Comisiei pe o perioadă de cinci ani de la data de 11 iunie 2019. Comisia elaborează un raport privind delegarea de competenţe cu cel puţin nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competenţe se prelungește tacit cu perioade de timp identice, cu excepţia cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puţin trei luni înainte de încheierea fiecărei perioade.

▼B

(3) Delegarea de competenţe menţionată la articolul 28 alineatul (5), articolul 39 alineatul (5), articolul 49 alineatul (6), articolul 63 alineatul (2) și articolul 65 alineatul (8) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competenţe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menţionată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) Înainte de adoptarea unui act delegat, Comisia consultă experţii desemnaţi de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituţional din 13 aprilie 2016 privind o mai bună legiferare.

(5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(6) Un act delegat adoptat în temeiul articolului 28 alineatul (5), al articolului 39 alineatul (5), al articolului 49 alineatul (6), al articolului 63 alineatul (2) și al articolului 65 alineatul (8) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecţii în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu, sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecţii. Respectivul termen se prelungește cu două luni la iniţiativa Parlamentului European sau a Consiliului.

Articolul 70

Procedura comitetului

(1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înţelesul Regulamentului (UE) nr. 182/2011.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

În cazul în care comitetul nu emite un aviz, Comisia nu adoptă proiectul de act de punere în aplicare și se aplică articolul 5 alineatul (4) al treilea paragraf din Regulamentul (UE) nr. 182/2011.

Articolul 71

Grupul consultativ

eu-LISA instituie un grup consultativ privind interoperabilitatea. În faza de concepere și dezvoltare a componentelor de interoperabilitate, se aplică articolul 54 alineatele (4), (5) și (6).

Articolul 72

Formare

eu-LISA îndeplinește atribuţii legate de furnizarea de cursuri de formare privind utilizarea tehnică a componentelor de interoperabilitate în conformitate cu Regulamentul (UE) 2018/1726.

Autorităţile statelor membre și agenţiile Uniunii îi oferă personalului lor autorizat să prelucreze date utilizând componentele de interoperabilitate programe adecvate de formare legate de securitatea datelor, calitatea

▼B

datelor, normele de protecţie a datelor, procedurile aplicabile prelucrării datelor și obligaţiile de informare în temeiul articolului 32 alineatul (4), al articolului 33 alineatul (4) și al articolului 47.

Dacă este cazul, se organizează la nivelul Uniunii cursuri comune de formare pe aceste teme, pentru a intensifica cooperarea și schimbul de bune practici între personalul autorităţilor statelor membre și cel al agenţiilor Uniunii care sunt autorizate să prelucreze date utilizând componentele de interoperabilitate. Se acordă o atenţie deosebită procesului de detectare a identităţilor multiple, inclusiv verificării manuale a identităţilor diferite și nevoii aferente de a oferi garanţii adecvate de protecţie a drepturilor fundamentale.

Articolul 73

Manual practic

Comisia, în strânsă cooperare cu statele membre, cu eu-LISA și cu alte agenţii relevante ale Uniunii, pune la dispoziţie un manual practic pentru implementarea și gestionarea componentelor de interoperabilitate. Manualul practic furnizează orientări, recomandări și bune practici de natură tehnică și operaţională. Comisia adoptă manualul sub forma unei recomandări.

Articolul 74

Monitorizare și evaluare

(1) eu-LISA se asigură că există proceduri pentru a monitoriza dezvoltarea componentelor de interoperabilitate și conectarea lor la interfaţa uniformă naţională din perspectiva obiectivelor legate de planificare și costuri și pentru a monitoriza funcţionarea componentelor de interoperabilitate din perspectiva obiectivelor legate de rezultatele tehnice, de raportul cost-eficacitate, de securitate și de calitatea serviciilor.

(2) Până la 12 decembrie 2019 și, ulterior, la fiecare șase luni în etapa de dezvoltare a componentelor de interoperabilitate, eu-LISA prezintă Parlamentului European și Consiliului un raport privind situaţia dezvoltării componentelor de interoperabilitate și legătura lor cu interfaţa uniformă naţională. După încheierea fazei de dezvoltare, se transmite Parlamentului European și Consiliului un raport în care se explică în detaliu modul în care au fost îndeplinite obiectivele, în special obiectivele legate de planificare și costuri, și în care se justifică eventualele abateri.

(3) După patru ani de la punerea în funcţiune a fiecărei componente de interoperabilitate în conformitate cu articolul 68 și, ulterior, o dată la patru ani, eu-LISA prezintă Parlamentului European, Consiliului și Comisiei un raport privind funcţionarea tehnică a componentelor de interoperabilitate, inclusiv în ceea ce privește securitatea acestora.

(4) În plus, la un an după fiecare raport prezentat de eu-LISA, Comisia realizează o evaluare generală a componentelor de interoperabilitate, inclusiv:

(a) o analiză a aplicării prezentului regulament;

▼B

(b) o examinare a rezultatelor obţinute în raport cu obiectivele prezentului regulament și a impactului asupra drepturilor fundamentale, inclusiv și mai ales o evaluare a impactului componentelor de interoperabilitate asupra dreptului la nediscriminare;

(c) o evaluare a funcţionării portalului web, inclusiv cifre privind utilizarea portalului web și numărul de cereri soluţionate;

(d) o analiză a valabilităţii în continuare a raţionamentului care stă la baza componentelor de interoperabilitate;

(e) o evaluare a securităţii componentelor de interoperabilitate;

(f) o evaluare a utilizării CIR pentru identificare;

(g) o evaluare a utilizării CIR pentru prevenirea, depistarea sau anchetarea infracţiunilor de terorism sau a altor infracţiuni grave;

(h) o evaluare a eventualelor implicaţii, inclusiv a impactului disproporţionat asupra fluidităţii traficului la punctele de trecere a frontierelor și a implicaţiilor cu un impact bugetar asupra bugetului general al Uniunii;

(i) o evaluare a căutării în bazele de date ale Interpolului prin intermediul ESP, inclusiv informaţii privind numărul de concordanţe în bazele de date ale Interpolului și informaţii despre orice problemă apărută;

Evaluarea generală realizată în temeiul primului paragraf de la prezentul alineat cuprinde orice recomandări necesare. Comisia transmite evaluarea Parlamentului European, Consiliului, Autorităţii Europene pentru Protecţia Datelor și Agenţiei pentru Drepturi Fundamentale a Uniunii Europene.

(5) Până la 12 iunie 2020 și, ulterior, în fiecare an până când Comisia adoptă actele de punere în aplicare menţionate la articolul 68, Comisia prezintă Parlamentului European și Consiliului un raport privind situaţia pregătirilor pentru a pune pe deplin în aplicare prezentul regulament. Raportul conţine și informaţii detaliate cu privire la costurile aferente și la orice risc care poate afecta costurile totale.

(6) La doi ani de la punerea în funcţiune a MID în conformitate cu articolul 68 alineatul (4), Comisia examinează impactul MID asupra dreptului la nediscriminare. După acest prim raport, examinarea impactului MID asupra dreptului la nediscriminare face parte din examinarea menţionată la alineatul (4) litera (b) din prezentul articol.

(7) Statele membre și Europolul furnizează eu-LISA și Comisiei informaţiile necesare pentru redactarea rapoartelor menţionate la alineatele (3)-(6). Aceste informaţii nu afectează metodele de lucru și nici nu includ date care dezvăluie sursele, membrii personalului sau investigaţiile autorităţilor desemnate.

(8) eu-LISA furnizează Comisiei informaţiile necesare pentru realizarea evaluării generale menţionate la alineatul (4).

▼B

(9) Respectând dispoziţiile dreptului intern referitoare la publicarea informaţiilor sensibile și fără a aduce atingere limitărilor necesare pentru protejarea securităţii și a ordinii publice, prevenirea infracţiunilor și a garanta că nicio anchetă naţională nu va fi pusă în pericol, fiecare stat membru și Europol întocmesc rapoarte anuale privind eficacitatea accesului la datele stocate în CIR în scopul prevenirii, depistării sau investigării infracţiunilor de terorism sau a altor infracţiuni grave care conţin informaţii și statistici privind:

(a) scopul exact al consultărilor, inclusiv tipurile de infracţiuni de terorism sau de alte infracţiuni grave;

(b) motivele întemeiate invocate în sprijinul suspiciunii justificate că suspectul, autorul sau victima intră sub incidenţa Regulamentului (UE) nr. 603/2013;

(c) numărul solicitărilor de acces la CIR în scopul prevenirii, depistării sau anchetării infracţiunilor de terorism sau a altor infracţiuni grave;

(d) numărul și tipurile de cazuri finalizate cu identificări reușite;

(e) necesitatea și utilizarea excepţiei justificate de urgenţă, precum și cazurile în care urgenţa respectivă nu a fost acceptată în urma verificării ex-post efectuate de punctul central de acces.

Rapoartele anuale elaborate de statele membre și de Europol se transmit Comisiei până la data de 30 iunie a anului următor.

(10) Statelor membre li se pune la dispoziţie o soluţie tehnică pentru a gestiona cererile de acces ale utilizatorilor menţionate la articolul 22 și a facilita colectarea informaţiilor în temeiul alineatelor (7) și (9) din prezentul articol, în scopul generării rapoartelor și statisticilor menţionate la alineatele respective. Comisia adoptă acte de punere în aplicare pentru a stabili specificaţiile soluţiei tehnice. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 70 alineatul (2).

Articolul 75

Intrarea în vigoare și aplicabilitatea

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Dispoziţiile prezentului regulament referitoare la ESP se aplică de la data stabilită de Comisie în conformitate cu articolul 68 alineatul (1).

Dispoziţiile prezentului regulament referitoare la BMS comun se aplică de la data stabilită de Comisie în conformitate cu articolul 68 alineatul (2).

Dispoziţiile prezentului regulament referitoare la CIR se aplică de la data stabilită de Comisie în conformitate cu articolul 68 alineatul (3).

Dispoziţiile prezentului regulament referitoare la MID se aplică de la data stabilită de Comisie în conformitate cu articolul 68 alineatul (4).

▼B

Dispoziţiile prezentului regulament referitoare la mecanismele și procedurile automatizate de control al calităţii datelor, indicatorii comuni de calitate a datelor și standardele minime de calitate a datelor se aplică de la datele corespunzătoare stabilite de Comisie în conformitate cu articolul 68 alineatul (5).

Dispoziţiile prezentului regulament referitoare la CRRS se aplică de la data stabilită de Comisie în conformitate cu articolul 68 alineatul (6).

Articolele 6, 12, 17, 25, 38, 42, 54, 56, 58, 66, 67, 69, 70, 71, 73 și articolul 74 alineatul (1) se aplică de la 11 iunie 2019.

Prezentul regulament se aplică în privinţa Eurodac de la data la care se aplică reformarea Regulamentului (UE) nr. 603/2013.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în statele membre în conformitate cu tratatele.