Jurnalul Oficial al Uniunii Europene

L 135

Anul 62

Ediția în limba română **Legislație** 22 mai 2019

Cuprins

RO

Actele ale căror titluri sunt tipărite cu caractere drepte sunt acte de gestionare curentă adoptate în cadrul politicii agricole și care au, în general, o perioadă de valabilitate limitată.

Titlurile celorlalte acte sunt tipărite cu caractere aldine și sunt precedate de un asterisc.

I

(Acte legislative)

REGULAMENTE

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 dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor (ECRIS-TCN), destinat să completeze sistemul european de informații cu privire la cazierele judiciare, și de modificare a Regulamentului (UE) 2018/1726

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 82 alineatul (1) al doilea paragraf litera (d),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

hotărând în conformitate cu procedura legislativă ordinară ([1]),

întrucât:

(1) Uniunea și-a stabilit obiectivul de a oferi cetățenilor săi un spațiu de libertate, securitate și justiție fără frontiere interne, în interiorul căruia este asigurată libera circulație a persoanelor. Obiectivul respectiv ar trebui să se realizeze, printre altele, prin intermediul unor măsuri adecvate de prevenire și combatere a criminalității, inclusiv a criminalității organizate și a terorismului.

(2) Obiectivul menționat impune ca informațiile privind condamnările pronunțate în statele membre să fie luate în considerare în afara statului membru de condamnare, atât în cadrul unor noi procese penale, astfel cum se prevede în Decizia-cadru 2008/675/JAI a Consiliului ([2]), precum și pentru a preveni comiterea de noi infracțiuni.

(3) Obiectivul menționat presupune schimbul de informații extrase din cazierele judiciare între autoritățile competente ale statelor membre. Schimbul de astfel de informații este organizat și facilitat de normele prevăzute în Decizia-cadru 2009/315/JAI a Consiliului ([3]) și de sistemul european de informații cu privire la cazierele judiciare (ECRIS), instituit prin Decizia 2009/316/JAI a Consiliului ([4]).

(4) Cu toate acestea, cadrul juridic existent al ECRIS nu ia suficient în considerare particularitățile cererilor referitoare la resortisanți ai țărilor terțe. Deși schimbul de informații privind resortisanții țărilor terțe prin intermediul ECRIS este deja posibil, nu există nicio procedură sau mecanism comun al Uniunii care să permită un schimb eficient, rapid și exact.

(5) În cadrul Uniunii, informațiile privind resortisanții țărilor terțe nu sunt colectate ca în cazul resortisanților statelor membre în statele membre de cetățenie, ci sunt stocate numai în statele membre în care s-au pronunțat condamnările. Prin urmare, situația completă a antecedentelor penale ale unui resortisant al unei țări terțe poate fi stabilită, numai dacă se solicită informații din partea tuturor statelor membre.

([1]) Poziția Parlamentului European din 12 martie 2019 (nepublicată încă în Jurnalul Oficial) și decizia Consiliului din 9 aprilie 2019.
([2]) Decizia-cadru 2008/675/JAI a Consiliului din 24 iulie 2008 privind luarea în considerare a condamnărilor în statele membre ale Uniunii Europene în cadrul unei noi proceduri penale (JO L 220, 15.8.2008, p. 32).
([3]) Decizia-cadru 2009/315/JAI a Consiliului din 26 februarie 2009 privind organizarea și conținutul schimbului de informații extrase din cazierele judiciare între statele membre (JO L 93, 7.4.2009, p. 23).
([4]) Decizia 2009/316/JAI a Consiliului din 6 aprilie 2009 de instituire a Sistemului european de informații cu privire la cazierele judiciare (ECRIS) în aplicarea articolului 11 din Decizia-cadru 2009/315/JAI (JO L 93, 7.4.2009, p. 33).

(6) Astfel de „cereri generice” impun o sarcină administrativă disproporționată tuturor statelor membre, inclusiv celor care nu dețin informații privind resortisantul țării terțe în cauză. În practică, această sarcină descurajează statele membre să solicite altor state membre informații privind resortisanții țărilor terțe, ceea ce îngreunează în mod serios schimbul de informații între ele, limitând accesul lor la informațiile referitoare la cazierele judiciare numai la informațiile stocate în registrul lor național. Prin urmare, crește riscul ca schimbul de informații dintre statele membre să fie ineficient și incomplet, fapt care, la rândul său, afectează nivelul de securitate și siguranță oferit cetățenilor Uniunii și persoanelor care își au reședința în Uniune.

(7) Pentru a îmbunătăți situația, ar trebui stabilit un sistem prin care autoritatea centrală a unui stat membru să poată afla prompt și eficient care alt stat membru sau alte state membre dețin informații privind cazierul judiciar al unui resortisant al unei țări terțe (denumit în continuare „ECRIS-TEN”). Cadrul existent al ECRIS ar putea fi utilizat apoi pentru a solicita informații cu privire la cazierele judiciare de la statele membre respective în conformitate cu Decizia-cadru 2009/315/JAI.

(8) Prin urmare, prezentul regulament ar trebui să stabilească un sistem centralizat la nivelul Uniunii care conține date cu caracter personal și să stabilească normele referitoare la împărțirea responsabilităților între statul membru și organizația responsabilă pentru dezvoltarea și întreținerea sistemului centralizat, precum și orice dispoziție specifică privind protecția datelor necesară pentru a completa dispozițiile existente în materie de protecție a datelor și să prevadă un nivel general corespunzător de protecție a datelor, securitatea datelor și protecția drepturilor fundamentale ale persoanelor în cauză.

(9) Obiectivul de a oferi cetățenilor Uniunii un spațiu de libertate, securitate și justiție, fără frontiere interne, în interiorul căruia este asigurată libera circulație a persoanelor, necesită și deținerea informațiilor privind condamnările cetățenilor Uniunii care dețin și cetățenia unei țări terțe. Având în vedere posibilitatea ca respectivele persoane să se identifice deținând una sau mai multe cetățenii, și posibilitatea ca diferite condamnări să fie consemnate fie în statul membru de condamnare, fie în statul membru de cetățenie, este necesar ca în domeniul de aplicare al prezentului regulament să fie incluși cetățenii Uniunii care dețin și cetățenia unei țări terțe. Excluderea unor astfel de persoane ar face ca informațiile stocate în ECRIS-TEN să fie incomplete. Acest lucru ar pune în pericol fiabilitatea sistemului. Cu toate acestea, întrucât persoanele în cauză dețin cetățenia Uniunii, condițiile în care datele dactiloscopice referitoare la respectivele persoane pot fi introduse în ECRIS-TEN ar trebui să fie comparabile cu condițiile în care are loc schimbul de date dactiloscopice între statele membre prin intermediul ECRIS, care a fost înființat prin Decizia-cadru 2009/315/JAI și Decizia 2009/316/JAI. Prin urmare, în cazul cetățenilor Uniunii care dețin și cetățenia unei țări terțe, datele dactiloscopice ar trebui introduse în ECRIS-TEN numai dacă au fost prelevate în conformitate cu dreptul intern în cursul proceselor penale, înțeles fiind că, pentru a opera o astfel de introducere, statele membre ar trebui să aibă posibilitatea de a utiliza datele dactiloscopice prelevate în alte scopuri decât procesele penale, în cazul în care o astfel de utilizare este permisă în temeiul dreptului intern.

(10) ECRIS-TCN ar trebui să permită prelucrarea datelor dactiloscopice în scopul de a determina statele membre care dețin informații privind cazierul judiciar al unui resortisant al unei țări terțe. Acesta ar trebui de asemenea să permită prelucrarea imaginilor faciale pentru a confirma identitatea acestuia. Este deosebit de important ca introducerea și utilizarea datelor dactiloscopice și a imaginilor faciale să nu depășească ceea ce este strict necesar pentru atingerea obiectivului urmărit, să respecte drepturile fundamentale, precum și interesul superior al copilului, și să respecte normele aplicabile ale Uniunii în materie de protecție a datelor.

(11) Sarcina dezvoltării și operării ECRIS-TCN ar trebui să fie încredințată Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA), instituită prin Regulamentul (UE) 2018/1726 al Parlamentului European și al Consiliului ([5]), având în vedere experiența sa în gestionarea altor sisteme la scară largă în domeniul justiției și al afacerilor interne. Mandatul său ar trebui să fie modificat pentru a reflecta aceste noi sarcini.

(12) Eu-LISA ar trebui să beneficieze de finanțare și de personal adecvat pentru a-și îndeplini responsabilitățile în temeiul prezentului regulament.

(13) Dată fiind necesitatea creării unor strânse legături tehnice între ECRIS-TCN și ECRIS, ar trebui să i se încredințeze eu-LISA și sarcina de a dezvolta în continuare și de a întreține aplicația de referință a ECRIS, iar mandatul său ar trebui să fie modificat pentru a reflecta acest lucru.

(14) Patru state membre și-au dezvoltat propriul software național de implementare a ECRIS, în conformitate cu Decizia-cadru 2009/316/JAI a Consiliului, și l-au utilizat în locul aplicației de referință a ECRIS pentru a face schimb de informații privind cazierele judiciare. Având în vedere caracteristicile speciale pe care aceste state membre le-au prevăzut pentru sistemele lor de uz național, precum și investițiile realizate de acestea, ar trebui ca acestor state membre să li se permită să utilizeze software-ul lor național de implementare a ECRIS și pentru ECRIS-TCN, cu condiția respectării condițiilor prevăzute în prezentul regulament.

([5]) Regulamentul (UE) 2018/1726 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA) și de modificare a Regulamentului (CE) nr. 1987/2006 și a Deciziei 2007/533/JAI a Consiliului, precum și de abrogare a Regulamentului (UE) nr. 1077/2011 (JO L 295, 21.11.2018, p. 99).

(15) ECRIS-TCN ar trebui să conțină numai informații privind identitatea resortisanților țărilor terțe condamnați de o instanță penală în cadrul Uniunii. Astfel de informații privind identitatea ar trebui să includă datele alfanumerice și datele dactiloscopice. Ar trebui să fie posibilă introducerea de imagini faciale, în măsura în care legislația statului membru în care se pronunță o condamnare permite colectarea și stocarea imaginilor faciale ale unei persoane condamnate.

(16) Datele alfanumerice care urmează a fi introduse de statele membre în sistemul central ar trebui să includă, printre altele, numele (numele de familie) și prenumele persoanei condamnate, precum și, dacă astfel de informații sunt la dispoziția autorității centrale, orice pseudonim sau nume de împrumut al(e) persoanei respective. În cazul în care statul membru în cauză are cunoștință de date cu caracter personal care nu coincid, cum ar fi o ortografiere diferită a numelui în alt alfabet, ar trebui ca datele respective să poată fi incluse în sistemul central ca informații suplimentare.

(17) Datele alfanumerice ar trebui să includă, de asemenea, ca informații suplimentare, numărul de identificare sau tipul și numărul documentului (documentelor) de identificare al(e) persoanei, precum și denumirea autorității emitente a respectivelor documente, în cazul în care autoritatea centrală deține astfel de informații. Statul membru ar trebui să încerce să verifice autenticitatea documentelor de identificare înainte de a introduce informațiile relevante în sistemul central. În orice caz, având în vedere că ar putea să nu fie fiabile, astfel de informații ar trebui să fie utilizate cu precauție.

(18) Autoritățile centrale ar trebui să utilizeze ECRIS-TCN pentru a determina statele membre care dețin informații privind cazierul judiciar al unui resortisant al unei țări terțe, atunci când informațiile privind cazierul judiciar al persoanei respective sunt solicitate în statul membru interesat, în scopul unor procese penale împotriva persoanei în cauză, în scopurile menționate în prezentul regulament. Cu toate că ECRIS-TCN ar trebui utilizat, în principiu, în toate situațiile de acest tip, autoritatea responsabilă pentru desfășurarea proceselor penale ar trebui să poată decide ca ECRIS-TCN să nu fie folosit atunci când acest lucru nu ar fi adecvat în cazul în speță, de exemplu, în cazul anumitor procese penale urgente, în cazurile de tranzit, atunci când au fost obținute recent informații privind cazierul judiciar prin intermediul ECRIS sau în ceea ce privește infracțiunile minore, în special infracțiunile rutiere minore, infracțiunile minore legate de reglementările locale generale și infracțiunile minore de tulburare a ordinii publice.

(19) Ar trebui, de asemenea, ca statele membre să poată utiliza ECRIS-TCN în scopuri altele decât cele menționate în prezentul regulament, dacă acest lucru este prevăzut în dreptul intern și este în conformitate cu acesta. Cu toate acestea, pentru a spori transparența utilizării ECRIS-TCN, statele membre ar trebui să notifice Comisiei respectivele scopuri, iar Comisia ar trebui să asigure publicarea tuturor notificărilor în *Jurnalul Oficial al Uniunii Europene*.

(20) De asemenea, ar trebui ca alte autorități care solicită informații privind cazierele judiciare să poată decide ca ECRIS-TCN să nu fie utilizat dacă utilizarea acestuia nu ar fi adecvată în cazul în speță, de exemplu atunci când trebuie efectuate anumite verificări administrative obișnuite referitoare la calificarea profesională a unei persoane, în special dacă se știe că nu vor fi solicitate altor state membre informații privind cazierele judiciare, indiferent de rezultatul căutării efectuate în ECRIS-TCN. Cu toate acestea, ECRIS-TCN ar trebui folosit de fiecare dată când cererea de informații privind cazierele judiciare a fost formulată de o persoană care solicită informații privind propriul cazier judiciar în conformitate cu Decizia-cadru 2009/315/JAI, sau când cererea urmărește obținerea de informații privind cazierele judiciare în conformitate cu Directiva 2011/93/UE a Parlamentului European și a Consiliului ([6]).

(21) Resortisanții țărilor terțe ar trebui să aibă dreptul de a obține informații în scris cu privire la propriile lor cazier judiciare, în conformitate cu dreptul statului membru în care solicită furnizarea acestor informații și în conformitate cu Decizia-cadru 2009/315/JAI. Înainte de a furniza astfel de informații unui resortisant al unei țări terțe, statul membru vizat ar trebui să efectueze o interogare în ECRIS-TCN.

(22) Cetățenii Uniunii care dețin și cetățenia unei țări terțe vor fi incluși în ECRIS-TCN numai dacă autoritățile competente sunt la curent cu faptul că persoanele respective dețin cetățenia unei țări terțe. În cazurile în care autoritățile competente nu sunt la curent cu faptul că cetățeni ai Uniunii dețin și cetățenia unei țări terțe, este totuși posibil ca persoanele respective să fi fost condamnate anterior în calitate de resortisanți ai unei țări terțe. Pentru a se asigura faptul că autoritățile competente au o viziune de ansamblu completă asupra cazierelor judiciare, ar trebui să fie posibilă efectuarea de interogări în ECRIS-TCN pentru a verifica dacă, în ceea ce îl privește pe un cetățean al Uniunii, există vreun stat membru care deține informații privind cazierul judiciar al acestei persoane, în calitatea sa de resortisant al unei țări terțe.

(23) În cazul în care există o concordanță între datele înregistrate în sistemul central și cele utilizate pentru căutare de un stat membru (rezultat pozitiv), informațiile privind identitatea pe baza cărora a fost înregistrat un „rezultat pozitiv” ar trebui să fie furnizate împreună cu rezultatul pozitiv. Rezultatul unei căutări ar trebui să fie utilizat de către autoritățile centrale numai în scopul trimiterii unei cereri prin intermediul ECRIS, iar în ceea ce privește Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust) instituită prin Regulamentul

([6]) Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO L 335, 17.12.2011, p. 1).

(UE) 2018/1727 al Parlamentului European și al Consiliului ([7]), Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) instituită prin Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului ([8]) și Parchetul European, instituit prin Regulamentul (UE) 2017/1939 al Consiliului ([9]), ar trebui să fie utilizat numai în scopul solicitării de informații referitoare la condamnări, astfel cum se menționează în prezentul regulament.

(24) În primul rând, imaginile faciale incluse în ECRIS-TCN ar trebui utilizate numai pentru a confirma identitatea unui resortisant al unei țări terțe, pentru a determina statele membre care dețin informații privind condamnările anterioare ale respectivului resortisant al unei țări terțe. În viitor, imaginile faciale ar trebui să poată fi utilizate pentru stabilirea automatizată de corespondențe biometrice, cu condiția să fi fost îndeplinite cerințele tehnice și în materie de politică. Comisia, luând în considerare necesitatea și proporționalitatea, precum și progresele tehnice în materie de software de recunoaștere facială, ar trebui să evalueze disponibilitatea și gradul de adecvare al tehnologiei necesare înainte de a adopta un act delegat privind utilizarea de imagini faciale pentru identificarea resortisanților țărilor terțe, pentru a determina statele membre care dețin informații privind condamnările anterioare cu privire la aceste persoane.

(25) Utilizarea datelor biometrice este necesară, deoarece este cea mai fiabilă metodă de identificare a resortisanților țărilor terțe aflați pe teritoriul statelor membre, care adesea nu dețin documente sau orice alt tip de mijloace de identificare, precum și pentru o corelare mai sigură a datelor privind resortisanții țărilor terțe.

(26) Statele membre ar trebui să introducă în sistemul central datele dactiloscopice ale resortisanților țărilor terțe condamnați, care au fost prelevate în conformitate cu dreptul intern în cursul unor procese penale. Pentru a dispune, în sistemul central, de informații privind identitatea cât mai complete posibil, statele membre trebuie să aibă posibilitatea, de asemenea, de a introduce în sistemul central datele dactiloscopice care au fost prelevate în alte scopuri decât al proceselor penale, în cazurile în care datele dactiloscopice respective pot fi utilizate în cadrul proceselor penale, în conformitate cu dreptul intern.

(27) Prezentul regulament ar trebui să stabilească criterii minime privind datele dactiloscopice pe care statele membre ar trebui să le introducă în sistemul central. Un stat membru ar trebui să poată alege fie să introducă datele dactiloscopice ale resortisanților țărilor terțe care au primit pedepse privative de libertate cu durata de cel puțin 6 luni, fie să introducă datele dactiloscopice ale resortisanților țărilor terțe care au fost condamnați pentru o infracțiune care se pedepsește, conform legislației respectivului stat membru, cu o pedeapsă privativă de libertate cu durată maximă de cel puțin 12 luni.

(28) Statele membre ar trebui să creeze înregistrări în ECRIS-TCN în ceea ce privește resortisanții țărilor terțe condamnați. Acest lucru ar trebui efectuat automat, ori de câte ori este posibil, fără întârzieri nejustificate, după înscrierea condamnării acestora în cazierul judiciar național. Statele membre ar trebui, în conformitate cu prezentul regulament, să introducă în sistemul central date alfanumerice și date dactiloscopice referitoare la condamnările pronunțate după data începerii introducerii datelor în ECRIS-TCN. Începând cu aceeași dată, precum și în orice moment ulterior, statelor membre ar trebui să li se permită introducerea de imagini faciale în sistemul central.

(29) Statele membre ar trebui, de asemenea, în conformitate cu prezentul regulament, să creeze înregistrări în ECRIS-TCN vizându-i pe resortisanții țărilor terțe condamnați înainte de data de începere a introducerii datelor, în vederea asigurării unei eficiențe maxime a sistemului. Cu toate acestea, în acest scop, statele membre nu ar trebui să fie obligate să colecteze informații care nu erau deja introduse în cazierele lor judiciare înainte de data de începere a introducerii datelor. Datele dactiloscopice ale resortisanților țărilor terțe prelevate în legătură cu astfel de condamnări anterioare ar trebui introduse numai în cazul în care au fost prelevate în cursul proceselor penale, iar statul membru interesat consideră că acestea pot fi corelate în mod clar cu alte informații privind identitatea din cazierele judiciare.

(30) Îmbunătățirea schimbului de informații privind condamnările ar trebui să contribuie la punerea în aplicare, de către statele membre, a Deciziei-cadru 2008/675/JAI, care introduce obligația statelor membre de a ține seama de condamnările anterioare din alte state membre în noile procese penale, în măsura în care condamnările naționale anterioare sunt luate în considerare în temeiul dreptului intern.

([7]) Regulamentul (UE) 2018/1727 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust) și de înlocuire și abrogare a Deciziei 2002/187/JAI a Consiliului (JO L 295, 21.11.2018, p. 138).

([8]) Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 24.5.2016, p. 53).

([9]) Regulamentul (UE) 2017/1939 al Consiliului din 12 octombrie 2017 de punere în aplicare a unei forme de cooperare consolidată în ceea ce privește instituirea Parchetului European (EPPO) (JO L 283, 31.10.2017, p. 1).

(31) Un rezultat pozitiv indicat de ECRIS-TCN nu ar trebui ca de sine-stătător să însemne că resortisantul în cauză al unei țări terțe a fost condamnat în statele membre indicate. Existența unor condamnări anterioare ar trebui să fie confirmată exclusiv pe baza informațiilor primite din cazierele judiciare din statele membre în cauză.

(32) Fără a aduce atingere posibilității de utilizare a programelor financiare ale Uniunii în conformitate cu normele aplicabile, fiecare stat membru ar trebui să suporte propriile costuri ocazionate de punerea în aplicare, administrarea, utilizarea și întreținerea propriei baze de date privind cazierele judiciare și a bazelor de date dactiloscopice naționale, precum și de punerea în aplicare, administrarea, utilizarea și întreținerea modificărilor tehnice necesare pentru a putea utiliza ECRIS-TCN, inclusiv conexiunile la punctul național central de acces.

(33) Europol și EPPO ar trebui să aibă acces la ECRIS-TCN cu scopul de a determina statele membre care dețin informații cu privire la cazierul judiciar al resortisantului unei țări terțe, pentru a sprijini îndeplinirea sarcinilor lor statutare. De asemenea, Eurojust ar trebui să aibă acces direct la ECRIS-TCN în scopul îndeplinirii sarcinii sale în temeiul prezentului regulament de a acționa ca punct de contact pentru țări terțe și organizații internaționale, fără a aduce atingere aplicării principiilor cooperării judiciare în materie penală, inclusiv normelor privind asistența judiciară reciprocă. Deși poziția statelor membre care nu fac parte din cooperarea consolidată de instituire a EPPO ar trebui să fie luată în considerare, nu ar trebui să se refuze accesul EPPO la informații privind condamnările numai pentru motivul că statul membru vizat nu participă la cooperarea consolidată.

(34) Prezentul regulament stabilește norme stricte de acces la ECRIS-TCN, precum și garanțiile necesare, inclusiv responsabilitatea statelor membre în ceea ce privește colectarea și utilizarea datelor. Acesta stabilește, de asemenea, modul în care persoanele își pot exercita drepturile la compensare, acces, rectificare, ștergere și despăgubire, în special dreptul la o cale de atac eficientă, precum și supravegherea operațiunilor de prelucrare de către autoritățile publice independente. Prin urmare, regulamentul respectă drepturile și libertățile fundamentale și principiile consacrate, în special în Carta drepturilor fundamentale a Uniunii Europene, inclusiv dreptul la protecția datelor cu caracter personal, principiul egalității în fața legii și interzicerea generală a discriminării. În acest context, aceasta ia în considerare, de asemenea, Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, Pactul internațional cu privire la drepturile civile și politice și alte obligații privind drepturile omului în temeiul dreptului internațional.

(35) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului ([10]) ar trebui să se aplice prelucrării datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau în scopul executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa securității publice. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([11]) ar trebui să se aplice prelucrării datelor cu caracter personal de către autoritățile naționale în cazul în care o astfel de prelucrare nu intră sub incidența Directivei (UE) 2016/680. Ar trebui să fie asigurată o supraveghere coordonată, în conformitate cu Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([12]) care ar trebui să se aplice și prelucrării datelor cu caracter personal de către eu-LISA.

(36) În ceea ce privește condamnările anterioare, autoritățile centrale ar trebui să introducă datele alfanumerice până la sfârșitul perioadei prevăzute pentru introducerea datelor în temeiul prezentului regulament, iar datele dactiloscopice în termen de doi ani de la data începerii funcționării ECRIS-TCN. Statele membre trebuie să aibă posibilitatea de a introduce toate datele în același timp, cu condiția ca respectivele termene să fie respectate.

(37) Ar trebui stabilite norme privind responsabilitatea care revine statelor membre, Eurojust, Europol, EPPO și eu-LISA în cazul unor daune care rezultă din încălcarea dispozițiilor prezentului regulament.

(38) Pentru a îmbunătăți determinarea statelor membre care dețin informații cu privire la condamnările anterioare ale resortisanților țărilor terțe, competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene (TFUE) ar trebui delegată Comisiei în ceea ce privește completarea prezentului regulament prin permiterea utilizării imaginilor faciale în scopul identificării resortisanților țărilor terțe în scopul de a determina statele membre care dețin informații privind condamnările anterioare. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din

([10]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

([11]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([12]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

13 aprilie 2016 privind o mai bună legiferare ([13]). În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(39) În vederea asigurării unor condiții uniforme pentru stabilirea și gestionarea operațională a ECRIS-TCN, ar trebui conferite Comisiei competențe de executare. Competențele respective ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([14]).

(40) Statele membre ar trebui să ia măsurile necesare pentru a se conforma prezentului regulament cât mai rapid posibil pentru a se asigura buna funcționare a ECRIS-TCN, ținându-se seama de timpul de care eu-LISA are nevoie pentru a dezvolta și pune în aplicare ECRIS-TCN. Totuși, după intrarea în vigoare a prezentului regulament, statele membre ar trebui să aibă la dispoziție cel puțin 36 de luni pentru a lua măsurile necesare pentru a se conforma prezentului regulament.

(41) Întrucât obiectivul prezentului regulament, și anume acela de a permite un schimb rapid și eficient de informații precise cu privire la cazierele judiciare ale resortisanților țărilor terțe, nu poate fi realizat în mod satisfăcător de către statele membre, dar, prin instituirea unor norme comune, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este enunțat la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea acestui obiectiv.

(42) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la TUE și la TFUE, Danemarca nu participă la adoptarea prezentului regulament, acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică.

(43) În conformitate cu articolele 1 și 2 și cu articolul 4a alineatul (1) din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la TUE și la TFUE, și fără a aduce atingere articolului 4 din protocolul respectiv, Irlanda nu participă la adoptarea prezentului regulament, acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică.

(44) În conformitate cu articolul 3 și cu articolul 4a alineatul (1) din Protocolul nr. 21, Regatul Unit și-a notificat intenția de a participa la adoptarea și la aplicarea prezentului regulament.

(45) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([15]) și a emis un aviz la 12 decembrie 2017 ([16]),

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

Dispoziții generale

Articolul 1

Obiect

Prezentul regulament stabilește:

(a) un sistem pentru a determina statele membre care dețin informații cu privire la condamnările anterioare ale resortisanților țărilor terțe (denumit în continuare „ECRIS-TCN”);

(b) condițiile de utilizare a ECRIS-TCN de către autoritățile centrale în scopul obținerii de informații cu privire la astfel de condamnări anterioare prin intermediul sistemului european de informații cu privire la cazierele judiciare (ECRIS), stabilit prin Decizia-cadru 2009/316/JAI, precum și condițiile în care Eurojust, Europol și EPPO utilizează ECRIS-TCN.

([13]) JO L 123, 12.5.2016, p. 1.
([14]) Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).
([15]) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).
([16]) JO C 55, 14.2.2018, p. 4.

Articolul 2

Domeniu de aplicare

Prezentul regulament se aplică prelucrării de informații privind identitatea resortisanților țărilor terțe care au făcut obiectul unor condamnări în statele membre, cu scopul de a determina statele membre în care au fost pronunțate aceste condamnări. Cu excepția articolului 5 alineatul (1) litera (b) punctul (ii), dispozițiile prezentului regulament care se aplică resortisanților țărilor terțe se aplică în egală măsură și cetățenilor Uniunii care dețin și cetățenia unei țări terțe și care au făcut obiectul unor condamnări în statele membre.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „condamnare” înseamnă orice hotărâre definitivă a unei instanțe penale împotriva unei persoane fizice pentru o infracțiune penală, în măsura în care hotărârea este înscrisă în cazierul judiciar din statul membru care a pronunțat condamnarea;

2. „proces penal” înseamnă procedura care cuprinde etapa premergătoare judecății, etapa judecății și executarea condamnării;

3. „cazier judiciar” înseamnă registrul național sau registrele naționale în care sunt consemnate condamnările pronunțate în conformitate cu dreptul intern;

4. „stat membru de condamnare” înseamnă statul membru în care se pronunță o condamnare;

5. „autoritate centrală” înseamnă o autoritate desemnată în conformitate cu articolul 3 alineatul (1) din Decizia-cadru 2009/315/JAI;

6. „autorități competente” înseamnă autoritățile centrale, Eurojust, Europol și EPPO, care sunt competente să aibă acces la ECRIS-TCN sau să efectueze interogări în ECRIS-TCN, în conformitate cu prezentul regulament;

7. „resortisant al unei țări terțe” înseamnă o persoană care nu este cetățean al Uniunii în sensul articolului 20 alineatul (1) din TFUE, sau care este un apatrid sau o persoană a cărei cetățenie este necunoscută;

8. „sistem central” înseamnă baza sau bazele de date dezvoltate și întreținute de către eu-LISA care conțin informații privind identitatea resortisanților țărilor terțe care au făcut obiectul unor condamnări în statele membre;

9. „interfață software” înseamnă interfața software găzduită de autoritățile competente care le permite acestora accesul la sistemul central prin intermediul infrastructurii de comunicare menționate la articolul 4 alineatul (1) litera (d);

10. „informații privind identitatea” înseamnă date alfanumerice, date dactiloscopice și imagini faciale care sunt utilizate pentru a stabili o legătură între aceste date și o persoană fizică;

11. „date alfanumerice” înseamnă date constând în litere, cifre, caractere speciale, spații și semne de punctuație;

12. „date dactiloscopice” înseamnă datele legate de impresiunile în plan și de cele prelevate prin apăsarea degetului de la un capăt al unghiei la celălalt ale amprentelor digitale ale fiecărui deget al unei persoane;

13. „imagine facială” înseamnă o imagine digitală a feței unei persoane;

14. „rezultat pozitiv” înseamnă una sau mai multe concordanțe stabilite prin compararea informațiilor privind identitatea înregistrate în sistemul central cu cele utilizate pentru efectuarea unei căutări;

15. „punctul național central de acces” înseamnă punctul național de conectare la infrastructura de comunicații menționată la articolul 4 alineatul (1) litera (d);

16. „aplicația de referință a ECRIS” înseamnă programul informatic dezvoltat de Comisie și pus la dispoziția statelor membre pentru schimbul de informații cu privire la cazierele judiciare prin intermediul ECRIS;

17. „autoritate națională de supraveghere” înseamnă o autoritate publică independentă înființată de un stat membru în temeiul normelor Uniunii aplicabile în materie de protecție a datelor;

18. „autorități de supraveghere” înseamnă Autoritatea Europeană pentru Protecția Datelor și autoritățile naționale de supraveghere.

Articolul 4

Arhitectura tehnică a ECRIS-TCN

(1) ECRIS-TCN este compus din:

(a) un sistem central în care sunt stocate informații privind identitatea resortisanților țărilor terțe condamnați;

(b) un punct național central de acces în fiecare stat membru;

(c) o interfață software care permite conectarea autorităților competente la sistemul central prin intermediul punctului național central de acces și al infrastructurii de comunicații menționată la litera (d);

(d) o infrastructură de comunicații între sistemul central și punctul național central de acces.

(2) Sistemul central va fi găzduit de eu-LISA la sediile sale tehnice.

(3) Interfața software trebuie să fie integrată în aplicația de referință a ECRIS. Statele membre utilizează aplicația de referință a ECRIS sau, în cazurile și în condițiile stabilite la alineatele (4)-(8), software-ul lor național de implementare a ECRIS, pentru a efectua interogări în ECRIS-TCN și pentru a trimite cereri ulterioare de informații privind cazierele judiciare.

(4) Statele membre care utilizează software-ul lor național de implementare a ECRIS sunt responsabile să se asigure că software-ul lor național de implementare a ECRIS permite autorităților lor naționale responsabile de cazierele judiciare să utilizeze ECRIS-TCN, cu excepția interfeței software, în conformitate cu prezentul regulament. În acest scop, acestea se asigură, înaintea datei de începere a funcționării ECRIS-TCN, în conformitate cu articolul 35 alineatul (4), că software-ul lor național de implementare a ECRIS funcționează în conformitate cu protocoalele și specificațiile tehnice stabilite în actele de punere în aplicare menționate la articolul 10, precum și cu orice cerință tehnică suplimentară stabilită de către eu-LISA în temeiul prezentului regulament care are la bază respectivele acte de punere în aplicare.

(5) Atât timp cât nu folosesc aplicația de referință a ECRIS, statele membre care își utilizează propriul software național de implementare a ECRIS asigură, de asemenea, implementarea, fără întârzieri nejustificate, a oricăror adaptări tehnice ulterioare la software-ul lor național de implementare a ECRIS care se impun în urma oricărei modificări aduse specificațiilor tehnice stabilite în actele de punere în aplicare menționate la articolul 10 sau a modificării oricărei cerințe tehnice ulterioare stabilită de către eu-LISA în temeiul prezentului regulament având care are la bază respectivele acte de punere în aplicare.

(6) Statele membre care utilizează software-ul lor național de implementare a ECRIS suportă toate costurile asociate implementării, întreținerii și dezvoltării ulterioare a software-ului lor național de implementare a ECRIS și interconectării acestuia cu ECRIS-TCN, cu excepția interfeței software.

(7) În cazul în care un stat membru care utilizează software-ul său național de implementare a ECRIS nu este în măsură să respecte obligațiile care îi revin în temeiul prezentului articol, acesta este obligat să utilizeze aplicația de referință a ECRIS, inclusiv interfața software integrată, pentru a utiliza ECRIS-TCN.

(8) Având în vedere evaluarea care urmează să fie efectuată de către Comisie în temeiul articolului 36 alineatul (10) litera (b), statele membre în cauză transmit Comisiei toate informațiile necesare.

CAPITOLUL II

Introducerea și utilizarea datelor de către autoritățile centrale

Articolul 5

Introducerea datelor în ECRIS-TCN

(1) Pentru fiecare resortisant al unei țări terțe condamnat, autoritatea centrală din statul membru de condamnare creează un fișier de date în sistemul central. Fișierul de date cuprinde următoarele date:

(a) în ce privește datele alfanumerice:

(i) informații care trebuie să fie introduse, exceptând situația în care, în cazuri individuale, autoritatea centrală nu are cunoștință de astfel de informații (informații obligatorii):

— numele (de familie);

— prenumele;

— data nașterii;

— locul nașterii (localitatea și țara);

— cetățenia sau cetățeniile;

— genul;

— numele anterioare, dacă este cazul;

— codul statului membru de condamnare;

(ii) informații care trebuie să fie introduse dacă sunt înscrise în cazierul judiciar (informații facultative):

— numele părinților;

(iii) informații care trebuie să fie introduse dacă sunt deținute de autoritatea centrală (informații suplimentare):

— numărul de identitate sau tipul și numărul documentelor de identificare ale persoanei, precum și denumirea autorității emitente;

— pseudonime sau nume de împrumut;

(b) în ce privește date dactiloscopice:

(i) datele dactiloscopice care au fost prelevate în conformitate cu dreptul intern în cursul unor procese penale;

(ii) cel puțin datele dactiloscopice prelevate:

— fie în cazul în care resortisantul țării terțe a fost condamnat la o pedeapsă privativă de libertate cu durata de cel puțin 6 luni;

— fie în cazul în care resortisantul țării terțe a fost condamnat pentru o infracțiune care, în temeiul legislației statului membru, se pedepsește cu o pedeapsă privativă de libertate cu durată maximă de cel puțin 12 luni.

(2) Datele dactiloscopice menționate la alineatul (1) litera (b) de la prezentul articol fac obiectul specificațiilor tehnice privind calitatea, rezoluția și prelucrarea datelor dactiloscopice prevăzute în actul de punere în aplicare menționat la articolul 10 alineatul (1) litera (b). Numărul de referință al datelor dactiloscopice ale persoanei condamnate include codul statului membru de condamnare.

(3) Fișierul de date poate, de asemenea, să conțină imagini faciale ale resortisantului țării terțe condamnat, dacă legislația statului membru de condamnare permite colectarea și stocarea imaginilor faciale ale persoanelor condamnate.

(4) Statul membru de condamnare creează automat fișierul de date, atunci când acest lucru este posibil, fără întârzieri nejustificate, după înscrierea condamnării în cazierul judiciar.

(5) Statele membre de condamnare creează fișiere de date inclusiv pentru condamnările pronunțate înainte de data începerii introducerii datelor în conformitate cu articolul 35 alineatul (1), în măsura în care datele referitoare la persoanele condamnate sunt stocate în bazele lor de date naționale. În astfel de cazuri, datele dactiloscopice trebuie să fie introduse numai dacă au fost prelevate în cursul unor procese penale în conformitate cu dreptul intern și în cazul în care pot fi corelate în mod clar cu alte informații privind identitatea din cazierul judiciar.

(6) În vederea respectării obligațiilor prevăzute la alineatul (1) litera (b) punctele (i) și (ii) și la alineatul (5), statele membre pot utiliza date dactiloscopice prelevate în alte scopuri decât cel al proceselor penale, în cazul în care o astfel de utilizare este permisă în temeiul dreptului intern.

Articolul 6

Imaginile faciale

(1) Până la intrarea în vigoare a actului delegat prevăzut la alineatul (2), imaginile faciale pot fi utilizate numai pentru a confirma identitatea resortisantului unei țări terțe care a fost identificat în urma unei căutări alfanumerice sau a unei căutări cu ajutorul datelor dactiloscopice.

(2) Comisia este împuternicită să adopte acte delegate în completarea prezentului regulament, în conformitate cu articolul 37, în ceea ce privește utilizarea imaginilor faciale pentru identificarea resortisanților țărilor terțe în scopul de a determina statele membre care dețin informații privind condamnările anterioare care se referă la aceste persoane, atunci când acest lucru devine posibil din punct de vedere tehnic. Înainte de a-și exercita această competență, Comisia, luând în considerare necesitatea și proporționalitatea, precum și progresele tehnice în materie de software de recunoaștere facială, evaluează disponibilitatea și gradul de adecvare al tehnologiei necesare.

Articolul 7

Utilizarea ECRIS-TCN pentru determinarea statelor membre care dețin informații privind cazierele judiciare

(1) Autoritățile centrale utilizează ECRIS-TCN pentru a determina statele membre care dețin informații privind cazierul judiciar al unui resortisant al unei țări terțe, pentru a obține informații cu privire la condamnările anterioare prin intermediul ECRIS, atunci când informațiile privind cazierul judiciar al persoanei respective sunt solicitate în statul membru interesat, în scopul unor procese penale împotriva persoanei în cauză sau în oricare dintre scopurile enumerate în continuare, dacă sunt prevăzute în dreptul intern și este în conformitate cu acesta:

— verificarea cazierului judiciar al unei persoane, la cererea acesteia;

— autorizările de securitate;

— obținerea unei autorizații sau a unui permis;

— verificarea în vederea angajării;

— verificarea pentru activitățile de voluntariat care implică contactul direct și periodic cu copii sau persoane vulnerabile;

— viza, dobândirea cetățeniei și procedurile în materie de migrație, inclusiv procedurile de azil; și

— controalele în legătură cu contractele de achiziții publice și examinările publice.

Cu toate acestea, în anumite cazuri, altele decât cele în care un resortisant al unei țări terțe solicită autorității centrale informații referitoare la propriul cazier judiciar sau în care cererea este făcută pentru a obține informații privind cazierele judiciare în temeiul articolului 10 alineatul (2) din Directiva 2011/93/UE, autoritatea care solicită informații privind cazierele judiciare poate decide că o astfel de utilizare a ECRIS-TCN nu este adecvată.

(2) Orice stat membru care decide, dacă acest lucru este prevăzut în dreptul intern și este în conformitate cu acesta, să utilizeze ECRIS-TCN pentru alte scopuri decât cele prevăzute la alineatul (1) în vederea obținerii de informații prin intermediul ECRIS cu privire la condamnările anterioare, comunică, până la data începerii funcționării sistemului, astfel cum se prevede la articolul 35 alineatul (4) sau în orice moment ulterior, Comisiei aceste alte scopuri și orice modificare a scopurilor respective. Comisia publică notificările respective în *Jurnalul Oficial al Uniunii Europene* în termen de 30 de zile de la primirea lor.

(3) Europol, Eurojust și EPPO au dreptul să efectueze interogări în ECRIS-TCN, în conformitate cu articolele 14-18, pentru a determina statele membre care dețin informații cu privire la cazierul judiciar al unui resortisant al unei țări terțe. Totuși, Europol, Eurojust și EPPO nu introduc, nu rectifică și nu șterg date din ECRIS-TCN.

(4) În scopurile menționate la alineatele (1), (2) și (3), autoritățile competente pot, de asemenea, să efectueze interogări în ECRIS-TCN pentru a verifica dacă, în ceea ce privește un cetățean al Uniunii, există vreun stat membru care deține informații privind cazierul judiciar al acestei persoane, în calitatea respectivei persoane de resortisant al unei țări terțe.

(5) Atunci când efectuează interogări în ECRIS-TCN, autoritățile competente pot utiliza, integral sau parțial, datele menționate la articolul 5 alineatul (1). Date minime necesare pentru a efectua interogări în sistem sunt precizate într-un act de punere în aplicare adoptat în conformitate cu articolul 10 alineatul (1) litera (g).

(6) Autoritățile competente pot, de asemenea, efectua interogări în ECRIS-TCN utilizând imagini faciale, dacă o astfel de funcționalitate a fost pusă în aplicare în conformitate cu articolul 6 alineatul (2).

(7) În cazul unui rezultat pozitiv, sistemul central comunică în mod automat autorității competente informații privind statele membre care dețin informații privind cazierul judiciar al resortisantului unei țări terțe, împreună cu numerele de referință asociate și orice informație corespunzătoare privind identitatea. Astfel de informații privind identitatea sunt utilizate exclusiv în scopul de a verifica identitatea respectivului resortisant al unei țări terțe. Rezultatul unei căutări în sistemul central poate fi utilizat numai în scopul de a adresa o cerere în conformitate cu articolul 6 din Decizia-cadru 2009/315/JAI sau o cerere menționată la articolul 17 alineatul (3) din prezentul regulament.

(8) În cazul în care nu există un rezultat pozitiv, sistemul central informează automat autoritatea competentă.

CAPITOLUL III

Păstrarea și modificarea datelor

Articolul 8

Perioada de păstrare a datelor stocate

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

(2) La expirarea perioadei de păstrare menționate la alineatul (1), autoritatea centrală a statului membru de condamnare șterge din sistemul central fișierul de date, inclusiv datele dactiloscopice sau imaginile faciale. Ștergerea se face, dacă este posibil, în mod automat și, în orice caz, în termen de cel mult o lună de la expirarea perioadei de păstrare.

Articolul 9

Modificarea și ștergerea datelor

(1) Statele membre pot modifica sau șterge datele pe care le-au introdus în ECRIS-TCN.

(2) Orice modificare a informațiilor din cazierele judiciare care au condus la crearea unui fișier de date în conformitate cu articolul 5 trebuie să antreneze o modificare identică a informațiilor stocate în fișierul de date respectiv în sistemul central de către statul membru de condamnare, fără întârzieri nejustificate.

(3) În cazul în care un stat membru de condamnare are motive să creadă că datele pe care le-a înregistrat în sistemul central sunt incorecte sau că acestea au fost prelucrate în sistemul central într-un mod care contravine prezentului regulament, acesta:

(a) lansează imediat o procedură de verificarea exactității datelor în cauză sau a legalității prelucrării acestora, după caz;

(b) dacă este necesar, rectifică sau șterge datele respective din sistemul central, fără întârzieri nejustificate.

(4) În cazul în care un stat membru, altul decât statul membru de condamnare care a introdus datele, are motive să creadă că datele înregistrate în sistemul central sunt incorecte sau că acestea au fost prelucrate în sistemul central într-un mod care contravine prezentului regulament, acesta contactează fără întârzieri nejustificate autoritatea centrală din statul membru de condamnare.

Statul membru de condamnare:

(a) lansează imediat procedura de verificare a exactității datelor în cauză sau a legalității prelucrării acestora, după caz;

(b) dacă este necesar, rectifică sau șterge datele respective din sistemul central, fără întârzieri nejustificate;

(c) informează celălalt stat membru cu privire la rectificarea sau ștergerea datelor sau cu privire la motivele pentru care datele nu au fost rectificate sau șterse, fără întârzieri nejustificate.

CAPITOLUL IV

Dezvoltare, operare și responsabilități

Articolul 10

Adoptarea actelor de punere în aplicare de către Comisie

(1) Comisia adoptă cât mai curând posibil actele de punere în aplicare necesare pentru dezvoltarea și implementarea tehnică a ECRIS-TCN, în special acte privind:

(a) specificațiile tehnice pentru prelucrarea datelor alfanumerice;

(b) specificațiile tehnice pentru calitatea, rezoluția și prelucrarea datelor dactiloscopice;

(c) specificațiile tehnice ale interfeței software;

(d) specificațiile tehnice pentru calitatea, rezoluția și prelucrarea imaginilor faciale în sensul articolului 6 și în condițiile stabilite la același articol;

(e) calitatea datelor, inclusiv un mecanism și proceduri pentru a efectua verificări ale calității datelor;

(f) introducerea datelor în conformitate cu articolul 5;

(g) accesarea și efectuarea de interogări în ECRIS-TCN în conformitate cu articolul 7;

(h) modificarea și ștergerea datelor în conformitate cu articolele 8 și 9;

(i) păstrarea și accesarea fișierelor de evidență în conformitate cu articolul 31;

(j) operarea registrului central și norme privind securitatea datelor și protecția datelor aplicabile registrului, în conformitate cu articolul 32;

(k) furnizarea de statistici în conformitate cu articolul 32;

(l) cerințele privind performanțele și disponibilitatea ECRIS-TCN, inclusiv specificațiile și cerințele minime privind performanțele biometrice ale ECRIS-TCN, în special în ceea ce privește cerințele privind rata rezultatelor de identificare fals pozitive și rata rezultatelor de identificare fals negative.

(2) Actele de punere în aplicare prevăzute la alineatul (1) se adoptă în conformitate cu procedura de examinare menționată la articolul 38 alineatul (2).

Articolul 11

Dezvoltarea și gestionarea operațională a ECRIS-TCN

(1) Eu-LISA este responsabilă pentru dezvoltarea ECRIS-TCN, în conformitate cu principiul protecției datelor începând cu momentul conceperii și în mod implicit. În plus, eu-LISA este responsabilă pentru gestionarea operațională a ECRIS-TCN. Dezvoltarea constă în elaborarea și implementarea specificațiilor tehnice, în testare și în coordonarea generală a proiectului.

(2) Eu-LISA este, de asemenea, responsabilă pentru dezvoltarea ulterioară și întreținerea aplicației de referință a ECRIS.

(3) Eu-LISA proiectează arhitectura fizică a ECRIS-TCN, inclusiv specificațiile tehnice și dezvoltarea ulterioară în ceea ce privește sistemul central, punctul național central de acces și interfața software. Această proiectare se adoptă de către Consiliul de administrație al eu-LISA, sub rezerva unui aviz favorabil din partea Comisiei.

(4) Eu-LISA dezvoltă și pune în aplicare ECRIS-TCN cât mai curând posibil după data intrării în vigoare a prezentului regulament și după adoptarea de către Comisie a actelor de punere în aplicare prevăzute la articolul 10.

(5) Înainte de faza de proiectare și dezvoltare a ECRIS-TCN, Consiliul de administrație al eu-LISA constituie un consiliu de administrație al programului, alcătuit din zece membri.

Consiliul de administrație al programului este alcătuit din opt membri numiți de Consiliul de administrație, președintele grupului consultativ menționat la articolul 39 și un membru numit de Comisie. Membrii numiți de către Consiliul de administrație sunt aleși numai din acele state membre care intră pe deplin, în temeiul dreptului Uniunii, sub incidența instrumentelor legislative care reglementează ECRIS și care vor participa la ECRIS-TCN. Consiliul de administrație se asigură că membrii pe care îi numește în cadrul Consiliului de administrație al programului dispun de experiența și expertiza necesare în domeniul dezvoltării și al gestionării sistemelor informatice care sprijină autoritățile judiciare și pe cele responsabile de cazierele judiciare.

Eu-LISA participă la lucrările Consiliului de administrație al programului. În acest scop, reprezentanții eu-LISA participă la ședințele Consiliului de administrație al programului, pentru a raporta cu privire la lucrările referitoare la proiectarea și dezvoltarea ECRIS-TCN, precum și la orice alte lucrări și activități conexe.

Consiliul de administrație al programului se reunește cel puțin o dată la trei luni sau mai des, dacă este necesar. Acesta asigură gestionarea adecvată a fazei de proiectare și dezvoltare a ECRIS-TCN și asigură consecvența dintre proiectele ECRIS-TCN de la nivel central și cele de la nivel național, precum și cu software-ul național de implementare a ECRIS. Consiliul de administrație al programului prezintă Consiliului de administrație al eu-LISA rapoarte scrise periodice, și cu frecvență lunară dacă este posibil, cu privire la evoluția proiectului. Consiliul de administrație al programului nu are competențe decizionale și nu dispune de un mandat pentru a-i reprezenta pe membrii Consiliului de administrație al eu-LISA.

(6) Consiliul de administrație al programului își stabilește regulamentul de procedură, care include în special norme privind:

(a) președinția;

(b) locul de desfășurare a reuniunilor;

(c) pregătirea reuniunilor;

(d) accesul experților la reuniuni;

(e) planurile de comunicare care asigură informarea completă a membrilor neparticipanți din cadrul Consiliului de administrație.

(7) Președinția Consiliului de administrație al programului este asigurată de un stat membru pentru care instrumentele legislative care reglementează ECRIS și cele care reglementează dezvoltarea, instituirea, operarea și utilizarea tuturor sistemelor IT la scară largă gestionate de eu-LISA au caracter pe deplin obligatoriu, în temeiul dreptului Uniunii.

(8) Toate cheltuielile de deplasare și de ședere suportate de membrii Consiliului de administrație al programului sunt plătite de eu-LISA. Articolul 10 din Regulamentul de procedură al eu-LISA se aplică *mutatis mutandis*. Secretariatul Consiliului de administrație al programului este asigurat de către eu-LISA.

(9) În cursul fazei de proiectare și dezvoltare, Grupul consultativ menționat la articolul 39 este alcătuit din managerii de proiect ai ECRIS-TCN de la nivel național și este prezidat de eu-LISA. În cursul fazei de proiectare și dezvoltare, Grupul consultativ se reunește în mod periodic, dacă este posibil cel puțin o dată pe lună, până la începerea funcționării ECRIS-TCN. După fiecare reuniune, Grupul consultativ prezintă un raport Consiliului de administrație al programului. Grupul consultativ pune la dispoziție expertiză tehnică necesară în sprijinul atribuțiilor care revin Consiliului de administrație al programului și monitorizează stadiul de pregătire al statelor membre.

(10) Pentru a asigura în permanență confidențialitatea și integritatea datelor stocate în ECRIS-TCN, eu-LISA stabilește, în cooperare cu statele membre, măsurile tehnice și organizatorice adecvate, luând în considerare stadiul actual al tehnologiei, costurile punerii în aplicare și riscurile reprezentate de prelucrare.

(11) Eu-LISA este responsabilă de următoarele sarcini legate de infrastructura de comunicații menționată la articolul 4 alineatul (1) litera (d):

(a) supraveghere;

(b) securitate;

(c) coordonarea relațiilor dintre statele membre și furnizorul infrastructurii de comunicații.

(12) Comisia este responsabilă de toate celelalte sarcini referitoare la infrastructura de comunicații menționată la articolul 4 alineatul (1) litera (d), în special:

(a) sarcini legate de execuția bugetului;

(b) achiziții și reînnoire;

(c) aspecte contractuale.

(13) Eu-LISA elaborează și întreține un mecanism și o serie de proceduri pentru efectuarea de controale de calitate privind datele stocate în ECRIS-TCN și prezintă periodic rapoarte statelor membre. Eu-LISA prezintă Comisiei rapoarte periodice cu privire la situațiile problematice întâmpinate și la statele membre vizate.

(14) Gestionarea operațională a ECRIS-TCN cuprinde toate sarcinile necesare pentru a menține ECRIS-TCN operațional în conformitate cu prezentul regulament, în special lucrările de întreținere și perfecționările tehnice necesare pentru a se asigura funcționarea ECRIS-TCN la un nivel satisfăcător, în conformitate cu specificațiile tehnice.

(15) Eu-LISA îndeplinește atribuții legate de furnizarea de formare privind utilizarea tehnică a ECRIS-TCN și a aplicației de referință a ECRIS.

(16) Fără a aduce atingere articolului 17 din Statutul funcționarilor Uniunii Europene, prevăzut în Regulamentul Consiliului (CEE, Euratom, CECO) nr. 259/68 ([17]), eu-LISA aplică normele corespunzătoare privind secretul profesional sau alte obligații echivalente privind confidențialitatea tuturor angajaților care trebuie să lucreze cu datele înregistrate în sistemul central. Această obligație continuă să se aplice și după ce aceste persoane nu mai sunt funcționari sau angajați sau după încheierea activității lor.

Articolul 12

Responsabilitățile statelor membre

(1) Fiecare stat membru este responsabil de:

(a) asigurarea unei conexiuni securizate între cazierele judiciare naționale, bazele de date dactiloscopice naționale și punctul național central de acces;

(b) dezvoltarea, operarea și întreținerea conexiunii menționate la litera (a);

(c) asigurarea unei conexiuni între sistemele naționale și aplicația de referință a ECRIS;

([17]) JO L 56, 4.3.1968, p. 1.

(d) gestionarea și modalitățile de acces la ECRIS-TCN pentru personalul autorizat în mod corespunzător din cadrul autorităților centrale în conformitate cu prezentul regulament, precum și de întocmirea și actualizarea periodică a unei liste cu membrii respectivului personal și profilurile lor, menționată la articolul 19 alineatul (3) litera (g).

(2) Fiecare stat membru asigură o formare profesională adecvată membrilor personalului din cadrul autorității sale centrale cu drept de acces la ECRIS-TCN, în special cu privire la normele de securitate și de protecție a datelor și la drepturile fundamentale aplicabile, înainte de a-i autoriza să prelucreze datele stocate în sistemul central.

Articolul 13

Responsabilitatea în materie de utilizare a datelor

(1) În conformitate cu nomele aplicabile ale Uniunii în materie de protecție a datelor, fiecare stat membru se asigură că datele înregistrate în ECRIS-TCN sunt prelucrate legal și, în special, că:

(a) numai personalul autorizat în mod corespunzător are acces la date în scopul îndeplinirii sarcinilor proprii;

(b) datele sunt colectate în mod legal într-o manieră care asigură respectarea deplină a demnității și a drepturilor fundamentale ale resortisantului țării terțe;

(c) datele sunt introduse în mod legal în ECRIS-TCN;

(d) datele sunt corecte și actualizate atunci când sunt introduse în ECRIS-TCN.

(2) Eu-LISA se asigură că ECRIS-TCN funcționează în conformitate cu prezentul regulament, cu actul delegat menționat la articolul 6 alineatul (2) și cu actele de punere în aplicare menționate la articolul 10, precum și în conformitate cu Regulamentul (UE) 2018/1725. În special, eu-LISA ia măsurile necesare pentru a asigura securitatea sistemului central și a infrastructurii de comunicații menționate la articolul 4 alineatul (1) litera (d), fără a aduce atingere responsabilităților fiecărui stat membru.

(3) Eu-LISA informează, cât mai curând posibil, Parlamentul European, Consiliul și Comisia, precum și Autoritatea Europeană pentru Protecția Datelor cu privire la măsurile pe care le ia în conformitate cu alineatul (2) în vederea începerii funcționării sistemului ECRIS-TCN.

(4) Comisia pune la dispoziția statelor membre și a publicului informațiile menționate la alineatul (3) prin intermediul unui site public de internet actualizat constant.

Articolul 14

Accesul de care beneficiază Eurojust, Europol și EPPO

(1) Eurojust are acces direct la ECRIS-TCN în scopul punerii în aplicare a articolului 17, precum și al îndeplinirii atribuțiilor sale statutare în temeiul articolului 2 din Regulamentul (UE) 2018/1727, pentru a determina statele membre care dețin informații cu privire la condamnările anterioare ale resortisanților țărilor terțe.

(2) Europol are acces direct la ECRIS-TCN în scopul îndeplinirii atribuțiilor sale în temeiul literelor (a)-(e) și al literei (h) de la articolul 4 alineatul (1) din Regulamentul (UE) 2016/794, pentru a determina statele membre care dețin informații cu privire la condamnările anterioare ale resortisanților țărilor terțe.

(3) EPPO are acces direct la ECRIS-TCN în scopul îndeplinirii atribuțiilor sale în temeiul articolului 4 din Regulamentul (UE) 2017/1939, pentru a determina statele membre care dețin informații cu privire la condamnările anterioare ale resortisanților țărilor terțe.

(4) În urma obținerii unui rezultat pozitiv care indică statele membre care dețin informații privind cazierele judiciare ale unui resortisant al unei țări terțe, Eurojust, Europol și EPPO pot să utilizeze contactele lor cu autoritățile naționale ale statelor membre în cauză pentru a solicita informații cu privire la cazierele judiciare în condițiile prevăzute în actele lor de înființare.

Articolul 15

Accesul de care beneficiază personalul autorizat al Eurojust, al Europol și al EPPO

Eurojust, Europol și EPPO sunt responsabile pentru gestionarea și reglementarea accesului la ECRIS-TCN, în conformitate cu prezentul regulament, al personalului autorizat în mod corespunzător, precum și pentru întocmirea și actualizarea periodică a unei liste cu membrii respectivului personal și profilurile lor.

Articolul 16

Responsabilități care revin Eurojust, Europol și EPPO

Eurojust, Europol și EPPO:

(a) stabilesc mijloacele tehnice pentru a se conecta la ECRIS-TCN și sunt responsabile de întreținerea conexiunii;

(b) asigură, acelor membri ai personalului propriu care au dreptul de a accesa ECRIS-TCN, o formare adecvată care vizează, in special, normele de securitate și de protecție a datelor, precum și drepturile fundamentale aplicabile, înainte de a-i autoriza să prelucreze datele stocate în sistemul central;

(c) se asigură că datele cu caracter personal pe care le prelucrează în temeiul prezentului regulament sunt protejate în conformitate cu normele aplicabile privind protecția datelor.

Articolul 17

Punctul de contact pentru țările terțe și organizațiile internaționale

(1) În scopul unor procese penale, țările terțe și organizațiile internaționale pot adresa Eurojust cererile de informații pentru a afla dacă există state membre care dețin informații referitoare la cazierele judiciare ale unui resortisant al unei țări terțe. În acest scop, utilizează formularul standard prevăzut în anexa la prezentul regulament.

(2) În cazul în care primește o cerere în temeiul alineatului (1), Eurojust utilizează ECRIS-TCN pentru a determina dacă există state membre care dețin informații privind cazierul judiciar al resortisantului respectiv al țării terțe.

(3) În cazul în care există un rezultat pozitiv, Eurojust solicită acordul statului membru care deține informații privind cazierul judiciar al resortisantului respectiv al unei țări terțe pentru a informa țara terță sau organizația internațională cu privire la numele statului membru în cauză. În cazul în care statul membru în cauză este de acord, Eurojust informează țara terță sau organizația internațională cu privire la numele statului membru în cauză și informează țara terță sau organizația internațională despre modul în care poate introduce o cerere de extrase din cazierele judiciare în statul membru respectiv în conformitate cu procedurile aplicabile.

(4) În cazul în care nu există un rezultat pozitiv sau în cazul în care Eurojust nu poate furniza un răspuns în conformitate cu alineatul (3) la cererile formulate în temeiul prezentului articol, acesta informează țara terță sau organizația internațională în cauză că a încheiat procedura, fără a furniza nicio indicație din care să rezulte dacă informațiile privind cazierul judiciar al persoanei în cauză sunt deținute de către vreunul dintre statele membre.

Articolul 18

Furnizarea de informații către o țară terță, o organizație internațională sau o entitate privată

Nici Eurojust, nici Europol, nici EPPO și nici vreo autoritate centrală nu pot să transfere sau să pună la dispoziția unei țări terțe, a unei organizații internaționale sau a unei entități private informații obținute prin intermediul ECRIS-TCN referitoare la un resortisant al unei țări terțe. Prezentul articol nu aduce atingere articolului 17 alineatul (3).

Articolul 19

Securitatea datelor

(1) Eu-LISA ia măsurile necesare pentru a asigura securitatea ECRIS-TCN, fără a aduce atingere responsabilităților fiecărui stat membru, luând în considerare măsurile de securitate menționate la alineatul (3).

(2) În ceea ce privește operarea ECRIS-TCN, eu-LISA ia măsurile necesare în vederea realizării obiectivelor stabilite la alineatul (3), inclusiv adoptarea unui plan de securitate și a unui plan de asigurare a continuității activității și de redresare în caz de dezastru, și pentru a se asigura că, în caz de întrerupere, sistemele instalate pot fi restabilite.

(3) Statele membre asigură securitatea datelor înaintea și în cursul transmiterii către punctul național central de acces, precum și înainte și în cursul primirii datelor de la acesta. În particular, fiecare stat membru are obligația:

(a) de a proteja în mod fizic datele, inclusiv prin elaborarea unor planuri de urgență pentru protecția infrastructurii;

(b) de a împiedica accesul persoanelor neautorizate la instalațiile naționale în care statul membru desfășoară operațiuni legate de ECRIS-TCN;

(c) de a împiedica citirea, copierea, modificarea sau îndepărtarea neautorizată a suporturilor de date;

(d) de a împiedica introducerea neautorizată de date și inspectarea, modificarea sau ștergerea neautorizată de date cu caracter personal stocate;

(e) de a împiedica prelucrarea neautorizată a datelor în ECRIS-TCN și orice modificare sau ștergere neautorizată a datelor prelucrate din ECRIS-TCN;

(f) de a garanta că persoanele autorizate să acceseze ECRIS-TCN au acces numai la datele prevăzute de autorizația lor de acces, exclusiv prin folosirea unor identități de utilizator individuale și a unor moduri confidențiale de acces;

(g) de a garanta că toate autoritățile cu drept de acces la ECRIS-TCN creează profiluri care descriu funcțiile și responsabilitățile persoanelor autorizate să introducă, să rectifice, să șteargă, să consulte și să caute date și de a pune profilurile acestora la dispoziția autorităților naționale de supraveghere, fără întârzieri nejustificate, la cererea acestora;

(h) de a se asigura că este posibil să se verifice și să se stabilească căror organisme, oficii și agenții ale Uniunii le pot fi transmise datele cu caracter personal prin utilizarea echipamentelor de comunicare a datelor;

(i) de a se asigura că este posibil să se verifice și să se stabilească ce date au fost prelucrate în ECRIS-TCN, în ce moment, de către cine și cu ce scop;

(j) de a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal pe durata transmiterii datelor cu caracter personal către sau din ECRIS-TCN sau în timpul transportului suporturilor de date, în special prin intermediul tehnicilor de criptare corespunzătoare;

(k) de a monitoriza eficacitatea măsurilor de securitate menționate la prezentul alineat și de a lua măsurile de organizare referitoare la monitorizarea și supravegherea interne necesare pentru a asigura respectarea prezentului regulament.

(4) Eu-LISA și statele membre cooperează pentru a asigura o abordare coerentă a securității datelor, pe baza unui proces de gestionare a riscurilor în materie de securitate, care să cuprindă întregul ECRIS-TCN.

Articolul 20

Răspundere

(1) Orice persoană sau orice stat membru care a suferit un prejudiciu material sau moral ca urmare a unei operațiuni de prelucrare ilicite sau a oricărui alt act incompatibil cu prezentul regulament are dreptul la despăgubire:

(a) din partea statului membru care este responsabil pentru prejudiciul suferit; sau

(b) din partea eu-LISA, în cazul în care eu-LISA nu a respectat obligațiile prevăzute în prezentul regulament sau în Regulamentul (UE) 2018/1725.

Statul membru care este responsabil pentru prejudiciul suferit, respectiv eu-LISA, este exonerat(ă) de responsabilitate, integral sau parțial, dacă dovedește că nu este responsabil(ă) pentru fapta care a provocat prejudiciul.

(2) În cazul în care nerespectarea în orice mod, de către un stat membru, Eurojust, Europol sau EPPO, a obligațiilor care îi revin în virtutea prezentului regulament cauzează prejudicii ECRIS-TCN, respectivul stat membru, Eurojust, Europol sau, după caz, EPPO este responsabil pentru prejudicii, cu excepția cazului și în măsura în care eu-LISA sau un alt stat membru participant la ECRIS-TCN nu a luat măsurile necesare pentru a preveni producerea prejudiciului sau pentru a-i reduce efectele.

(3) Acțiunile în despăgubiri împotriva unui stat membru pentru prejudiciile menționate la alineatele (1) și (2) sunt reglementate de legislația statului membru pârât. Acțiunile în despăgubiri împotriva eu-LISA, a Eurojust, a Europol sau a EPPO pentru prejudiciile menționate la alineatele (1) și (2) sunt reglementate de actele de înființare ale acestora.

Articolul 21

Automonitorizare

Statele membre se asigură că fiecare autoritate centrală ia măsurile necesare pentru asigurarea conformității cu prezentul regulament și cooperează, după caz, cu autoritățile de supraveghere.

Articolul 22

Sancțiuni

Orice utilizare abuzivă a datelor introduse în ECRIS-TCN face obiectul unor sancțiuni sau măsuri disciplinare, în conformitate cu dreptul intern sau al Uniunii, care sunt efective, proporționale și cu efect de descurajare.

CAPITOLUL V

Drepturi și supraveghere în materie de protecție a datelor

Articolul 23

Operatorul de date și persoana împuternicită de către operator

(1) Fiecare autoritate centrală este considerată drept operator de date, în conformitate cu normele aplicabile ale Uniunii în materie de protecție a datelor, în ceea ce privește prelucrarea datelor cu caracter personal de către autoritatea centrală a statului membru respectiv în temeiul prezentului regulament.

(2) Eu-LISA este considerată a fi persoană împuternicită de către operator în conformitate cu Regulamentul (UE) 2018/1725 în ceea ce privește datele cu caracter personal introduse în sistemul central de către statele membre.

Articolul 24

Scopul prelucrării datelor cu caracter personal

(1) Datele introduse în sistemul central sunt prelucrate doar în scopul identificării statelor membre care dețin informații privind cazierele judiciare ale resortisanților țărilor terțe.

(2) Cu excepția personalului autorizat în mod corespunzător din cadrul Eurojust, al Europol sau al EPPO, care are acces la ECRIS-TCN în scopul reglementat prin prezentul regulament, accesul la ECRIS-TCN este rezervat în mod exclusiv personalului autorizat în mod corespunzător din cadrul autorităților centrale. Accesul este limitat la ceea ce este necesar pentru îndeplinirea sarcinilor în conformitate cu scopul prevăzut la alineatul (1) și la ceea ce este necesar și proporțional cu obiectivele urmărite.

Articolul 25

Dreptul la acces, la rectificare, la ștergere și la restricționarea prelucrării

(1) Cererile resortisanților țărilor terțe referitoare la drepturile de acces la datele cu caracter personal, la rectificarea și ștergerea acestora și la restricționarea prelucrării datelor cu caracter personal, prevăzute de normele Uniunii în materie de protecție a datelor, pot fi adresate autorității centrale din oricare stat membru.

(2) În cazul în care o cerere este adresată altui stat membru decât statul membru de condamnare, statul membru căruia i s-a adresat cererea o transmite statului membru de condamnare fără întârzieri nejustificate și, în orice caz, în termen de 10 zile lucrătoare de la primirea cererii. După primirea cererii, statul membru de condamnare:

(a) lansează imediat o procedură de verificare a exactității datelor în cauză sau a legalității prelucrării acestora în ECRIS-TCN; și

(b) răspunde statului membru care a transmis cererea, fără întârzieri nejustificate.

(3) În cazul în care datele înregistrate în ECRIS-TCN sunt incorecte sau au fost prelucrate în mod ilegal, statul membru de condamnare le rectifică sau le șterge în conformitate cu articolul 9. Statul membru de condamnare sau, după caz, statul membru căruia i s-a adresat cererea îi confirmă în scris și fără întârzieri nejustificate persoanei interesate că a luat măsuri pentru rectificarea sau ștergerea datelor referitoare la persoana respectivă. Statul membru de condamnare informează de asemenea, fără întârzieri nejustificate, orice alt stat membru care a primit informații privind condamnările obținute în urma efectuării unei interogări a ECRIS-TCN cu privire la acțiunile care au fost întreprinse.

(4) În cazul în care statul membru de condamnare nu este de acord că datele înregistrate în ECRIS-TCN sunt incorecte sau că au fost prelucrate în mod ilegal, acesta emite o decizie administrativă sau judiciară prin care explică în scris persoanei interesate motivele pentru care nu este dispus să rectifice sau să șteargă datele care o privesc. Astfel de cazuri pot fi comunicate autorității naționale de supraveghere, dacă acest lucru este oportun.

(5) Statul membru care a adoptat decizia în temeiul alineatului (4) comunică totodată persoanei interesate informații care detaliază demersurile pe care această persoană le poate întreprinde dacă găsește inacceptabilă explicația dată în temeiul alineatului (4). Aceste informații se referă inclusiv la modalitățile de a introduce o acțiune sau de a depune o plângere pe lângă autoritățile sau instanțele competente din statul membru sau la orice asistență, inclusiv din partea autorităților naționale de supraveghere, care este disponibilă în conformitate cu dreptul intern al respectivului stat membru.

(6) Orice cerere formulată în temeiul alineatului (1) conține informațiile necesare pentru a identifica persoana în cauză. Aceste informații sunt folosite exclusiv pentru a permite exercitarea drepturilor prevăzute la alineatului (1) și sunt apoi șterse imediat.

(7) În cazul în care se aplică alineatul (2), autoritatea centrală căreia îi este adresată cererea păstrează o înregistrare scrisă a unei astfel de cereri, a modului în care a fost soluționată și a autorității către care a fost transmisă. La solicitarea autorității naționale de supraveghere, autoritatea centrală îi pune acesteia la dispoziție, fără întârziere, respectiva înregistrare. Autoritatea centrală și autoritatea națională de supraveghere șterg astfel de înregistrări după trei ani de la crearea lor.

Articolul 26

Cooperarea în vederea respectării drepturilor privind protecția datelor

(1) Autoritățile centrale cooperează reciproc în vederea asigurării respectării drepturilor prevăzute la articolul 25.

(2) În fiecare stat membru, autoritatea națională de supraveghere oferă persoanei interesate, la cerere, informații privind modul de exercitare a dreptului său de a obține rectificarea sau ștergerea datelor care o privesc, în conformitate cu normele aplicabile ale Uniunii în materie de protecție a datelor.

(3) În sensul prezentului articol, autoritatea națională de supraveghere a statului membru care a transmis datele și autoritatea națională de supraveghere din statul membru căruia i s-a adresat cererea cooperează între ele.

Articolul 27

Căi de atac

Orice persoană are dreptul de a depune o plângere și dreptul la o cale de atac în statul membru de condamnare care a refuzat dreptul de acces sau dreptul de rectificare sau de ștergere a datelor referitoare la persoana respectivă, menționat la articolul 25, în conformitate cu dreptul intern sau al Uniunii.

Articolul 28

Supravegherea de către autoritatea națională de supraveghere

(1) Fiecare stat membru se asigură că autoritățile naționale de supraveghere desemnate în temeiul normelor aplicabile ale Uniunii în materie de protecție a datelor monitorizează legalitatea prelucrării datelor cu caracter personal menționate la articolele 5 și 6 de către statul membru în cauză, inclusiv transmiterea acestora către și dinspre ECRIS-TCN.

(2) Autoritatea națională de supraveghere asigură efectuarea unui audit al operațiunilor de prelucrare a datelor în bazele de date naționale ale cazierelor judiciare și dactiloscopice privind schimbul de date dintre respectivele sisteme și ECRIS-TCN în conformitate cu standardele internaționale de audit corespunzătoare cel puțin o dată la fiecare trei ani de la data începerii funcționării ECRIS-TCN.

(3) Statele membre se asigură că autoritățile lor naționale de supraveghere au resurse suficiente pentru a îndeplini sarcinile care le-au fost încredințate în conformitate cu prezentul regulament.

(4) Fiecare stat membru comunică toate informațiile solicitate de autoritățile naționale de supraveghere și, în special, le comunică acestora informații privind activitățile desfășurate în conformitate cu articolele 12, 13 și 19. Fiecare stat membru acordă autorităților naționale de supraveghere accesul la înregistrările sale în temeiul articolului 25 alineatul (7) și la fișierele sale de evidență în temeiul articolului 31 alineatul (6) și le permite în orice moment accesul la toate incintele sale aferente ECRIS-TCN.

Articolul 29

Supravegherea de către Autoritatea Europeană pentru Protecția Datelor

(1) Autoritatea Europeană pentru Protecția Datelor monitorizează îndeplinirea în conformitate cu prezentul regulament a activităților de prelucrare a datelor cu caracter personal desfășurate de eu-LISA cu privire la ECRIS-TCN.

(2) Autoritatea Europeană pentru Protecția Datelor asigură efectuarea unui audit al operațiunilor de prelucrare a datelor cu caracter personal desfășurate de eu-LISA, în conformitate cu standardele internaționale de audit corespunzătoare, cel puțin o dată la trei ani. Un raport al acestui audit se trimite Parlamentului European, Consiliului, Comisiei, eu-LISA și autorităților de supraveghere. Eu-LISA i se oferă posibilitatea de a face observații înainte de adoptarea raportului.

(3) Eu-LISA comunică informațiile cerute de către Autoritatea Europeană pentru Protecția Datelor, acordându-i acces la toate documentele și la fișierele de evidență prevăzute la articolul 31 și asigurându-i accesul la toate incintele sale, în orice moment.

Articolul 30

Cooperarea dintre autoritățile naționale de supraveghere și Autoritatea Europeană pentru Protecția Datelor

O supraveghere coordonată a ECRIS-TCN se asigură în conformitate cu articolul 62 din Regulamentul (UE) 2018/1725.

Articolul 31

Ținerea evidențelor

(1) Eu-LISA și autoritățile competente se asigură, în conformitate cu responsabilitățile lor respective, că se ține evidența tuturor operațiunilor de prelucrare din ECRIS-TCN, în conformitate cu alineatul (2), pentru a verifica admisibilitatea solicitărilor și a monitoriza integritatea și securitatea datelor și legalitatea prelucrării datelor, precum și în scopul automonitorizării.

(2) Fișierul de evidență indică:

(a) scopul cererii de acces la datele ECRIS-TCN;

(b) datele transmise, astfel cum sunt menționate la articolul 5;

(c) numărul de referință din arhivele naționale;

(d) data și ora exactă a operațiunii;

(e) datele utilizate pentru o interogare;

(f) datele de identificare ale agentului care a efectuat căutarea.

(3) Fișierul de evidență a consultărilor și a informațiilor furnizate permite stabilirea motivelor care justifică operațiunile respective.

(4) Fișierele de evidență sunt folosite doar pentru a monitoriza legalitatea prelucrării datelor și pentru a garanta integritatea și securitatea datelor. Doar fișierele de evidență care conțin date fără caracter personal pot fi folosite în vederea monitorizării și evaluării menționate la articolul 36. Aceste fișiere de evidență sunt protejate, prin măsuri adecvate, împotriva accesului neautorizat și sunt șterse după o perioadă de trei ani, în cazul în care nu mai sunt necesare pentru proceduri de monitorizare deja inițiate.

(5) La cerere, eu-LISA pune la dispoziția autorităților centrale fișierele de evidență a propriilor operațiuni de prelucrare, fără întârzieri nejustificate.

(6) Autoritățile naționale de supraveghere competente care sunt responsabile de verificarea admisibilității cererii și de monitorizarea legalității prelucrării datelor, precum și de integritatea și securitatea datelor au acces la fișierele de evidență, la cerere, în scopul îndeplinirii atribuțiilor care le revin. La cerere, autoritățile centrale pun la dispoziția autorităților naționale de supraveghere competente fișierele de evidență a propriilor operațiuni de prelucrare, fără întârzieri nejustificate.

CAPITOLUL VI

Dispoziții finale

Articolul 32

Utilizarea datelor în scopul întocmirii de rapoarte și statistici

(1) Personalul autorizat în mod corespunzător al eu-LISA, autoritățile competente și Comisia au acces la datele prelucrate în cadrul ECRIS-TCN exclusiv în scopul elaborării de rapoarte și statistici, fără a permite identificarea persoanelor.

(2) În sensul alineatului (1), eu-LISA întocmește, pune în aplicare și găzduiește în propriile sedii tehnice un registru central care conține datele menționate la alineatul (1) și care, fără a permite identificarea persoanelor, ar face posibilă în schimb elaborarea unor rapoarte și statistici configurabile. Accesul la registrul central se realizează sub forma unui acces securizat, cu controlul accesului și prin profiluri de utilizator specifice, exclusiv în scopul elaborării de rapoarte și statistici.

(3) Procedurile instituite de eu-LISA pentru a monitoriza funcționarea ECRIS-TCN menționate la articolul 36, precum și aplicația de referință a ECRIS includ posibilitatea de a elabora statistici periodice în scopuri de monitorizare.

În fiecare lună, eu-LISA transmite Comisiei statistici referitoare la înregistrarea, stocarea și schimbul de informații extrase din cazierele judiciare prin intermediul ECRIS-TCN și al aplicației de referință a ECRIS. Eu-LISA se asigură că nu este posibilă identificarea individuală pe baza acestor statistici. La cererea Comisiei, eu-LISA pune la dispoziția acesteia statistici privind aspecte specifice legate de punerea în aplicare a prezentului regulament.

(4) Statele membre pun la dispoziția eu-LISA statisticile necesare pentru ca aceasta să-și îndeplinească obligațiile prevăzute la prezentul articol. Acestea pun la dispoziția Comisiei statistici cu privire la numărul resortisanților țărilor terțe condamnați, precum și la numărul de condamnări ale resortisanților țărilor terțe pe teritoriul lor.

Articolul 33

Costuri

(1) Costurile aferente instituirii și operării sistemului central, infrastructurii de comunicații menționate la articolul 4 alineatul (1) litera (d), interfeței software și aplicației de referință a ECRIS sunt suportate din bugetul general al Uniunii.

(2) Costurile conectării Eurojust, a Europol și a EPPO la ECRIS-TCN sunt suportate din bugetele proprii ale acestora.

(3) Alte costuri sunt suportate de statele membre, în special costurile generate de conectarea registrelor naționale de cazier judiciare existente, a bazelor de date dactiloscopice și a autorităților centrale la ECRIS-TCN, precum și costurile aferente găzduirii aplicației de referință a ECRIS.

Articolul 34

Notificări

(1) Fiecare stat membru notifică eu-LISA autoritatea sa centrală sau autoritățile care au acces în ceea ce privește introducerea, rectificarea, ștergerea, consultarea datelor sau efectuarea de căutări în date, precum și orice modificări în acest sens.

(2) Eu-LISA asigură publicarea listei autorităților centrale, astfel cum au fost notificate de statele membre, atât în *Jurnalul Oficial al Uniunii Europene* cât și pe site-ul său de internet. Atunci când primește o notificare privind o modificare a unei autorități centrale a unui stat membru, eu-LISA actualizează lista fără întârzieri nejustificate.

Articolul 35

Introducerea datelor și începerea funcționării

(1) De îndată ce Comisia constată că următoarele condiții au fost îndeplinite, stabilește data de la care statele membre încep să introducă datele menționate la articolul 5 în ECRIS-TCN:

(a) actele relevante de punere în aplicare prevăzute la articolul 10 au fost adoptate;

(b) statele membre au validat schemele tehnice și juridice necesare pentru colectarea și transmiterea datelor prevăzute la articolul 5 către ECRIS-TCN și au notificat aceste scheme Comisiei;

(c) eu-LISA a efectuat un test complet al ECRIS-TCN, în cooperare cu statele membre, utilizând date-test anonime.

(2) După ce stabilește data de începere a perioadei de introducere a datelor în conformitate cu alineatul (1), Comisia comunică respectiva dată statelor membre. În termen de două luni de la data respectivă, statele membre introduc datele menționate la articolul 5 în ECRIS-TCN, ținând seama de articolul 41 alineatul (2).

(3) După încheierea perioadei menționate la alineatul (2), eu-LISA efectuează un test final al ECRIS-TCN, în cooperare cu statele membre.

(4) Atunci când testul menționat la alineatul (3) este finalizat cu succes, iar eu-LISA consideră că ECRIS-TCN este gata pentru începerea funcționării, aceasta notifică Comisia. Comisia informează Parlamentul European și Consiliul cu privire la rezultatele testului și decide data de la care ECRIS-TCN urmează să își înceapă funcționarea.

(5) Decizia Comisiei cu privire la data începerii funcționării ECRIS-TCN, astfel cum este menționată la alineatul (4), se publică în *Jurnalul Oficial al Uniunii Europene*.

(6) Statele membre încep să utilizeze ECRIS-TCN de la data stabilită de Comisie în conformitate cu alineatul (4).

(7) La luarea deciziilor prevăzute la prezentul articol, Comisia poate să precizeze date diferite pentru introducerea în ECRIS-TCN a datelor alfanumerice și a datelor dactiloscopice, astfel cum sunt menționate la articolul 5, precum și pentru demararea operațiunilor legate de respectivele categorii diferite de date.

Articolul 36

Monitorizare și evaluare

(1) Eu-LISA se asigură că există proceduri pentru a monitoriza dezvoltarea ECRIS-TCN din perspectiva obiectivelor legate de planificare și costuri și pentru a monitoriza funcționarea ECRIS-TCN și a aplicației de referință a ECRIS din perspectiva obiectivelor legate de rezultatele tehnice, eficacitatea costurilor, securitate și calitatea serviciilor.

(2) Pentru a asigura monitorizarea funcționării ECRIS-TCN și a întreținerii tehnice, eu-LISA are acces la informațiile necesare legate de operațiunile de prelucrare a datelor efectuate în cadrul ECRIS-TCN și al aplicației de referință a ECRIS.

(3) Până la 12 decembrie 2019 și, ulterior, la fiecare șase luni în etapele de proiectare și dezvoltare, eu-LISA prezintă Parlamentului European și Consiliului un raport cu privire la situația curentă a dezvoltării ECRIS-TCN și a aplicației de referință a ECRIS.

(4) Raportul menționat la alineatul (3) include o imagine de ansamblu a costurilor și a progreselor curente ale proiectului, o evaluare a impactului financiar, precum și informații cu privire la orice problemă tehnică și la riscurile care ar putea avea un impact asupra costurilor totale ale ECRIS-TCN care trebuie suportate de bugetul general al Uniunii, în conformitate cu articolul 33.

(5) În cazul unor întârzieri substanțiale în procesul de dezvoltare, eu-LISA informează Parlamentul European și Consiliul cât mai curând posibil cu privire la motivele acestor întârzieri, precum și cu privire la implicațiile financiare și temporale ale acestora.

(6) După încheierea fazei de dezvoltare a ECRIS-TCN și a finalizării aplicației de referință a ECRIS, eu-LISA prezintă Parlamentului European și Consiliului un raport în care se explică modul în care au fost realizate obiectivele, în special cele legate de planificare și costuri, și în care se justifică eventualele abateri.

(7) În cazul unei actualizări tehnice a ECRIS-TCN, care ar putea conduce la costuri substanțiale, eu-LISA informează Parlamentul European și Consiliul.

(8) După doi ani de la începerea funcționării ECRIS-TCN și, ulterior, în fiecare an, eu-LISA prezintă Comisiei un raport privind funcționarea tehnică a ECRIS-TCN și a aplicației de referință a ECRIS, inclusiv în ceea ce privește securitatea acestora, în special pe baza datelor statistice privind funcționarea și utilizarea ECRIS-TCN și privind schimbul de informații extrase din cazierele judiciare prin intermediul aplicației de referință a ECRIS.

(9) După patru ani de la începerea funcționării ECRIS-TCN și, ulterior, la fiecare patru ani, Comisia realizează o evaluare globală a ECRIS-TCN și a aplicației de referință a ECRIS. Raportul de evaluare globală întocmit pe această bază include o evaluare a aplicării prezentului regulament și o examinare a rezultatelor obținute în raport cu obiectivele stabilite și impactul asupra drepturilor fundamentale. Raportul include, de asemenea, o evaluare pentru a stabili dacă raționamentul care stă la baza operării ECRIS-TCN este în continuare valabil, a caracterului adecvat al utilizării datelor biometrice pentru ECRIS-TCN, a securității ECRIS-TCN și a oricăror implicații în materie de securitate asupra operațiunilor viitoare. Evaluarea include orice recomandare necesară. Comisia transmite raportul Parlamentului European, Consiliului, Autorității Europene pentru Protecția Datelor și Agenției pentru Drepturi Fundamentale a Uniunii Europene.

(10) În plus, prima evaluare globală, astfel cum este menționată la alineatul (9), include o evaluare a:

(a) măsurii în care, pe baza datelor statistice relevante și a informațiilor suplimentare din partea statelor membre, introducerea în ECRIS-TCN a informațiilor privind identitatea unor cetățeni ai Uniunii care dețin și cetățenia unei țări terțe a contribuit la îndeplinirea obiectivelor prezentului regulament;

(b) posibilității, pentru unele state membre, de a continua să utilizeze software-ul național de implementare a ECRIS, astfel cum este menționat la articolul 4;

(c) introducerii datelor dactiloscopice în ECRIS-TCN, în special a aplicării criteriilor minime prevăzute la articolul 5 alineatul (1) litera (b) punctul (ii);

(d) impactului ECRIS și al ECRIS-TCN asupra protecției datelor cu caracter personal.

Evaluarea poate fi însoțită, dacă este cazul, de propuneri legislative. Evaluările globale ulterioare pot include o evaluare a unuia sau a tuturor acestor aspecte.

(11) Statele membre, Eurojust, Europol și EPPO transmit eu-LISA și Comisiei informațiile necesare întocmirii rapoartelor menționate la alineatele (3), (8) și (9), conform indicatorilor cantitativi predefiniți de către Comisie, de către eu-LISA sau de către ambele. Aceste informații nu periclitează metodele de lucru și nici nu includ informații care dezvăluie sursele, membrii personalului sau investigațiile.

(12) Atunci când este cazul, autoritățile de supraveghere transmit eu-LISA și Comisiei informațiile necesare întocmirii rapoartelor menționate la alineatul (9), conform indicatorilor cantitativi predefiniți de către Comisie, de către eu-LISA sau de către ambele. Aceste informații nu periclitează metodele de lucru și nici nu includ informații care dezvăluie sursele, membrii personalului sau investigațiile.

(13) eu-LISA transmite Comisiei informațiile necesare pentru realizarea evaluărilor globale menționate la alineatul (9).

Articolul 37

Exercitarea delegării de competențe

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

(2) Competența de a adopta acte delegate menționată la articolul 6 alineatul (2) se conferă Comisiei pe o perioadă nedeterminată de la 11 iunie 2019.

(3) Delegarea de competențe menționată la articolul 6 alineatul (2) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe 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 menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional 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 6 alineatul (2) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții 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 obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 38

Procedura comitetului

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

(2) Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

În cazul în care comitetul nu emite niciun 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 39

Grupul consultativ

Eu-LISA înființează un grup consultativ pentru a obține cunoștințe de specialitate referitoare la ECRIS-TCN și la aplicația de referință a ECRIS, în special în contextul pregătirii programului său anual de lucru și a raportului său anual de activitate. În cursul fazei de proiectare și dezvoltare, se aplică articolul 11 alineatul (9).

Articolul 40

Modificarea Regulamentului (UE) 2018/1726

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

1. La articolul 1, alineatul (4) se înlocuiește cu următorul text:

„(4) Agenția este responsabilă de pregătirea, dezvoltarea sau gestionarea operațională a Sistemului de intrare/ieșire (EES), a DubliNet, a Sistemului european de informații și de autorizare privind călătoriile (ETIAS), a ECRIS-TCN și a aplicației de referință a ECRIS."

2. Se introduce următorul articol:

„*Articolul 8a*

Atribuții legate de ECRIS-TCN și de aplicația de referință a ECRIS

În ceea ce privește ECRIS-TCN și aplicația de referință a ECRIS, agenția îndeplinește:

(a) atribuțiile care i-au fost conferite prin Regulamentul (UE) 2019/816 al Parlamentului European și al Consiliului (*);

(b) atribuții legate de formarea privind utilizarea tehnică a sistemului ECRIS-TCN și a aplicației de referință a ECRIS.

(*) 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 dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor (ECRIS-TCN), destinat să completeze sistemul european de informații cu privire la cazierele judiciare, și de modificare a Regulamentului (UE) 2018/1726 (JO L 135, 22.5.2019, p. 1)."

3. La articolul 14, alineatul (1) se înlocuiește cu următorul text:

„(1) Agenția monitorizează evoluțiile din domeniul cercetării care sunt relevante pentru gestionarea operațională a SIS II, a VIS, a Eurodac, a EES, a ETIAS, a DubliNet, a ECRIS-TCN și a altor sisteme informatice la scară largă, după cum se menționează la articolul 1 alineatul (5)."

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

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

„(ee) adoptă rapoartele privind dezvoltarea EES în temeiul articolului 72 alineatul (2) din Regulamentul (UE) 2017/2226, rapoartele privind dezvoltarea ETIAS în temeiul articolului 92 alineatul (2) din Regulamentul (UE) 2018/1240 și rapoartele privind dezvoltarea ECRIS-TCN și a aplicației de referință a ECRIS în temeiul articolului 36 alineatul (3) din Regulamentul (UE) 2019/816;";

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

„(ff) adoptă rapoartele privind funcționarea tehnică a SIS II, în temeiul articolului 50 alineatul (4) din Regulamentul (CE) nr. 1987/2006 și, respectiv, al articolului 66 alineatul (4) din Decizia 2007/533/JAI, a VIS, în temeiul articolului 50 alineatul (3) din Regulamentul (CE) nr. 767/2008 și al articolului 17 alineatul (3) din Decizia 2008/633/JAI, a EES, în temeiul articolului 72 alineatul (4) din Regulamentul (UE) 2017/2226, a ETIAS în temeiul articolului 92 alineatul (4) din Regulamentul (UE) 2018/1240 și a ECRIS-TCN și a aplicației de referință a ECRIS în temeiul articolului 36 alineatul (8) din Regulamentul (UE) 2019/816;";

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

„(hh) „adoptă observații formale privind rapoartele de audit ale Autorității Europene pentru Protecția Datelor desfășurate în temeiul articolului 45 alineatul (2) din Regulamentul (CE) nr. 1987/2006, al articolului 42 alineatul (2) din Regulamentul (CE) nr. 767/2008 și 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 și al articolului 29 alineatul (2) din Regulamentul (UE) 2019/816 și asigură transpunerea în practică corespunzătoare a rezultatelor auditurilor respective;";

(d) se introduce următoarea literă:

„(lla) transmite Comisiei statistici referitoare la ECRIS-TCN și la aplicația de referință a ECRIS în temeiul articolului 32 alineatul (3) al doilea paragraf din Regulamentul (UE) 2019/816;";

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

„(mm) asigură publicarea anuală a listei autorităților competente autorizate să consulte direct datele introduse în SIS II, în temeiul articolului 31 alineatul (8) din Regulamentul (CE) nr. 1987/2006 și al articolului 46 alineatul (8) din Decizia 2007/533/JAI, precum și a listei oficiilor sistemelor naționale ale SIS II (oficiile N. SIS II) și a birourilor SIRENE, în temeiul articolului 7 alineatul (3) din Regulamentul (CE) nr. 1987/2006 și, respectiv, al articolului 7 alineatul (3) din Decizia 2007/533/JAI, precum și a listei autorităților competente, în temeiul articolului 65 alineatul (2) din Regulamentul (UE) 2017/2226, a listei autorităților competente, în temeiul articolului 87 alineatul (2) din Regulamentul (UE) 2018/1240 și a listei autorităților centrale, în temeiul articolului 34 alineatul (2) din Regulamentul (UE) 2019/816;".

5. La articolul 22 alineatul (4), după al treilea paragraf se introduce un nou paragraf cu următorul text:

„Eurojust, Europol și EPPO pot participa la reuniunile consiliului de administrație în calitate de observatori atunci când pe ordinea de zi figurează o chestiune referitoare la sistemul ECRIS-TCN în legătură cu aplicarea Regulamentului (UE) 2019/816".

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

„(p) stabilirea, fără a aduce atingere articolului 17 din Statutul funcționarilor, a 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 și a articolul 11 alineatul (16) din Regulamentul (UE) 2019/816;".

7. La articolul 27 alineatul (1), se introduce următoarea literă:

„(da) grupul consultativ al ECRIS-TCN;".

Articolul 41

Punere în aplicare și dispoziții tranzitorii

(1) Statele membre iau măsurile necesare pentru a se conforma prezentului regulament cât mai curând posibil, pentru a asigura buna funcționare a ECRIS-TCN.

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

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

(b) datele dactiloscopice sunt introduse în sistemul central în termen de doi ani de la începerea funcționării în conformitate cu articolul 35 alineatul (4).

Articolul 42

Intrare în vigoare

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

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

Adoptat la Strasbourg, 17 aprilie 2019.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*
A. TAJANI	G. CIAMBA

ANEXĂ

FORMULAR STANDARD DE CERERE DE INFORMAȚII ASTFEL CUM ESTE MENȚIONAT LA ARTICOLUL 17 ALINEATUL (1) DIN REGULAMENTUL (UE) 2019/816 ÎN VEDEREA OBȚINERII DE INFORMAȚII CU PRIVIRE LA STATUL MEMBRU AL UE CARE POATE DEȚINE INFORMAȚII CU PRIVIRE LA CAZIERELE JUDICIARE ALE UNUI RESORTISANT AL UNEI ȚĂRI TERȚE

Acest formular, disponibil la adresa www.eurojust.europa.eu în toate cele 24 de limbi oficiale ale instituțiilor Uniunii, ar trebui transmis, în una dintre aceste limbi, în atenția ECRIS-TCN@eurojust.europa.eu

Statul solicitant sau organizația internațională solicitantă:

Numele statului sau al organizației internaționale:
Autoritatea care depune cererea:
Reprezentată de (*numele persoanei*):
Titlu:
Adresă:
Număr de telefon:
Adresa de e-mail:

Procese penale pentru care sunt solicitate informațiile:

Numărul intern de referință:
Autoritatea competentă:
Tipul de infracțiuni în curs de investigare [*vă rugăm să menționați articolul (articolele) relevant(e) din Codul penal*]:
Alte informații relevante (*de exemplu, urgența cererii*):

Informații privind identitatea persoanei care deține cetățenia unei țări terțe în cazul căreia sunt solicitate informații privind statul membru de condamnare:

NB: vă rugăm să furnizați cât mai multe informații posibile.

Numele (*de familie*):
Prenumele:
Data nașterii:
Locul nașterii (*localitatea și țara*):
Cetățenia sau cetățeniile:
Genul:
Numele anterior (anterioare), dacă este cazul:
Numele părinților:
Numărul de identificare:
Tipul și numărul documentului (documentelor) de identificare al(e) persoanei:
Autoritatea emitentă a documentului (documentelor):
Pseudonimul sau numele de împrumut:
În cazul în care amprentele digitale sunt disponibile, vă rugăm să le furnizați.

În cazul mai multor persoane, vă rugăm să le indicați separat

O listă derulantă ar permite adăugarea unor subiecte suplimentare

Locul	
Data	

Semnătura și ștampila (în versiune electronică):

REGULAMENTUL (UE) 2019/817 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 20 mai 2019

privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații 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

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16 alineatul (2), articolul 74 și articolul 77 alineatul (2) literele (a), (b), (d) și (e),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European ([1]),

după consultarea Comitetului Regiunilor,

hotărând în conformitate cu procedura legislativă ordinară ([2]),

întrucât:

(1) În comunicarea sa din 6 aprilie 2016 intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”, Comisia a subliniat faptul că arhitectura de gestionare a datelor din Uniune în materie de gestionare a frontierelor și de securitate trebuie îmbunătățită. În urma acestei comunicări a început un proces care vizează asigurarea interoperabilității dintre sistemele de informații ale UE în materie de securitate, frontiere și gestionarea migrației, în vederea abordării deficiențelor structurale legate de sistemele respective care împiedică autoritățile naționale să își desfășoare activitatea și în vederea accesului polițiștilor de frontieră, al autorităților vamale, al agenților de poliție și al autorităților judiciare la informațiile de care au nevoie.

(2) În Foaia de parcurs pentru a consolida schimbul de informații și gestionarea informațiilor, inclusiv soluțiile de interoperabilitate, în domeniul justiției și afacerilor interne din 6 iunie 2016, Consiliul a identificat diferite provocări juridice, tehnice și operaționale pe care le presupune asigurarea interoperabilității sistemelor de informații ale UE și a făcut apel la căutarea unor soluții.

(3) În Rezoluția sa din 6 iulie 2016 privind prioritățile strategice ale programului de lucru al Comisiei pentru 2017 ([3]), Parlamentul European a solicitat Comisiei să prezinte propuneri pentru îmbunătățirea și dezvoltarea sistemelor de informații existente, pentru abordarea lacunelor în materie de informații și pentru asigurarea tranziției către interoperabilitate, precum și propuneri privind obligativitatea schimbului de informații la nivelul UE, însoțite de garanțiile necesare în materie de protecție a datelor.

(4) În concluziile sale din 15 decembrie 2016, Consiliul European a îndemnat la continuarea asigurării interoperabilității sistemelor de informații și ale bazelor de date ale UE.

(5) În raportul său final din 11 mai 2017, Grupul de experți la nivel înalt pentru sistemele de informații și interoperabilitate a concluzionat că este necesar și posibil din punct de vedere tehnic să se găsească soluții practice pentru realizarea interoperabilității și că aceasta ar putea, în principiu, să ofere câștiguri operaționale, și, totodată, să fie instituite în conformitate cu cerințele în materie de protecție a datelor.

([1]) JO C 283, 10.8.2018, p. 48.
([2]) Poziția Parlamentului European din 16 aprilie 2019 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 14 mai 2019.
([3]) JO C 101, 16.3.2018, p. 116.

(6) În comunicarea sa din 16 mai 2017 intitulată Al șaptelea raport referitor la progresele înregistrate pentru realizarea unei uniuni a securității efective și reale, Comisia a prezentat, în conformitate cu comunicarea sa din 6 aprilie 2016 și cu constatările și recomandările Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate, o nouă abordare privind gestionarea datelor în materie de frontiere, securitate și migrație, în care toate sistemele UE de informații privind securitatea, frontierele și gestionarea migrației urmau să fie interoperabile, într-o manieră care respectă în deplinătate drepturile fundamentale.

(7) În concluziile sale din 9 iunie 2017 privind calea de urmat pentru îmbunătățirea schimbului de informații și asigurarea interoperabilității sistemelor de informații ale UE, Consiliul a invitat Comisia să caute în continuare soluții pentru interoperabilitate, astfel cum a propus grupul de experți la nivel înalt.

(8) În concluziile sale din 23 iunie 2017, Consiliul European a subliniat necesitatea îmbunătățirii interoperabilității între bazele de date și a invitat Comisia să elaboreze un proiect legislativ pe baza propunerilor făcute de Grupul de experți la nivel înalt pentru sistemele de informații și interoperabilitate, cât mai curând posibil.

(9) Pentru îmbunătățirea eficacității și eficienței verificărilor la frontierele externe, pentru participarea la prevenirea și combaterea imigrației ilegale și la asigurarea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție al Uniunii, inclusiv menținerea securității și a ordinii publice și pentru garantarea securității pe teritoriul statelor membre, pentru a îmbunătăți punerea în aplicare a politicii comune a vizelor, pentru a facilita examinarea cererilor de protecție internațională, pentru a contribui la prevenirea, depistarea și investigarea infracțiunilor de terorism și a altor infracțiuni grave, pentru a facilita identificarea persoanelor cu identitate necunoscută care nu se pot legitima sau a rămășițelor umane neidentificate în cazul unui dezastru natural, al unui accident sau al unui atac terorist, cu scopul de a păstra încrederea publicului în sistemul Uniunii din domeniul migrației și al azilului, în măsurile Uniunii din domeniul securității și în capacitatea Uniunii de gestionare a frontierelor externe, ar trebui realizată interoperabilitatea dintre sistemele de informații ale Uniunii, și anume Sistemul de intrare/ieșire (EES), Sistemul de informații privind vizele (VIS), Sistemul european de informații și de autorizare privind călătoriile (ETIAS), Eurodac, Sistemul de informații Schengen (SIS) și Sistemul european de informații cu privire la cazierele judiciare pentru resortisanții țărilor terțe (ECRIS-TCN), astfel încât aceste sisteme de informații ale UE și datele pe care le conțin să se completeze reciproc respectându-se totodată drepturile fundamentale ale persoanelor, în special dreptul la protecția datelor cu caracter personal. Pentru a realiza acest lucru, ar trebui instituite componentele de interoperabilitate: un portal european de căutare (ESP), un serviciu comun de comparare a datelor biometrice (BMS comun), un registru comun de date de identitate (CIR) și un detector de identități multiple (MID).

(10) Interoperabilitatea dintre sistemele de informații ale UE ar trebui să permită completarea reciprocă pentru a facilita identificarea corectă a persoanelor, inclusiv a persoanelor cu identitate necunoscută care nu se pot legitima sau a rămășițelor umane neidentificate, pentru a contribui la combaterea fraudelor de identitate, pentru a îmbunătăți și armoniza cerințele de calitate a datelor prevăzute în respectivele sisteme de informații ale UE, pentru a facilita implementarea tehnică și operațională a sistemelor de informații ale UE, pentru a consolida garanțiile în materie de securitate și protecție a datelor prevăzute de respectivele sisteme de informații ale UE, pentru a simplifica accesul în scopul prevenirii, depistării sau investigării infracțiunilor de terorism ori a altor infracțiuni grave la EES, VIS, ETIAS și Eurodac și pentru a îndeplini obiectivele EES, VIS, ETIAS, Eurodac, SIS și ale ECRIS-TCN.

(11) Componentele de interoperabilitate ar trebui să vizeze EES, VIS, ETIAS, Eurodac, SIS și ECRIS-TCN. Acestea ar trebui, de asemenea, să vizeze datele Europol, dar numai pentru a permite ca datele Europol să fie interogate în același timp prin intermediul respectivelor sisteme de informații ale UE.

(12) Componentele de interoperabilitate ar trebui să prelucreze datele personale ale persoanelor ale căror date cu caracter personal sunt prelucrate în sistemele de informații de bază ale UE și de către Europol.

(13) ESP ar trebui instituit pentru a facilita din punct de vedere tehnic accesul rapid, fără sincope, eficient, sistematic și controlat al autorităților statelor membre și al agențiilor Uniunii la sistemele de informații ale UE, datele Europol și bazele de date ale Organizației Internaționale de Poliție Criminală (Interpol), în măsura în care acest lucru este necesar pentru a-și îndeplini sarcinile în conformitate cu drepturile lor de acces. ESP ar trebui de asemenea instituit pentru a susține obiectivele EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN și ale datelor Europol. Permițând interogarea în paralel a tuturor sistemelor de informații ale UE relevante, a datelor Europol și a bazelor de date ale

Interpol, ESP ar trebui să funcționeze ca un ghișeu unic sau ca un „broker de mesaje” prin care să se interogheze diverse sisteme centrale și să se extragă fără probleme informațiile necesare, cu respectarea deplină a cerințelor privind controlul accesului și protecția datelor care se aplică sistemelor de bază.

(14) Concepția ESP ar trebui să asigure faptul că, atunci când se lansează interogări în bazele de date ale Interpol, datele utilizate de către un utilizator ESP pentru a lansa o interogare nu sunt partajate cu proprietarii datelor Interpol. Modul în care este conceput ESP asigură, de asemenea, faptul că bazele de date ale Interpol sunt interogate doar în conformitate cu dreptul Uniunii și dreptul intern aplicabil.

(15) Cu ajutorul bazei de date a Interpol privind documentele de călătorie pierdute și furate (baza de date SLTD), entitățile autorizate responsabile de prevenirea, depistarea sau investigarea infracțiunilor de terorism ori a altor infracțiuni grave din statele membre, inclusiv funcționarii din cadrul serviciilor de imigrare și autoritățile responsabile de controlul la frontieră, pot stabili autenticitatea unui document de călătorie. ETIAS interoghează baza de date SLTD și baza de date Interpol privind documentele de călătorie asociate unor notițe (baza de date TDAWN) pentru a evalua dacă o persoană care solicită o autorizație de călătorie ar putea, de exemplu, să migreze în mod neregulamentar sau ar putea constitui o amenințare la adresa securității. ESP ar trebui să permită interogarea bazelor de date SLTD și TDAWN folosindu-se datele de identitate ale unei persoane sau datele din documentele de călătorie. În cazul transferului de date cu caracter personal din Uniune către Interpol prin intermediul ESP, se aplică dispozițiile privind transferurile internaționale din capitolul V din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([4]) sau dispozițiile naționale de transpunere a capitolului V din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului ([5]). Aceasta nu ar trebui să aducă atingere normelor specifice stabilite în Poziția comună 2005/69/JAI a Consiliului ([6]) și în Decizia 2007/533/JAI a Consiliului ([7]).

(16) ESP ar trebui astfel dezvoltat și configurat încât, pentru interogări, să nu permită utilizarea câmpurilor de date care nu sunt legate de persoane sau de documente de călătorie sau care nu sunt prezente într-un sistem de informații al UE, în datele Europol sau în baza de date a Interpol.

(17) Pentru a asigura utilizarea sistematică a sistemelor relevante de informații ale UE, ESP ar trebui utilizat pentru efectuarea de interogări în CIR, EES, VIS, ETIAS, Eurodac și în ECRIS-TCN. Cu toate acestea, o conexiune națională la diferitele sisteme de informații ale UE ar trebui menținută ca soluție tehnică alternativă. ESP ar trebui, de asemenea, să fie utilizat de către agențiile Uniunii pentru a efectua interogări în SIS central, cu respectarea drepturile lor de acces, pentru a-și îndeplini sarcinile. ESP ar trebui să fie un mijloc suplimentar de a efectua interogări în SIS central, în datele Europol și în bazele de date Interpol, care să completeze interfețele dedicate deja existente.

(18) Pentru identificarea unei persoane, datele biometrice, precum amprentele digitale și imaginile faciale, sunt unice și, prin urmare, mult mai fiabile decât datele alfanumerice. BMS comun ar trebui să fie un instrument tehnic care să consolideze și să faciliteze activitatea sistemelor de informații ale UE relevante și a celorlalte componente de interoperabilitate. Obiectivul esențial al BMS comun ar trebui să fie facilitarea identificării unei persoane care este înregistrată în mai multe baze de date, prin folosirea unei singure componente tehnologice pentru compararea datelor biometrice ale persoanei respective, în loc de mai multe componente. BMS comun ar trebui să contribuie la securitate și să aducă beneficii financiare, de întreținere și operaționale. Toate sistemele automate de identificare a amprentelor digitale, inclusiv cele utilizate în prezent pentru Eurodac, VIS și SIS, utilizează șabloane biometrice care conțin date ce provin dintr-o extragere de caracteristici a unor eșantioane biometrice efective. BMS comun ar trebui să regrupeze și să stocheze toate aceste șabloane biometrice, separate în mod logic, în funcție de sistemul de informații din care provin datele, în același loc, facilitând astfel comparațiile între sisteme prin utilizarea de șabloane biometrice și permițând obținerea unor economii de scară în dezvoltarea și întreținerea sistemelor centrale ale Uniunii.

([4]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([5]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

([6]) Poziția comună 2005/69/JAI a Consiliului din 24 ianuarie 2005 privind schimbul de anumite date cu Interpol (JO L 27, 29.1.2005, p. 61).

([7]) Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II) (JO L 205, 7.8.2007, p. 63).

(19) Șabloanele biometrice stocate în BMS comun, care ar trebui să conțină date ce provin dintr-o extragere de caracteristici a unor eșantioane biometrice efective, ar trebui să fie obținute în așa fel încât procesul de extragere să nu poată fi inversat. Șabloanele biometrice ar trebui obținute din datele biometrice, însă nu ar trebui să fie posibil să se obțină aceleași date biometrice plecând de la șabloanele biometrice. Întrucât datele privind amprentele palmare și profilurile ADN sunt stocate doar în SIS, și nu pot fi utilizate pentru a efectua verificări încrucișate cu datele existente în alte sisteme de informații, urmând principiile necesității și proporționalității, BMS comun nu ar trebui să stocheze profiluri ADN sau șabloane biometrice obținute din datele privind amprentele palmare.

(20) Datele biometrice reprezintă date cu caracter personal sensibile. Prezentul regulament ar trebui să stabilească baza și garanțiile privind prelucrarea unor astfel de date pentru identificarea univocă a persoanelor în cauză.

(21) EES, VIS, ETIAS, Eurodac și ECRIS-TCN necesită identificarea precisă a persoanelor ale căror date cu caracter personal sunt stocate în acestea. Prin urmare, CIR ar trebui să faciliteze identificarea corectă a persoanelor înregistrate în aceste sisteme.

(22) Datele cu caracter personal stocate în acele sisteme de informații ale UE pot face referire la aceleași persoane, dar cu identități diferite sau incomplete. Statele membre dispun de instrumente eficiente pentru identificarea cetățenilor sau a rezidenților permanenți înregistrați pe teritoriul lor. Interoperabilitatea dintre sistemele de informații ale UE ar trebui să contribuie la identificarea corectă a persoanelor prezente în sistemele respective. CIR ar trebui să stocheze datele cu caracter personal care sunt necesare pentru a permite o identificare mai precisă a persoanelor ale căror date sunt stocate în acele sisteme, inclusiv datele de identitate ale acestora, datele din documentul de călătorie al acestora și datele biometrice ale acestora, indiferent de sistemul în care au fost colectate inițial datele. În CIR ar trebui stocate doar datele cu caracter personal care sunt strict necesare pentru efectuarea unui control corect al identității. Datele cu caracter personal înregistrate în CIR nu ar trebui păstrate mai mult decât este strict necesar pentru îndeplinirea scopurilor pentru care au fost constituite sistemele de bază și ar trebui șterse în mod automat atunci când datele sunt șterse din sistemele de bază, respectându-se separarea lor logică.

(23) O nouă operațiune de prelucrare, care constă în stocarea acestor date în CIR și nu în fiecare dintre sistemele separate, este necesară pentru a face posibilă sporirea preciziei identificării, prin compararea automată a acestor date. Faptul că datele de identitate, datele din documentele de călătorie și datele biometrice sunt stocate în CIR nu ar trebui să împiedice în niciun fel prelucrarea datelor în EES, Eurodac, VIS, ETIAS, Eurodac sau ECRIS-TCN, întrucât CIR ar urma să fie o componentă comună nouă a acestor sisteme de bază.

(24) Prin urmare, este necesară crearea unui dosar individual în CIR pentru fiecare persoană înregistrată în EES, VIS, ETIAS, Eurodac sau ECRIS-TCN, pentru realizarea obiectivului de identificare corectă a persoanelor în spațiul Schengen și pentru sprijinirea MID atât pentru facilitarea controalelor de identitate pentru călătorii de bună credință, cât și pentru combaterea fraudelor de identitate. Dosarul individual ar trebui să stocheze toate informațiile privind identitatea legate de o persoană într-un singur loc și să le pună la dispoziția utilizatorilor finali autorizați în mod corespunzător.

(25) CIR ar trebui, așadar, să faciliteze și să eficientizeze accesul autorităților responsabile de prevenirea, depistarea sau investigarea infracțiunilor de terorism ori a altor infracțiuni grave la sistemele de informații ale UE care nu sunt instituite exclusiv în scopul prevenirii, detectării sau investigării infracțiunilor grave.

(26) CIR ar trebui să prevadă un sistem comun care să conțină datele de identitate, datele din documentele de călătorie și datele biometrice ale persoanelor care sunt înregistrate în EES, VIS, ETIAS, Eurodac și în ECRIS-TCN. Acesta ar trebui să facă parte din arhitectura tehnică a respectivelor sisteme și să servească drept componentă comună a acestora pentru stocarea și interogarea datelor de identitate, datelor din documentele de călătorie și a datelor biometrice pe care le prelucrează.

(27) Toate înregistrările din CIR ar trebui separate în mod logic prin atribuirea automată a unei etichete distinctive care să lege fiecare înregistrare de denumirea sistemului de bază care deține respectiva înregistrare. Sistemul de control al accesului la CIR ar trebui să utilizeze aceste etichete pentru a determina dacă permite accesul la înregistrarea respectivă.

(28) În cazul în care o autoritate de poliție a unui stat membru 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 sau în cazul în care există îndoieli cu privire la datele de identitate furnizate de persoana în cauză sau la autenticitatea documentului de călătorie ori la identitatea titularului său, sau în cazul în care persoana nu poate ori

refuză să coopereze, respectiva autoritate de poliție ar trebui să poată lansa interogări în CIR pentru a identifica persoana. În aceste scopuri, autoritățile de poliție ar trebui să preleve amprente folosind tehnici de amprentare electronică prin scanare în timp real, cu condiția ca procedura să fi fost inițiată în prezența persoanei respective. Astfel de interogări în CIR nu ar trebui să fie permise pentru identificarea minorilor cu vârsta mai mică de 12 ani, cu excepția cazului în care se urmărește interesul superior al copilului.

(29) În cazul în care datele biometrice ale unei persoane nu pot fi utilizate sau în cazul în care, în urma unei interogări a datelor respective, nu se obține niciun răspuns, interogarea ar trebui efectuată cu datele de identitate ale persoanei în combinație cu datele din documentul de călătorie. În cazul în care din interogare reiese că datele referitoare la persoana respectivă sunt înregistrate în CIR, autoritățile statelor membre ar trebui să aibă acces să consulte datele de identitate și datele din documentul de călătorie ale persoanei respective, fără ca CIR să furnizeze vreun indiciu cu privire la sistemul de informații al UE de care aparțin datele.

(30) Statele membre ar trebui să adopte măsuri legislative naționale prin care să desemneze autoritățile competente care vor efectua controale de identitate folosind CIR și prin care să stabilească procedurile, condițiile și criteriile pentru aceste controale, care ar trebui să respecte principiul proporționalității. în special, competența de a colecta date biometrice în cursul unui control al identității unei persoane aflate în fața unui reprezentant al acestor autorități ar trebui să fie prevăzută de dreptul intern.

(31) Prezentul regulament ar trebui, de asemenea, să introducă o nouă soluție pentru simplificarea accesului autorităților responsabile de prevenirea, depistarea sau investigarea infracțiunilor de terorism ori a altor infracțiuni grave desemnate de statele membre și al Europol și la alte tipuri de date din EES, VIS, ETIAS sau Eurodac în afară de datele de identitate sau datele din documentele de călătorie. Astfel de date pot fi necesare pentru prevenirea, detectarea sau investigarea infracțiunilor de terorism sau a altor infracțiuni grave într-un anumit caz în care există motive întemeiate să se considere că consultarea acestora va contribui în mod semnificativ la prevenirea, depistarea sau investigarea infracțiunilor de terorism sau a altor infracțiuni grave, în special în cazurile în care există suspiciunea că suspectul, autorul sau victima unei infracțiuni de terorism sau altei infracțiuni grave este o persoană ale cărei date sunt stocate în EES, VIS, ETIAS și Eurodac.

(32) Accesul deplin la datele conținute în EES, VIS, ETIAS sau Eurodac care este necesar în scopul prevenirii, depistării sau investigării infracțiunilor cu caracter terorist sau a altor infracțiuni grave, în afara accesului la datele de identitate la datele din documentele de călătorie care sunt păstrate în CIR ar trebui să fie în continuare reglementat de instrumentele juridice aplicabile. Nici autoritățile responsabile de prevenirea, depistarea sau investigarea infracțiunilor de terorism ori a altor infracțiuni grave desemnate, nici Europol nu știu dinainte care dintre sistemele de informații ale UE cuprinde date referitoare la persoanele care fac obiectul unei interogări. Acest lucru duce la întârzieri și deficiențe. Utilizatorul final autorizat de autoritatea desemnată ar trebui să aibă posibilitatea să vadă în care dintre acele sisteme de informații ale UE sunt înregistrate datele corespunzătoare rezultatului unei interogări. Sistemul în cauză ar fi, prin urmare, marcat după verificarea automată a prezenței unei concordanțe în sistem [o așa-numită funcționalitate – marcaj privind concordanța („match-flag”)].

(33) În acest context, un răspuns de la CIR nu ar trebui interpretat sau utilizat ca motiv sau cauză pentru a trage concluzii despre o persoană sau pentru a lua măsuri în legătură cu o persoană, ci ar trebui folosit doar pentru a adresa o cerere de acces la sistemele de informații de bază ale UE, cu respectarea condițiilor și a procedurilor prevăzute de instrumentele juridice respective care reglementează un astfel de acces. O astfel de cerere de acces ar trebui să facă obiectul capitolului VII din prezentul regulament și, după caz, Regulamentului (UE) 2016/679, Directivei (UE) 2016/680 sau Regulamentului (UE) 2018/1725 al Parlamentului European și al Consiliului ([8]).

(34) De regulă, atunci când un marcaj privind concordanța arată că datele sunt înregistrate în EES, VIS, ETIAS sau Eurodac, autoritățile desemnate sau Europol ar trebui să solicite acces deplin la cel puțin unul dintre sistemele de informații ale UE în cauză. În cazul în care, în mod excepțional, nu se solicită un astfel de acces deplin, de exemplu pentru că autoritățile desemnate sau Europol au obținut deja datele prin alte mijloace, sau pentru că dreptul intern nu mai permite obținerea datelor, ar trebui să se înregistreze motivele pentru nesolicitarea accesului.

([8]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

(35) Înregistrările interogărilor efectuate în CIR ar trebui să indice scopul acestora. În cazul în care o astfel de interogare a fost efectuată utilizându-se o abordare în două etape de consultare a datelor, înregistrările ar trebui să includă o trimitere la dosarul național al investigației sau al cazului, indicând astfel că interogarea a fost efectuată în scopul prevenirii, depistării sau investigării unor infracțiuni de terorism sau a altor infracțiuni grave.

(36) Efectuarea unei interogări în CIR de către autoritățile desemnate și de către Europol pentru a obține un răspuns de tip marcaj privind concordanța, prin care să se indice faptul că datele sunt înregistrate în EES, VIS, ETIAS sau în Eurodac, necesită prelucrarea automată a datelor cu caracter personal. Un marcaj privind concordanța ar trebui să nu dezvăluie datele cu caracter personal ale persoanei în cauză, ci numai să indice dacă anumite date referitoare la persoana respectivă sunt păstrate în vreunul dintre sisteme. Utilizatorul final autorizat nu ar trebui să ie nicio decizie în defavoarea persoanei în cauză bazându-se exclusiv pe apariția unui marcaj privind concordanța. Prin urmare, accesul utilizatorului final la un marcaj privind concordanța reprezintă o ingerință foarte limitată în dreptul persoanei vizate la protecția datelor cu caracter personal, permițând însă autorităților desemnate și Europol solicite acces la datele cu caracter personal într-un mod mai eficace.

(37) Ar trebui instituit MID pentru a sprijini funcționarea CIR și pentru a susține realizarea obiectivelor EES, VIS, ETIAS, Eurodac, SIS și ale ECRIS-TCN. Pentru a fi eficace în ceea ce privește îndeplinirea obiectivelor lor respective, toate aceste sisteme de informații ale UE necesită identificarea precisă a persoanelor ale căror date cu caracter personal sunt stocate în acestea.

(38) Pentru a realiza mai bine obiectivele sistemelor de informații ale UE, autoritățile care utilizează respectivele sisteme ar trebui să poată efectua verificări suficient de sigure cu privire la identitatea persoanelor ale căror date sunt înregistrate în diverse sisteme. Datele de identitate sau datele din documentele de călătorie stocate într-un anumit sistem pot fi incorecte, incomplete sau frauduloase, și în prezent nu există nicio modalitate de detectare a datelor de identitate sau a datelor din documentele de călătorie incorecte, incomplete sau frauduloase prin comparație cu datele stocate într-un alt sistem. Pentru a remedia această situație, este necesar ca la nivelul Uniunii să existe un instrument tehnic care să permită identificarea precisă a persoanelor în aceste scopuri.

(39) MID ar trebui să creeze și să stocheze conexiunile dintre datele stocate în diferitele sisteme de informații ale UE în vederea detectării identităților multiple, cu scopul dublu de a facilita controalele de identitate pentru călătorii de bună credință și, în același timp, de a combate fraudele de identitate. MID ar trebui să conțină exclusiv conexiunile dintre datele privind persoanele care sunt prezente în mai mult de un sistem de informații al UE. Datele conexate ar trebui să se limiteze în mod strict la datele necesare pentru a verifica dacă o persoană este înregistrată în mod justificat sau nejustificat cu mai multe identități diferite în sisteme diferite sau pentru a clarifica dacă două persoane cu date de identitate similare nu sunt, de fapt, aceeași persoană. Prelucrarea datelor prin intermediul ESP și al BMS comun în vederea stabilirii de conexiuni între dosarele din diferite sisteme ar trebui menținută la un nivel minim absolut și, prin urmare, ar trebui să se limiteze la o detectare a identităților multiple care trebuie efectuată la momentul adăugării de date noi în unul dintre sistemele care conțin date stocate în CIR sau la momentul adăugării de date noi în SIS. MID ar trebui să includă garanții împotriva unor eventuale cazuri de discriminare sau a unor decizii nefavorabile care vizează persoane cu identități multiple legale.

(40) Prezentul regulament prevede noi operațiuni de prelucrare a datelor care vizează identificarea corectă a persoanelor în cauză. Aceasta constituie o ingerință în drepturile fundamentale ale acestora, astfel cum sunt protejate prin articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene. Întrucât implementarea efectivă a sistemelor de informații ale UE depinde de identificarea corectă a persoanelor în cauză, o astfel de ingerință este justificată prin invocarea acelorași obiective ca și cele care stau la baza instituirii fiecăruia dintre aceste sisteme: gestionarea eficace a frontierelor Uniunii, securitatea internă a Uniunii și punerea în aplicare eficace a politicilor Uniunii în materie de azil și vize.

(41) Atunci când o autoritate națională sau o agenție a UE creează sau încarcă noi înregistrări, ESP și BMS comun ar trebui să compare datele privind persoanele în CIR și în SIS. O astfel de comparație ar trebui să fie automatizată. CIR și SIS ar trebui să utilizeze BMS comun pentru a detecta posibilele conexiuni pe baza datelor biometrice. CIR și SIS ar trebui să utilizeze ESP pentru a detecta posibilele conexiuni pe baza datelor alfanumerice. CIR și SIS ar trebui să fie în măsură să identifice datele care sunt aceleași sau similare privind o persoană stocate în mai multe sisteme. Dacă este cazul, ar trebui creată o conexiune care să indice că este vorba de aceeași persoană. CIR și SIS ar trebui astfel configurate încât greșelile minore de ortografie sau de transcriere să fie detectate, în așa fel încât să nu se creeze obstacole nejustificate pentru persoana în cauză.

(42) Autoritatea națională sau agenția Uniunii care a înregistrat datele respective în sistemul de informații ar trebui să confirme sau să modifice conexiunile. Această autoritate națională sau agenție a Uniunii ar trebui să aibă acces la datele stocate în CIR sau în SIS, precum și în MID, în scopul verificării manuale a identităților diferite.

(43) O verificare manuală a identităților diferite ar trebui asigurată de către autoritatea care a creat sau actualizat datele care au generat o concordanță, în urma căreia s-a stabilit o conexiune cu date înregistrate în alt sistem de informații al UE. Autoritatea responsabilă de verificarea manuală a identităților diferite ar trebui să evalueze dacă există mai multe identități care se referă la aceeași persoană într-un mod justificat sau nejustificat. Această evaluare ar trebui efectuată, acolo unde este posibil, în prezența persoanelor în cauză, solicitându-se, dacă este necesar, clarificări sau informații suplimentare. Evaluarea ar trebui efectuată fără întârziere, în conformitate cu cerințele legale privind exactitatea informațiilor în temeiul dreptului Uniunii și al dreptului intern. În special la frontiere, circulația persoanelor implicate va fi restricționată pe durata verificării, care nu ar trebui, prin urmare, să dureze pe o perioadă nedefinită. Existența unei conexiuni galbene în MID nu ar trebui să constituie în sine un motiv de refuz al intrării, iar orice decizie privind autorizarea sau refuzul intrării ar trebui să fie luată exclusiv în temeiul dispozițiilor aplicabile din Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului ([9]).

(44) Pentru conexiunile obținute prin intermediul SIS referitoare la semnalări privind persoane căutate în vederea arestării în scopul predării sau al extrădării, privind persoane dispărute sau vulnerabile, privind persoane căutate în vederea participării la o procedură judiciară sau privind persoane vizate pentru controale discrete, controale prin interviu sau controale specifice, autoritatea responsabilă cu verificarea manuală a identităților diferite ar trebui să fie biroul SIRENE din statul membru care a creat semnalarea. Aceste categorii de semnalări SIS sunt sensibile și nu ar trebui neapărat să facă obiectul unui schimb cu autoritățile care au creat sau actualizat datele care sunt în conexiune cu acestea din unul dintre celelalte sisteme de informații ale UE. Crearea unei conexiuni cu datele din SIS nu ar trebui să aducă atingere măsurilor care urmează să fie adoptate în conformitate cu Regulamentele (UE) 2018/1860 ([10]), (UE) 2018/1861 ([11]) și (UE) 2018/1862 ([12]) ale Parlamentului European și ale Consiliului.

(45) Crearea acestor conexiuni necesită transparență față de persoanele în cauză. Pentru a facilita punerea în aplicare a garanțiilor necesare în conformitate cu normele aplicabile ale Uniunii în materie de protecție a datelor, persoanele care sunt vizate de o conexiune roșie sau de o conexiune albă ca urmare a unei verificări manuale a identităților diferite ar trebui să fie informate în scris, fără a aduce atingere restricțiilor pentru protejarea securității și a ordinii publice, pentru prevenirea infracțiunilor și pentru garantarea faptului că nicio anchetă națională nu este pusă în pericol. Persoanele respective ar trebui să primească un număr unic de identificare, care să le permită să identifice autoritatea căreia ar trebui să i se adreseze pentru a-și exercita drepturile.

(46) În cazul în care se creează o conexiune galbenă, autoritatea responsabilă cu verificarea manuală a identităților diferite ar trebui să aibă acces la MID. În cazul în care există o conexiune roșie, autoritățile statelor membre și agențiile Uniunii care au acces la cel puțin un sistem de informații al UE inclus in CIR sau la SIS ar trebui să aibă acces la MID. O conexiune roșie ar trebui să indice faptul că o persoană utilizează identități diferite în mod nejustificat sau că o persoană utilizează identitatea unei alte persoane.

(47) Când există o conexiune albă sau verde între datele din două sisteme de informații ale UE, autoritățile statelor membre și agențiile Uniunii ar trebui să aibă acces la MID atunci când respectiva autoritate sau agenție are acces la ambele sisteme de informații. Acest acces ar trebui să se acorde exclusiv pentru a permite respectivei autorități sau agenții să detecteze cazurile potențiale în care datele au fost conexate incorect sau prelucrate în MID, CIR și SIS cu încălcarea prezentului regulament și pentru a lua măsurile pentru a remedia situația și a actualiza sau șterge conexiunea.

([9]) 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).

([10]) Regulamentul (UE) 2018/1860 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind utilizarea Sistemului de informații Schengen pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală (JO L 312, 7.12.2018, p. 1).

([11]) Regulamentul (UE) 2018/1861 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Convenției 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).

([12]) Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare și de 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).

(48) Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA) ar trebui să instituie mecanisme automatizate de control al calității datelor și indicatori comuni de calitate a datelor. În plus, ar trebui să fie responsabilă de dezvoltarea unei capacități centrale de monitorizare pentru calitatea datelor și de prezentarea în mod regulat de rapoarte de analiză a datelor în vederea îmbunătățirii controlului în ceea ce privește implementarea și utilizarea sistemelor de informații ale UE de către statele membre. Indicatorii comuni de calitate a datelor ar trebui să includă standarde minime de calitate pentru stocarea datelor în sistemele de informații ale UE sau în componentele de interoperabilitate. Scopul standardelor de calitate privind datele ar trebui să fie, pentru sistemele de informații ale UE sau pentru componentele de interoperabilitate, acela de a identifica într-un mod automatizat datele care par a fi incorecte sau inconsecvente, astfel încât statul membru din care provin să fie în măsură să le verifice și să ia măsurile necesare pentru a le corecta.

(49) Comisia ar trebui să evalueze rapoartele privind calitatea întocmite de eu-LISA și, după caz, ar trebui să formuleze recomandări adresate statelor membre. Statele membre ar trebui să fie responsabile cu pregătirea unui plan de acțiune care să descrie măsurile care vizează remedierea eventualelor deficiențe în ceea ce privește calitatea datelor și ar trebui să prezinte periodic progresele înregistrate.

(50) Formatul universal de mesaje (UMF) ar trebui să reprezinte un standard pentru schimburile de informații transfrontaliere structurate între sistemele de informații, autoritățile sau organizațiile din domeniul justiției și afacerilor interne. UMF ar trebui să definească un vocabular comun și structuri logice pentru informațiile care fac frecvent obiectul schimburilor, cu scopul de a facilita interoperabilitatea, permițând crearea și citirea conținutului în mod coerent și cu asigurarea echivalenței semantice.

(51) Aplicarea standardului UMF poate fi avută în vedere în VIS, SIS și în orice alt model de schimb transfrontalier de informații și sistem de informații în domeniul justiției și afacerilor interne, nou sau existent, elaborat de statele membre.

(52) Ar trebui înființat un registru central de raportare și statistici (CRRS) care să genereze date statistice între sisteme și rapoarte analitice în scopuri strategice, operaționale și de asigurare a calității datelor, în conformitate cu instrumentele juridice aplicabile. eu-LISA ar trebui să instituie, să implementeze și să găzduiască CRRS în amplasamentele sale tehnice. CRRS ar trebui să conțină date statistice anonime din sistemele de informații ale UE, CIR, MID și BMS comun. Datele conținute în CRRS nu ar trebui să permită identificarea persoanelor. eu-LISA ar trebui să anonimizeze într-un mod automat datele și ar trebui să înregistreze aceste date anonimizate în CRRS. Procesul de anonimizare a datelor ar trebui să fie automatizat, iar personalul eu-LISA nu ar trebui să aibă acces direct la datele cu caracter personal stocate în sistemele de informații ale UE sau în componentele de interoperabilitate.

(53) Regulamentul (UE) 2016/679 se aplică prelucrării datelor cu caracter personal în scopul interoperabilității efectuate în temeiul prezentului regulament de către autoritățile naționale, cu excepția cazului în care această prelucrare este efectuată de către autoritățile desemnate sau de către punctele centrale de acces din statele membre în scopul prevenirii, depistării sau investigării infracțiunilor de terorism sau a altor infracțiuni grave.

(54) În cazul în care prelucrarea datelor cu caracter personal de către statele membre în scopul interoperabilității în temeiul prezentului regulament este efectuată de către autoritățile competente în scopul prevenirii, depistării sau investigării infracțiunilor de terorism sau a altor infracțiuni grave, se aplică Directiva (UE) 2016/680.

(55) Regulamentul (UE) 2016/679, Regulamentul (UE) 2018/1725 sau, după caz, Directiva (UE) 2016/680 se aplică oricărui transfer de date cu caracter personal către state terțe sau organizații internaționale, efectuate în temeiul prezentului regulament. Fără a aduce atingere motivelor de transfer în temeiul capitolului V din Regulamentul (UE) 2016/679 sau, după caz, al Directivei (UE) 2016/680, orice hotărâre a unei instanțe sau a unui tribunal și orice decizie a unei autorități administrative a unei țări terțe care impun unui operator sau persoanei împuternicite de operator să transfere sau să divulge date cu caracter personal ar trebui să fie recunoscută sau executorie în orice fel numai dacă se bazează pe un acord internațional în vigoare între țara terță solicitantă și Uniune sau un stat membru.

(56) Dispozițiile specifice privind protecția datelor din Regulamentele (UE) 2017/2226 ([13]), (CE) nr. 767/2008 ([14]), (UE) 2018/1240 ([15]) ale Parlamentului European și ale Consiliului și Regulamentul (UE) 2018/1861se aplică prelucrării datelor cu caracter personal în sistemele guvernate de respectivele regulamente.

(57) Regulamentul (UE) 2018/1725 se aplică în cazul prelucrării datelor cu caracter personal de către eu-LISA și de către alte instituții și organisme ale Uniunii atunci când își exercită responsabilitățile care le revin în temeiul prezentului regulament, fără a aduce atingere dispozițiilor Regulamentului (UE) 2016/794 al Parlamentului European și al Consiliului ([16]), care se aplică prelucrării datelor cu caracter personal de către Europol.

(58) Autoritățile de supraveghere prevăzute în Regulamentul (UE) 2016/679 sau Directiva (UE) 2016/680 ar trebui să monitorizeze legalitatea prelucrării datelor cu caracter personal de către statele membre. Autoritatea Europeană pentru Protecția Datelor ar trebui să monitorizeze activitățile instituțiilor și organelor Uniunii în ceea ce privește prelucrarea datelor cu caracter personal. Autoritatea Europeană pentru Protecția Datelor și autoritățile de supraveghere ar trebui să coopereze între ele în cadrul activităților de monitorizare a prelucrării datelor de către componentele de interoperabilitate. Pentru ca Autoritatea Europeană pentru Protecția Datelor să îndeplinească sarcinile care i-au fost încredințate în temeiul prezentului regulament, sunt necesare resurse suficiente, atât umane, cât și financiare.

(59) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([17]) și a emis un aviz la 16 aprilie 2018 ([18]).

(60) Grupul de lucru instituit prin articolul 29 a emis un aviz la 11 aprilie 2018.

(61) Atât statele membre, cât și eu-LISA ar trebui să dispună de planuri de securitate pentru a facilita îndeplinirea obligațiilor privind securitatea și ar trebui să coopereze între ele pentru a aborda chestiunile legate de securitate. eu-LISA ar trebui, de asemenea, să se asigure că sunt valorificate permanent cele mai recente evoluții tehnologice pentru a asigura integritatea datelor în contextul dezvoltării, proiectării și gestionării componentelor de interoperabilitate. Printre obligațiile eu-LISA în acest sens ar trebui să se numere adoptarea măsurilor necesare pentru a împiedica accesul persoanelor neautorizate, cum ar fi angajații prestatorilor externi de servicii, la datele personale prelucrate prin intermediul componentelor de interoperabilitate. Atunci când atribuie contracte pentru prestarea de servicii, statele membre și eu-LISA ar trebui să ia în considerare toate măsurile necesare pentru a asigura respectarea actelor cu putere de lege și a reglementărilor referitoare la protecția datelor personale și la viața privată a persoanelor sau pentru a proteja interesele esențiale de securitate, în temeiul Regulamentului (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului ([19]) și cu convențiile internaționale aplicabile. eu-LISA ar trebui să aplice principiile protejării vieții private începând cu momentul conceperii și în mod implicit pe parcursul dezvoltării componentelor de interoperabilitate.

(62) Implementarea componentelor de interoperabilitate prevăzute în prezentul regulament vor avea un impact asupra modului în care se efectuează controalele la punctele de trecere a frontierei. Acest impact va fi rezultatul aplicării coroborate a normelor în vigoare prevăzute de Regulamentul (UE) 2016/399 și a normelor privind interoperabilitatea prevăzute în prezentul regulament.

(63) Ca o consecință a acestei aplicări combinate a normelor, ESP ar trebui să constituie principalul punct de acces pentru consultarea sistematică obligatorie a bazelor de date pentru persoane la punctele de trecere a frontierei prevăzută în Regulamentul (UE) 2016/399. În plus, polițiștii de frontieră care evaluează dacă o persoană

([13]) Regulamentul (UE) 2017/2226 al Parlamentului European și al Consiliului din 30 noiembrie 2017 de instituire a Sistemului de intrare/ieșire (EES) pentru înregistrarea datelor de intrare și de ieșire și a datelor referitoare la refuzul intrării ale resortisanților țărilor terțe care trec frontierele externe ale statelor membre, de stabilire a condițiilor de acces la EES în scopul aplicării legii și de modificare a Convenției de punere în aplicare a Acordului Schengen și a Regulamentelor (CE) nr. 767/2008 și (UE) nr. 1077/2011 (JO L 327, 9.12.2017, p. 20).

([14]) 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).

([15]) Regulamentul (UE) 2018/1240 al Parlamentului European și al Consiliului din 12 septembrie 2018 de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS) și de modificare a Regulamentelor (UE) nr. 1077/2011, (UE) nr. 515/2014, (UE) 2016/399, (UE) 2016/1624 și (UE) 2017/2226 (JO L 236, 19.9.2018, p. 1).

([16]) Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 24.5.2016, p. 53).

([17]) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

([18]) JO C 233, 4.7.2018, p. 12.

([19]) Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 privind normele financiare aplicabile bugetului general al Uniunii, de modificare a Regulamentelor (UE) nr. 1296/2013, (UE) nr. 1301/2013, (UE) nr. 1303/2013, (UE) nr. 1304/2013, (UE) nr. 1309/2013, (UE) nr. 1316/2013, (UE) nr. 223/2014, (UE) nr. 283/2014 și a Deciziei nr. 541/2014/UE și de abrogare a Regulamentului (UE, Euratom) nr. 966/2012 (JO L 193, 30.7.2018, p. 1).

îndeplinește condițiile de intrare definite în Regulamentul (UE) 2016/399 ar trebui să țină cont de datele de identitate sau de datele din documentele de călătorie care au condus la clasificarea unei conexiuni din MID ca fiind o conexiune roșie. Cu toate acestea, prezența unui conexiuni roșii nu ar trebui să constituie în sine un motiv de refuz al intrării și, așadar, motivele de refuz al intrării prevăzute în Regulamentul (UE) 2016/399 nu ar trebui să fie modificate.

(64) Manualul practic pentru polițiștii de frontieră ar trebui actualizat, astfel încât aceste precizări să fie explicite.

(65) În cazul în care, în urma interogării MID prin intermediul ESP, se identifică o conexiune galbenă sau roșie, polițistul de frontieră ar trebui să consulte CIR sau SIS, sau ambele, pentru a verifica informațiile privind persoana controlată, pentru a verifica manual diferitele sale identități și pentru a adapta culoarea conexiunii, dacă este necesar.

(66) În vederea sprijinirii întocmirii de statistici și rapoarte, este necesar ca personalul autorizat al autorităților competente, al instituțiilor și al agențiilor Uniunii menționate în prezentul regulament să aibă acces la anumite date referitoare la anumite componente de interoperabilitate, dar nu și la date care ar permite identificarea persoanelor.

(67) Pentru ca autoritățile din statele membre și agențiile Uniunii să se poată adapta noilor cerințe privind utilizarea ESP, este necesar să se prevadă o perioadă de tranziție. În mod similar, pentru a se asigura coerența și funcționarea optimă a MID, ar trebui stabilite măsuri tranzitorii pentru punerea în funcțiune a acestuia.

(68) Întrucât obiectivul prezentului regulament, și anume instituirea unui cadru de interoperabilitate între sistemele de informații ale Uniunii, nu poate fi realizat într-o măsură suficientă de statele membre, dar, având în vedere amploarea și efectele acțiunii, poate fi îndeplinit mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană (TUE). În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea acestui obiectiv.

(69) Suma rămasă din bugetul alocat frontierelor inteligente în Regulamentul (UE) nr. 515/2014 al Parlamentului European și al Consiliului ([20]) ar trebui realocată prezentului regulament, în temeiul articolului 5 alineatul (5) litera (b) din Regulamentul (UE) nr. 515/2014, pentru a acoperi costurile dezvoltării componentelor de interoperabilitate.

(70) Pentru a completa anumite aspecte tehnice detaliate ale prezentului regulament, competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene (TFUE) ar trebui să fie delegată Comisiei în ceea ce privește:

— prelungirea perioadei de tranziție pentru utilizarea ESP;

— prelungirea perioadei de tranziție pentru detectarea identităților multiple efectuată de unitatea centrală a ETIAS;

— procedurile de identificare a cazurilor în care datele de identitate pot fi considerate ca fiind aceleași sau similare;

— normele privind funcționarea CRRS, inclusiv garanții specifice pentru prelucrarea datelor cu caracter personal și normele de securitate aplicabile registrului;

— normele detaliate privind funcționarea portalului web.

Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare ([21]). În special, pentru a se asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(71) Pentru a asigura condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui conferite competențe de executare Comisiei în vederea stabilirii datelor de la care ESP, BMS comun, CIR, MID și CRRS trebuie să fie puse în funcțiune.

([20]) Regulamentul (UE) nr. 515/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 de instituire, în cadrul Fondului pentru securitate internă, a instrumentului de sprijin financiar pentru frontiere externe și vize și de abrogare a Deciziei nr. 574/2007/CE (JO L 150, 20.5.2014, p. 143).

([21]) JO L 123, 12.5.2016, p. 1.

(72) De asemenea, ar trebui conferite competențe de executare Comisiei în vederea adoptării unor norme detaliate privind: detaliile tehnice ale profilurilor utilizatorilor ESP; specificațiile soluției tehnice menite să permită interogarea sistemelor de informații ale UE, a datelor Europol și a bazelor de date ale Interpol prin ESP și formatul răspunsurilor ESP; normele tehnice de creare a unor conexiuni în MID între datele provenite de la diferitele sisteme de informații ale Uniunii; conținutul și prezentarea formularului care trebuie utilizat pentru informarea persoanei vizate în cazul în care este creată o conexiune roșie; cerințele în materie de performanță și monitorizarea performanței BMS comun; mecanismele și procedurile automatizate de control al calității datelor și indicatorii aferenți; dezvoltarea standardului UMF; procedura de cooperare în cazul unor incidente de securitate; și specificațiile soluției tehnice care dă statelor membre posibilitatea de a gestiona cererile de acces ale utilizatorilor. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([22]).

(73) Întrucât componentele de interoperabilitate vor presupune prelucrarea unor volume semnificative de date cu caracter personal sensibile, este important ca persoanele ale căror date sunt prelucrate prin intermediul acestor componente să își poată exercita în mod efectiv drepturile în calitate de persoane vizate, astfel cum se prevede în Regulamentul (UE) 2016/679, în Directiva (UE) 2016/680 și în Regulamentul (UE) 2018/1725. Persoanelor vizate ar trebui să li se pună la dispoziție un portal web care să le înlesnească exercitarea drepturilor de acces, de rectificare, de ștergere și de restricționare a prelucrării datelor lor cu caracter personal. eu-LISA ar trebui să creeze și să gestioneze un astfel de portal web.

(74) Unul dintre principiile de bază ale protecției datelor este reducerea la minimum a datelor: în temeiul articolului 5 alineatul (1) litera (c) din Regulamentul (UE) 2016/679, prelucrarea datelor cu caracter personal trebuie să fie adecvată, relevantă și limitată la ceea ce este necesar în raport cu scopurile în care sunt prelucrate. Din acest motiv, componentele de interoperabilitate ar trebui să nu prevadă stocarea oricăror date cu caracter personal noi, cu excepția conexiunilor care vor fi stocate în MID și care sunt minimumul necesar în scopul prezentului regulament.

(75) Prezentul regulament ar trebui să cuprindă dispoziții clare privind răspunderea și dreptul la despăgubiri în cazul prelucrării ilegale a datelor cu caracter personal sau al oricărui alt act incompatibil cu acesta. Astfel de dispoziții nu ar trebui să aducă atingere dreptului la despăgubiri ori răspunderii operatorului sau a persoanei împuternicite de operator în conformitate cu Regulamentul (UE) 2016/679, cu Directiva (UE) 2016/680 și cu Regulamentul (UE) 2018/1725. eu-LISA ar trebui să răspundă pentru orice prejudiciu pe care l-a cauzat în calitatea sa de persoană împuternicită de operator în cazul în care nu a respectat obligațiile care îi sunt impuse în mod specific de prezentul regulament sau în cazul în care a acționat în afara sau în contradicție cu instrucțiunile legale ale statului membru care este operator.

(76) Prezentul regulament nu aduce atingere aplicării Directivei 2004/38/CE a Parlamentului European și a Consiliului ([23]).

(77) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la TUE și la TFUE, Danemarca nu participă la adoptarea prezentului regulament, acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică. Deoarece prezentul regulament constituie o dezvoltare a acquis-ului Schengen, Danemarca decide, în conformitate cu articolul 4 din protocolul respectiv, în termen de șase luni de la data la care Consiliul decide cu privire la prezentul regulament dacă îl va pune în aplicare în legislația sa națională.

(78) Prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen la care Regatul Unit nu participă, în conformitate cu Decizia 2000/365/CE a Consiliului ([24]); prin urmare, Regatul Unit nu participă la adoptarea prezentului regulament, acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică.

(79) Prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen la care Irlanda nu participă, în conformitate cu Decizia 2002/192/CE a Consiliului ([25]); prin urmare, Irlanda nu participă la adoptarea prezentului regulament, acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică.

([22]) Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

([23]) Directiva 2004/38/CE a Parlamentului European și a Consiliului din 29 aprilie 2004 privind dreptul la liberă circulație și ședere pe teritoriul statelor membre pentru cetățenii Uniunii și membrii familiilor acestora, de modificare a Regulamentului (CEE) nr. 1612/68 și de abrogare a Directivelor 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE și 93/96/CEE (JO L 158, 30.4.2004, p. 77).

([24]) Decizia 2000/365/CE a Consiliului din 29 mai 2000 privind solicitarea Regatului Unit al Marii Britanii și Irlandei de Nord de a participa la unele dintre dispozițiile acquis-ului Schengen (JO L 131, 1.6.2000, p. 43).

([25]) Decizia 2002/192/CE a Consiliului din 28 februarie 2002 privind solicitarea Irlandei de a participa la unele dintre dispozițiile acquis-ului Schengen (JO L 64, 7.3.2002, p. 20).

(80) În ceea ce privește Islanda și Norvegia, prezentul regulament reprezintă o dezvoltare a dispozițiilor acquis-ului Schengen, în înțelesul Acordului încheiat între Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei privind asocierea acestora din urmă la implementarea, aplicarea și dezvoltarea acquis-ului Schengen ([26]), care intră sub incidența articolului 1 punctele A, B, C și G din Decizia 1999/437/CE a Consiliului ([27]).

(81) În ceea ce privește Elveția, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen, în înțelesul Acordului între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen ([28]), care se află sub incidența articolului 1 punctele A, B, C și G din Decizia 1999/437/CE, coroborat cu articolul 3 din Decizia 2008/146/CE a Consiliului ([29]).

(82) În ceea ce privește Liechtenstein, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Protocolului între Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen ([30]), care se află sub incidența articolului 1 punctele A, B, C și G din Decizia 1999/437/CE, coroborat cu articolul 3 din Decizia 2011/350/UE a Consiliului ([31]).

(83) Prezentul regulament respectă drepturile fundamentale și se conformează principiilor recunoscute, în special, de Carta drepturilor fundamentale a Uniunii Europene, și ar trebui să fie pus în aplicare în conformitate cu aceste drepturi și principii.

(84) Pentru ca prezentul regulament să se încadreze în cadrul juridic existent, regulamentele (CE) nr. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 și (UE) 2018/1861 și Deciziile 2004/512/CE ([32]) și 2008/633/JAI ([33]) ale Consiliului ar trebui modificate în consecință,

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

Dispoziții generale

Articolul 1

Obiect

(1) Prezentul regulament, împreună cu Regulamentul (UE) 2019/818 al Parlamentului European și al Consiliului ([34]), stabilește un cadru pentru a asigura interoperabilitatea dintre Sistemul de intrare/ieșire (EES), Sistemul de informații privind vizele (VIS), Sistemul european de informații și de autorizare privind călătoriile (ETIAS), Eurodac, Sistemul de informații Schengen (SIS) și Sistemul european de informații cu privire la cazierele judiciare ale resortisanților țărilor terțe (ECRIS-TCN).

([26]) JO L 176, 10.7.1999, p. 36.
([27]) Decizia 1999/437/CE a Consiliului din 17 mai 1999 privind anumite modalități de aplicare a Acordului încheiat între Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei în ceea ce privește asocierea acestor două state în vederea punerii în aplicare, a asigurării respectării și dezvoltării acquis-ului Schengen (JO L 176, 10.7.1999, p. 31).
([28]) JO L 53, 27.2.2008, p. 52.
([29]) Decizia 2008/146/CE a Consiliului din 28 ianuarie 2008 privind încheierea, în numele Comunității Europene, a Acordului între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen (JO L 53, 27.2.2008, p. 1).
([30]) JO L 160, 18.6.2011, p. 21.
([31]) Decizia 2011/350/UE a Consiliului din 7 martie 2011 privind încheierea, în numele Uniunii Europene, a Protocolului dintre Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen, în ceea ce privește eliminarea controalelor la frontierele interne și circulația persoanelor (JO L 160, 18.6.2011, p. 19).
([32]) Decizia 2004/512/CE a Consiliului din 8 iunie 2004 de instituire a Sistemului de Informații privind Vizele (VIS) (JO L 213, 15.6.2004, p. 5).
([33]) Decizia 2008/633/JAI a Consiliului din 23 iunie 2008 privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave (JO L 218, 13.8.2008, p. 129).
([34]) 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 (a se vedea pagina 85 din prezentul Jurnal Oficial).

(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 identități multiple (MID).

(3) Prezentul regulament cuprinde, de asemenea, dispoziții privind cerințele de calitate a datelor, formatul universal pentru mesaje (UMF), registrul central de raportare și statistici (CRRS) și responsabilitățile statelor membre și ale Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA) în ceea ce privește conceperea, dezvoltarea și funcționarea componentelor de interoperabilitate.

(4) Prezentul regulament adaptează totodată procedurile și condițiile în care autoritățile desemnate și Agenția 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 infracțiunilor de terorism sau a altor infracțiuni grave.

(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;

(f) raționalizarea condițiilor de acces al autorităților desemnate la EES, VIS, ETIAS și Eurodac, asigurând totodată condiții necesare și proporționale 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 EES, VIS, ETIAS și SIS.

(2) Prezentul regulament se aplică persoanelor ale căror date cu caracter personal pot fi prelucrate în sistemele de informații ale UE la care se face referire la alineatul (1) din prezentul articol și ale căror date sunt colectate în scopurile definite la articolele 1 și 2 din Regulamentul (CE) nr. 767/2008, la articolul 1 din Regulamentul (UE) 2017/2226, la articolele 1 și 4 din Regulamentul (UE) 2018/1240, la articolul 1 din Regulamentul (UE) 2018/1860 și la articolul 1 din Regulamentul (UE) 2018/1861.

Articolul 4

Definiții

În sensul prezentului regulament:

1. „frontiere externe” înseamnă frontierele externe, astfel cum sunt definite la articolul 2 punctul 2 din Regulamentul (UE) 2016/399;
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 polițistul de frontieră desemnat în conformitate cu dreptul intern să efectueze verificări la frontiere;
4. „autorități de supraveghere” înseamnă autoritatea de supraveghere menționată la articolul 51 alineatul (1) din Regulamentul (UE) 2016/679 și autoritatea de supraveghere menționată la articolul 41 alineatul (1) din Directiva (UE) 2016/680;
5. „verificare” înseamnă procesul de comparare a unor serii de date în vederea stabilirii autenticității unei identități declarate (controlul realizat prin compararea a două serii de date);
6. „identificare” înseamnă procesul de determinare a identității 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);
7. „date alfanumerice” înseamnă date constând în litere, cifre, caractere speciale, spații și semne de punctuație;
8. „date de identitate” înseamnă datele prevăzute la articolul 27 alineatul (3) literele (a)-(e);
9. „date dactiloscopice” înseamnă imagini de amprente digitale și imagini de amprente digitale latente care, datorită unicității lor și punctelor de referință pe care le conțin, permit comparații fiabile și concludente referitoare la identitatea unei persoane;
10. „imagine facială” înseamnă imagini digitale ale feței;
11. „date biometrice” înseamnă datele dactiloscopice sau imaginea facială sau ambele;
12. „șablon biometric” înseamnă o reprezentare matematică obținută 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, țara care l-a eliberat, data expirării perioadei de valabilitate a documentului de călătorie și codul din trei litere al țării care a eliberat documentul de călătorie;
15. „sisteme de informații 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 menționate 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 notițe (baza de date TDAWN);
18. „concordanță” înseamnă existența unei corespondențe 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 informații sau într-o bază de date;
19. „autoritate polițienească” înseamnă „autoritate competentă”, astfel cum este definită la articolul 3 punctul 7 din Directiva (UE) 2016/680;
20. „autorități desemnate” înseamnă autoritățile desemnate de statele membre, definite la articolul 3 alineatul (1) punctul 26 din Regulamentul (UE) 2017/2226, la articolul 2 alineatul (1) litera (e) din Decizia 2008/633/JAI și la articolul 3 alineatul (1) punctul 21 din Regulamentul (UE) 2018/1240;

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 ([35]) 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 ([36]) 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;

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 ([37]);

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 al Parlamentului European și al Consiliului ([38]).

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, apartenență la o minoritate națională, situație 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 vieții private și la protecția datelor cu caracter personal. Se acordă o atenție specială copiilor, persoanelor în vârstă, persoanelor cu handicap și persoanelor care au nevoie de protecție internațională. 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 autorităților statelor membre și al agențiilor Uniunii la sistemele de informații 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.

([35]) 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).

([36]) 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).

([37]) 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).

([38]) 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 dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor (ECRIS-TCN), destinat să completeze sistemul european de informații cu privire la cazierele judiciare și de modificare a Regulamentului (UE) 2018/1726 (a se vedea pagina 1 din prezentul Jurnal Oficial).

(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 comunicații între ESP, statele membre și agențiile Uniunii care au dreptul să utilizeze ESP;

(c) o infrastructură de comunicații 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.

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

Articolul 7

Utilizarea portalului european de căutare

(1) Utilizarea ESP este rezervată autorităților statelor membre și agențiilor Uniunii care au acces la cel puțin unul dintre sistemele de informații ale UE, în conformitate cu instrumentele juridice care reglementează aceste sisteme de informații 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 autorități ale statelor membre și agenții ale Uniunii pot utiliza ESP și datele furnizate de acesta exclusiv pentru obiectivele și scopurile prevăzute de instrumentele juridice care reglementează respectivele sisteme de informații ale UE, de Regulamentul (UE) 2016/794 și de prezentul regulament.

(2) Autoritățile statelor membre și agențiile Uniunii menționate la alineatul (1) utilizează ESP pentru a căuta date referitoare la persoane sau la documentele de călătorie ale acestora în sistemele centrale ale EES, VIS și ETIAS, în conformitate cu drepturile de acces de care beneficiază în temeiul instrumentelor juridice care reglementează aceste sisteme de informații 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 menționate la articolele 20, 21 și 22.

(3) Autoritățile statelor membre menționate la alineatul (1) pot utiliza ESP pentru a căuta date referitoare la persoane sau la documentele de călătorie ale acestora în SIS central menționat în Regulamentul (UE) 2018/1860 și în Regulamentul (UE) 2018/1861.

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

(5) Autoritățile statelor membre și agențiile Uniunii menționate la alineatul (1) pot utiliza ESP pentru a căuta date referitoare la documente de călătorie în bazele de date ale Interpol, atunci când dreptul intern și dreptul Uniunii prevăd acest lucru și 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 menționate la alineatul (2). Fiecare profil cuprinde, în conformitate cu dreptul Uniunii și dreptul intern următoarele informații:

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

(b) sistemele de informații 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 informații 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 menționate la alineatul (1), în conformitate cu drepturile de acces ale utilizatorilor ESP în temeiul instrumentelor juridice care reglementează sistemele de informații ale UE și în temeiul dreptului intern. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

(3) Profilurile menționate la alineatul (1) sunt revizuite cu regularitate de către eu-LISA în cooperare cu statele membre, cel puțin 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 funcție 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 informații 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 interfeței pe baza UMF menționat 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 conțin.

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

ESP nu furnizează nicio informație referitoare la datele din sistemele de informații 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.

(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 74 alineatul (2).

Articolul 10

Păstrarea înregistrărilor

(1) Fără a aduce atingere articolului 46 din Regulamentul (UE) 2017/2226, articolului 34 din Regulamentul (CE) nr. 767/2008, articolului 69 din Regulamentul (UE) 2018/1240 și articolelor 12 și 18 din Regulamentul (UE) 2018/1861, 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 bazele de date ale Interpol 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.

(2) În cazul în care, din cauza unei disfuncționalități a infrastructurii naționale 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 informații ale UE sau în CIR, statul membru respectiv notifică eu-LISA și Comisia în mod automat.

(3) În cazurile menționate la alineatele (1) și (2) din prezentul articol și până la remedierea problemei tehnice, obligația menționată la articolul 7 alineatele (2) și (4) nu se aplică, iar statele membre au acces la sistemele de informații 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 disfuncționalități a infrastructurii unei agenții 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 informații ale Uniunii sau în CIR, agenția 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 obținute pe baza datelor biometrice menționate la articolul 13 care sunt stocate în CIR și în SIS și permite efectuarea de interogări folosind date biometrice în mai multe sisteme de informații 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 comunicații 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 obține din următoarele date biometrice:

(a) datele menționate la articolul 16 alineatul (1) litera (d), la articolul 17 alineatul (1) literele (b) și (c) și la articolul 18 alineatul (2) literele (a), (b) și (c) din Regulamentul (UE) 2017/2226;

(b) datele menționate la articolul 9 alineatul (6) din Regulamentul (CE) nr. 767/2008;

(c) datele menționate la articolul 20 alineatul (2) literele (w) și (x) din Regulamentul (UE) 2018/1861, cu excepția datelor privind amprentele palmare;

(d) datele menționate la articolul 4 alineatul (1) literele (u) și (v) din Regulamentul (UE) 2018/1860, cu excepția datelor privind amprentele palmare;

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

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

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

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

(5) Prin intermediul unui act de punere în aplicare, Comisia stabilește cerințele de performanță pentru BMS comun și modalitățile practice de monitorizare a performanței 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 menționată la articolul 74 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 menționate 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.

Articolul 16

Păstrarea înregistrărilor

(1) Fără a aduce atingere articolului 46 din Regulamentul (UE) 2017/2226, articolului 34 din Regulamentul (CE) nr. 767/2008 și articolelor 12 și 18 din Regulamentul (UE) 2018/1861, 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.

(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 menționate la articolul 18;

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

(c) o infrastructură de comunicații 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 disfuncționalități 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 identități multiple în temeiul articolului 21 sau al prevenirii, depistării ori investigării infracțiunilor de terorism sau a altor infracțiuni grave în temeiul articolului 22, utilizatorii CIR sunt notificați în mod automat de către eu-LISA.

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

Articolul 18

Datele din registrul comun de date de identitate

(1) CIR stochează următoarele date, separate în mod logic, în funcție de sistemul de informații din care provin datele:

(a) datele menționate la articolul 16 alineatul (1) literele (a)-(d), la articolul 17 alineatul (1) literele (a), (b) și (c) și la articolul 18 alineatele (1) și (2) din Regulamentul (UE) 2017/2226;

(b) datele menționate la articolul 9 punctul 4 literele (a)-(c) și punctele 5 și 6 din Regulamentul (CE) nr. 767/2008;

(c) datele menționate la articolul 17 alineatul (2) literele (a)-(e) din Regulamentul (UE) 2018/1240.

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

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

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

(5) Stocarea datelor menționate 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 EES, VIS și ETIAS, datele menționate 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 informații 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 poliție, în conformitate cu alineatele (2) și (5), numai în următoarele circumstanțe:

(a) în cazul în care o autoritate de poliție 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.

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

(2) În cazul în care survine una dintre circumstanțele enumerate la alineatul (1) și o autoritate de poliție are competențe în acest sens în temeiul unor măsuri legislative naționale, astfel cum se menționează 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 condiția ca această procedură să fie inițiată în prezența persoanei respective.

(3) În cazul în care, în urma interogării, reiese că în CIR sunt stocate date referitoare la persoana respectivă, autoritatea de poliție are acces să consulte datele menționate 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 combinație 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 poliție are competențe în acest sens în temeiul unor măsuri legislative naționale, 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 rămășițelor 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 naționale. Cu această ocazie, statele membre iau în considerare necesitatea de a evita orice discriminare împotriva resortisanților țărilor terțe. Aceste măsuri legislative precizează scopurile precise ale identificării din cele menționate la articolul 2 alineatul (1) literele (b) și (c). Statele membre desemnează autoritățile de poliție competente și stabilesc procedurile, condițiile și criteriile aferente acestor controale.

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

Articolul 21

Accesul la registrul comun de date de identitate în scopul detectării de identități 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 identităților diferite în conformitate cu articolul 29 are acces, exclusiv în scopul verificării respective, la datele menționate la articolul 18 alineatele (1) și (2) stocate în CIR conexate printr-o conexiune galbenă.

(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 EES, VIS sau ETIAS, autoritățile desemnate și Europol pot consulta CIR pentru a afla dacă datele unei anumite persoane sunt prezente în EES, VIS și ETIAS.

(2) În cazul în care, ca răspuns la o interogare, CIR indică faptul că există date privind persoana respectivă în EES, VIS sau ETIAS, 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 în care dintre sistemele de informații ale UE există datele 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 oricare dintre sistemele de informații ale UE menționate în alineatul (1) poate fi utilizat numai în scopul de a depune o cerere de acces integral, conform condițiilor și procedurilor prevăzute de respectivele instrumente juridice 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 EES, VIS sau ETIAS în scopul prevenirii, depistării sau investigării infracțiunilor cu caracter terorist sau a altor infracțiuni grave rămâne supus condițiilor și procedurilor prevăzute în instrumentele juridice respective 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 Regulamentele (UE) 2017/2226, (CE) nr. 767/2008 și, respectiv, (UE) 2018/1240.

(2) Dosarul individual este stocat în CIR numai atât timp cât datele corespondente sunt stocate cel puțin într-unul din sistemele de informații 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 46 din Regulamentul (UE) 2017/2226, articolului 34 din Regulamentul (CE) nr. 767/2008 și articolului 69 din Regulamentul (UE) 2018/1240, eu-LISA păstrează înregistrări ale tuturor operațiunilor de prelucrare a datelor efectuate în CIR, în conformitate cu alineatele (2), (3) și (4) din prezentul articol.

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

(a) statul membru sau agenția 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 operațiunilor de prelucrare a datelor efectuate în CIR în temeiul articolului 21. În aceste înregistrări sunt incluse următoarele informații:

(a) statul membru sau agenția 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 informații al UE de la care s-au primit datele.

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

(a) data și ora efectuării interogării;

(b) datele utilizate pentru lansarea interogării;

(c) rezultatele interogării;

(d) statul membru sau agenția 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 Protecția 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 condițiile prevăzute la articolul 22 alineatele (1) și (2) din prezentul regulament.

(5) Fiecare stat membru păstrează înregistrările interogărilor efectuate de autoritățile sale și de personalul acestora autorizat în mod corespunzător să utilizeze CIR în temeiul articolelor 20, 21 și 22. Fiecare agenție 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) referința dosarului național;

(b) scopul accesării;

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

(7) Înregistrările menționate la alineatele (2)-(6) 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.

(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 identități multiple

Articolul 25

Detectorul de identități multiple

(1) Pentru a susține funcționarea CIR și a sprijini realizarea obiectivelor EES, VIS, ETIAS, Eurodac, SIS și ECRIS-TCN, se instituie un detector de identități multiple (MID), care creează și stochează dosare de confirmare a identității, astfel cum se menționează la articolul 34, și 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) autorităților competente desemnate în conformitate cu articolul 9 alineatul (2) din Regulamentul (UE) 2017/2226 atunci când creează sau actualizează un dosar individual în EES, în conformitate cu articolul 14 din regulamentul respectiv;

(b) autorităților responsabile în domeniul vizelor menționate la articolul 6 alineatul (1) din Regulamentul (CE) nr. 767/2008 atunci când creează sau actualizează un dosar individual în VIS, în conformitate cu regulamentul respectiv;

(c) unității centrale a ETIAS și unităților naționale ale ETIAS atunci când efectuează prelucrarea menționată la articolele 22 și 26 din Regulamentul (UE) 2018/1240;

(d) biroului SIRENE din statul membru atunci când creează sau actualizează o semnalare SIS în conformitate cu Regulamentele (UE) 2018/1860 și (UE) 2018/1861.

(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 un dosar individual în EES, în conformitate cu articolul 14 din Regulamentul (UE) 2017/2226;

(b) se creează sau se actualizează un dosar de cerere în VIS, în conformitate cu Regulamentul (CE) nr. 767/2008;

(c) se creează sau se actualizează un dosar de cerere în ETIAS în conformitate cu articolul 19 din Regulamentul (UE) 2018/1240;

(d) se creează sau se actualizează o semnalare în SIS privind o persoană, în conformitate cu articolul 3 din Regulamentul (UE) 2018/1860 și cu capitolul V din Regulamentul (UE) 2018/1861.

(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 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; data nașterii; cetățenia sau cetățeniile; și sexul, astfel cum se menționează la articolul 16 alineatul (1) litera (a), la articolul 17 alineatul (1) și la articolul 18 alineatul (1) din Regulamentul (UE) 2017/2226;

(b) numele (de familie); prenumele; data nașterii; sexul; locul și țara nașterii; și cetățeniile, astfel cum se menționează la articolul 9 punctul 4 literele (a) și (aa) din Regulamentul (CE) nr. 767/2008;

(c) numele (de familie), prenumele, numele (de familie) la naștere, numele de împrumut, data nașterii, locul nașterii, sexul și cetățenia actuală, astfel cum se menționează la articolul 17 alineatul (2) din Regulamentul (UE) 2018/1240;

(d) numele (de familie), prenumele, numele la naștere, numele folosite anterior și pseudonimele, locul nașterii, data nașterii, genul și orice cetățenii deținute, astfel cum se menționează la articolul 20 alineatul (2) din Regulamentul (UE) 2018/1861;

(e) numele (de familie), prenumele, numele la naștere, numele folosite anterior și pseudonimele, locul nașterii, data nașterii, genul și orice cetățenii deținute, astfel cum se menționează la articolul 4 din Regulamentul (UE) 2018/1860.

(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 obține(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.

(4) 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 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 73 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 identității menționat 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 informații ale UE. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

Articolul 29

Verificarea manuală a identităților diferite și autoritățile responsabile

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

(a) autoritatea competentă desemnată în conformitate cu articolul 9 alineatul (2) din Regulamentul (UE) 2017/2226 pentru concordanțe obținute la crearea sau actualizarea unui dosar individual în EES, în conformitate cu regulamentul respectiv;

(b) autoritățile responsabile în domeniul vizelor menționate la articolul 6 alineatul (1) din Regulamentul (CE) nr. 767/2008 pentru concordante obținute la crearea sau actualizarea unui dosar de cerere în VIS, în conformitate cu respectivul regulament;

(c) unitatea centrală a ETIAS și unitățile naționale ale ETIAS pentru concordanțe obținute la crearea sau actualizarea unui dosar de cerere, în conformitate cu Regulamentul (UE) 2018/1240;

(d) biroul SIRENE din statul membru pentru concordanțe obținute la crearea sau actualizarea unei semnalări în SIS, în conformitate cu Regulamentele (UE) 2018/1860 și (UE) 2018/1861.

MID indică autoritatea responsabilă de verificarea manuală a identităților diferite în dosarul de confirmare a identității.

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

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

(b) cu privire la persoane dispărute sau vulnerabile, menționată 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.

(3) Fără a aduce atingere alineatului (4) din prezentul articol, autoritatea responsabilă de verificarea manuală a identităților diferite are acces la datele conexate conținute 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 identitățile 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 autoritatea responsabilă de verificarea manuală a identităților diferite în dosarul de confirmare a identității este autoritatea competentă desemnată în conformitate cu articolul 9 alineatul (2) din Regulamentul (UE) 2017/2226 care a creat sau a actualizat un dosar individual în EES în conformitate cu articolul 14 din regulamentul respectiv și în cazul în care se creează o conexiune galbenă, autoritatea respectivă efectuează verificări suplimentare. Exclusiv în acest scop, autoritatea respectivă are acces la datele relevante de identitate conținute în dosarul de confirmare a identității relevant. Aceasta evaluează identitățile diferite, actualizează conexiunea în conformitate cu articolele 31, 32 și 33 din prezentul regulament și o adaugă fără întârziere la dosarul de confirmare a identității.

O astfel de verificare manuală a identităților diferite se inițiază în prezența persoanei în cauză, care trebuie să aibă posibilitatea de a explica circumstanțele în fața autorității responsabile, aceasta trebuind să ia în considerare explicațiile respective.

În cazul în care verificarea manuală a identităților diferite se face la frontieră, aceasta are loc în termen de 12 ore de la crearea unei legături galbene în temeiul articolului 28 alineatul (4), dacă este posibil.

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

(6) În cazul în care datele care au generat concordanța erau deja conexate, autoritatea responsabilă de verificarea manuală a identităților diferite ține 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 identităților diferite, o conexiune între datele din două sau mai multe sisteme de informații 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 puțin unul dintre sistemele de informații ale UE nu conține 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 informații 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 identităților 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 identităților diferite a ajuns la concluzia că datele conexate se referă la două persoane diferite;

(c) datele conexate au date de identitate diferite, dar au în comun aceleași date privind documentele de călătorie, cel puțin unul dintre sistemele de informații ale UE nu conține date biometrice privind persoana în cauză, iar autoritatea responsabilă de verificarea manuală a identităților 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 informații 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 deține 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 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.

Articolul 32

Conexiune roșie

(1) O conexiune între datele din două sau mai multe sisteme de informații 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 identităților 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 identităților diferite a ajuns la concluzia că datele conexate se referă la două persoane diferite dintre care cel puțin 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 identităților 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 puțin unul dintre sistemele de informații ale UE nu conține date biometrice privind persoana în cauză, iar autoritatea responsabilă de verificarea manuală a identităților diferite a ajuns la concluzia că datele conexate se referă în mod nejustificat la aceeași persoană.

(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 informații ale UE, MID indică datele menționate la articolul 34. Măsurile subsecvente creării unei conexiuni roșii se iau în conformitate cu dreptul Uniunii și cu dreptul intern, orice consecință juridică pentru persoana în cauză bazându-se exclusiv pe datele relevante privind persoana respectivă. Din simpla existență a unei conexiuni roșii nu derivă nicio consecință 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 dispozițiilor referitoare la gestionarea semnalărilor în SIS din Regulamentele (UE) 2018/1860, (UE) 2018/1861 și (UE) 2018/1862 și fără a aduce atingere restricțiilor necesare pentru protejarea securității și a ordinii publice, pentru prevenirea infracțiunilor și pentru garantarea faptului că nicio anchetă națională nu va fi pusă în pericol, în cazul în care se creează o conexiune roșie, autoritatea responsabilă de verificarea manuală a identităților diferite informează persoana în cauză cu privire la prezența unor date de identitate multiple ilegale și pune la dispoziția persoanei în cauză un număr de identificare unic, astfel cum este menționat la articolul 34 litera (c) din prezentul regulament, o trimitere la autoritatea responsabilă de verificarea manuală a identităților diferite, astfel cum este menționată 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) Informațiile menționate la 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 74 alineatul (2).

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

(7) În cazul în care o autoritate a unui stat membru sau o agenție 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 dispozițiilor prezentului regulament, autoritatea sau agenția respectivă verifică datele relevante stocate în CIR și SIS și:

(a) în cazul în care conexiunea se referă la una dintre semnalările SIS menționate 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 agenția Uniunii și, dacă este cazul, rectifică sau șterge conexiunea din MID imediat.

Autoritatea competentă a statului membru care obține dovezile informează fără întârziere autoritatea statului membru responsabil de verificarea manuală a identităților 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 informații 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 puțin unul dintre sistemele de informații 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 identităților 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 informații ale UE, MID indică faptul că datele de identitate ale datelor conexe corespund aceleiași persoane. Sistemele de informații ale UE în care s-a lansat interogarea răspund indicând, după caz, toate datele conexate referitoare la persoana respectivă și generând, prin urmare, o concordanță 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 dispozițiilor referitoare la gestionarea semnalărilor în SIS din Regulamentele (UE) 2018/1860, (UE) 2018/1861 și (UE) 2018/1862 și fără a aduce atingere restricțiilor necesare pentru protejarea securității și a ordinii publice, pentru prevenirea infracțiunilor și pentru garantarea faptului că nicio anchetă națională nu va fi pusă în pericol, în cazul în care este creată o conexiune albă în urma unei verificări manuale a unor identități diferite, autoritatea responsabilă de verificarea manuală a identităților diferite informează persoana în cauză cu privire la prezența unor date de identitate similare sau diferite și furnizează persoanei în cauză un număr de identificare unic, astfel cum este menționat la articolul 34 litera (c) din prezentul regulament, o trimitere către la autoritatea responsabilă de verificarea manuală a identităților diferite, astfel cum este menționată 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) 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 74 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;

(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 EES, VIS, ETIAS, SIS, 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 EES, VIS, ETIAS, SIS, BMS comun și CIR.

Numai datele care respectă standardele minime de calitate pot fi introduse în EES, VIS, ETIAS, SIS, 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 EES, VIS, ETIAS, SIS, 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 74 alineatul (2).

(5) La un an de la instituirea mecanismelor și procedurilor automatizate de control al calității 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 dispoziția Comisiei un plan de acțiune pentru remedierea deficiențelor identificate în raportul de evaluare și, în special, a problemelor de calitate a datelor cauzate de datele eronate din sistemele de informații ale UE. Statele membre raportează regulat Comisiei cu privire la progresele înregistrate în funcție de acest plan de acțiune până în momentul în care acesta este pus în aplicare pe deplin.

Comisia transmite raportul de evaluare Parlamentului European, Consiliului, Autorității Europene pentru Protecția Datelor, Comitetului european pentru protecția datelor și Agenției pentru Drepturi Fundamentale a Uniunii Europene instituită prin Regulamentul (CE) nr. 168/2007 al Consiliului ([39]).

Articolul 38

Formatul universal pentru mesaje

(1) Se instituie un format universal pentru mesaje (UMF). UMF definește standardele pentru anumite elemente de conținut ale schimbului transfrontalier de informații între sistemele de informații, autoritățile sau organizațiile participante din domeniul justiției și afacerilor interne.

(2) Standardul UMF se utilizează în dezvoltarea EES, a ETIAS, a ESP, a CIR, a MID și, dacă este necesar, în dezvoltarea de către eu-LISA sau de către orice altă agenție a Uniunii a unor noi modele de schimb de informații și sisteme de informații în domeniul justiției și afacerilor interne.

(3) Comisia adoptă un act de punere în aplicare pentru a stabili și dezvolta standardul UMF menționat la alineatul (1) din prezentul articol. Respectivul act de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

Articolul 39

Registrul central de raportare și statistici

(1) Se instituie un registru central de raportare și statistici (CRRS) în scopul de a susține obiectivele EES, VIS, ETIAS și SIS, în conformitate cu instrumentele juridice respective care reglementează sistemele menționate, și de a furniza date statistice utilizabile între sisteme și rapoarte analitice în scop operațional, de elaborare a politicilor și de asigurare a calității datelor.

(2) eu-LISA creează, implementează și găzduiește în amplasamentele sale tehnice CRRS care conține datele și statisticile menționate la articolul 63 din Regulamentul (UE) 2017/2226, articolul 17 din Regulamentul (CE) nr. 767/2008, articolul 84 din Regulamentul (UE) 2018/1240, articolul 60 din Regulamentul (UE) 2018/1861 și articolul 16 din Regulamentul (UE) 2018/1860, separate în mod logic pe sisteme de informații ale UE. 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, autorităților menționate la articolul 63 din Regulamentul (UE) 2017/2226, la articolul 17 din Regulamentul (CE) nr. 767/2008, la articolul 84 din Regulamentul (UE) 2018/1240 și la articolul 60 din Regulamentul (UE) 2018/1861.

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

Datele conținute 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 comunicații securizată pentru a conecta CRRS la EES, VIS, ETIAS și SIS, precum și la infrastructurile centrale ale BMS comun, CIR și MID.

(5) Comisia adoptă un act delegat în conformitate cu articolul 73 prin care stabilește norme detaliate privind funcționarea CRRS, inclusiv garanții specifice pentru prelucrarea datelor cu caracter personal în temeiul alineatelor (2) și (3) din prezentul articol și norme de securitate aplicabile registrului.

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

CAPITOLUL VII

Protecția datelor

Articolul 40

Operatorul de date

(1) În ceea ce privește prelucrarea datelor în BMS comun, autoritățile statelor membre care sunt operatori pentru EES, VIS, și, respectiv, SIS 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 obținute din datele menționate 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, autoritățile statelor membre care sunt operatori pentru EES, VIS, și, respectiv, ETIAS sunt operatori în conformitate cu articolul 4 punctul 7 din Regulamentul (UE) 2016/679 în ceea ce privește datele menționate 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.

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

(a) Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă este operator de date în înțelesul 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) autoritățile statelor membre care introduc sau modifică date în dosarul de confirmare a identității 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 protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, operatorii de date au acces la înregistrările menționate la articolele 10, 16, 24 și 36 pentru automonitorizarea menționată 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 înțelesul 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 autoritățile din statele membre asigură securitatea prelucrărilor de date cu caracter personal efectuate în temeiul prezentului regulament. eu-LISA, unitatea centrală a ETIAS, Europol și autoritățile 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 comunicații aferente.

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

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

(b) a interzice accesul persoanelor neautorizate la echipamentele și instalațiile 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;

(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.

(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 74 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:

(a) orice persoană sau stat membru care a suferit prejudicii materiale sau morale ca urmare a unei operațiuni ilegale de prelucrare a datelor cu caracter personal sau a oricărei alte acțiuni 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 acțiuni realizate de către Europol, Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă sau eu-LISA care este incompatibilă cu prezentul regulament are dreptul de a primi despăgubiri din partea agenției respective.

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

(2) Dacă orice nerespectare de către un stat membru a obligațiilor în temeiul prezentului regulament provoacă prejudicii componentelor de interoperabilitate, răspunderea aparține statului membru respectiv, cu excepția cazului în care eu-LISA sau un alt stat membru care are obligații 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 menționate 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 menționate la alineatele (1) și (2) fac obiectul condițiilor 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 dispoziția persoanelor ale căror date sunt colectate informațiile 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 informațiile la momentul colectării acestor date.

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

(3) Persoanele ale căror date sunt înregistrate în EES, VIS sau ETIAS sunt informate cu privire la prelucrarea datelor personale în sensul prezentului regulament, în conformitate cu alineatul (1) atunci când:

(a) se creează sau se actualizează un dosar individual în EES, în conformitate cu articolul 14 din Regulamentul (UE) 2017/2226;

(b) se creează sau se actualizează un dosar de cerere în VIS, în conformitate cu articolul 8 din Regulamentul (CE) nr. 767/2008;

(c) se creează sau se actualizează un dosar de cerere în ETIAS în conformitate cu articolul 19 din Regulamentul (UE) 2018/1240.

Articolul 48

Dreptul de acces, de rectificare și de ștergere a datelor cu caracter personal stocate în MID și dreptul la restricționarea 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 (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 de 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 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 model de e-mail pentru a facilita comunicarea între utilizatorul portalului și autoritatea competentă a statului membru responsabil de verificarea manuală a identităților diferite. Acest e-mail trebuie să includă un spațiu dedicat numărului de identificare unic menționat la articolul 34 litera (c) pentru a permite autorității competente a statului membru responsabil de verificarea manuală a identităților diferite să identifice datele în cauză.

(4) Statele membre comunică eu-LISA datele de contact ale tuturor autorităților care sunt competente să examineze și să răspundă oricărei cereri menționate 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 73 prin care adoptă norme detaliate privind funcționarea portalului web, inclusiv a interfeței pentru utilizatori, limbile în care acesta este disponibil și modelul de e-mail.

Articolul 50

Comunicarea datelor cu caracter personal către țări terțe, organizații internaționale și părți private

Fără a aduce atingere articolului 65 din Regulamentul (UE) 2018/1240, articolelor 25 și 26 din Regulamentul (UE) 2016/794, articolului 41 din Regulamentul (UE) 2017/2226, articolului 31 din Regulamentul (CE) nr. 767/2008 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 dispoziția unei țări terțe, a unei organizații internaționale sau a unei părți private.

Articolul 51

Supravegherea de către autoritățile de supraveghere

(1) Fiecare stat membru se asigură că autoritățile 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 naționale adoptate în temeiul Directivei (UE) 2016/680 sunt aplicabile, dacă este relevant, accesului autorităților polițienești și autorităților desemnate la componentele de interoperabilitate, inclusiv în ceea ce privește drepturile persoanelor ale căror date sunt accesate în acest mod.

(3) Autoritățile de supraveghere garantează că, cel puțin la fiecare patru ani, se realizează un audit al operațiunilor de prelucrare a datelor cu caracter personal de către autoritățile naționale responsabile, în sensul prezentului regulament, în conformitate cu standardele internaționale de audit relevante.

Autoritățile de supraveghere publică anual numărul solicitărilor de rectificare sau ștergere a datelor cu caracter personal sau de restricționare a prelucrării datelor cu caracter personal, acțiunile întreprinse ulterior și numărul rectificărilor, ștergerilor și restricționărilor prelucrării efectuate în urma solicitărilor depuse de persoanele în cauză.

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

(5) Statele membre oferă toate informațiile solicitate de autoritatea de supraveghere menționată la articolul 51 alineatul (1) din Regulamentul (UE) 2016/679 și, în special, îi comunică informații privind activitățile desfășurate în conformitate cu responsabilitățile lor, în temeiul prezentului regulament. Statele membre acordă autorităților de supraveghere menționate la articolul 51 alineatul (1) din Regulamentul (UE) 2016/679 acces la înregistrările lor menționate la articolele 10, 16, 24 și 36 din prezentul regulament, la motivele menționate la articolul 22 alineatul (2) din prezentul regulament și le permit în orice moment accesul în toate localurile proprii utilizate pentru asigurarea interoperabilității.

Articolul 52

Auditurile efectuate de Autoritatea Europeană pentru Protecția Datelor

Autoritatea Europeană pentru Protecția Datelor garantează că cel puțin o dată la patru ani se realizează un audit al operațiunilor 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 internaționale de audit relevante. Un raport al acestui audit se trimite Parlamentului European, Consiliului, eu-LISA, Comisiei, statelor membre și agenției Uniunii în cauză. eu-LISA, unității centrale ETIAS și Europol li se oferă posibilitatea de a face observații înainte de adoptarea rapoartelor.

eu-LISA, unitatea centrală a ETIAS și Europol pun la dispoziția Autorității Europene pentru Protecția Datelor informațiile solicitate de aceasta, oferă Autorității Europene pentru Protecția Datelor acces la toate documentele solicitate de aceasta și la înregistrările lor menționate la articolele 10, 16, 24 și 36, precum și la toate localurile proprii, în orice moment.

Articolul 53

Cooperarea dintre autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor

(1) Autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor, fiecare acționând în limitele competențelor sale, cooperează activ în cadrul responsabilităților lor și asigură o supraveghere coordonată a utilizării componentelor de interoperabilitate și aplicarea celorlalte dispoziții ale prezentului regulament, în special dacă Autoritatea Europeană pentru Protecția Datelor sau o autoritate de supraveghere identifică discrepanțe majore între practicile statelor membre sau transferuri potențial ilegale efectuate prin canalele de comunicare ale componentelor de interoperabilitate.

(2) În cazurile menționate 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 protecția datelor transmite Parlamentului European, Consiliului, Comisiei, Europol, Agenției Europene pentru Poliția de Frontieră și Garda de Coastă și eu-LISA un raport comun privind activitățile 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

Responsabilități

Articolul 54

Responsabilitățile 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 funcționalitățile prevăzute în prezentul regulament, în conformitate cu condițiile de securitate, disponibilitate, calitate și performanță prevăzute la articolul 55 alineatul (1).

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

Fără a aduce atingere articolului 66, 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 comunicații, precum și specificațiile tehnice și evoluția acestora în ceea ce privește infrastructura centrală și infrastructura de comunicații securizată, care sunt adoptate de către Consiliul de administrație, sub rezerva unui aviz favorabil din partea Comisiei. De asemenea, eu-LISA pune în aplicare orice adaptare necesară a EES, VIS, ETIAS sau SIS care rezultă din stabilirea interoperabilității 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 78 alineatul (10).

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

(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 75, 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 76 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.

Articolul 55

Responsabilitățile eu-LISA după punerea în funcțiune

(1) După punerea în funcțiune a fiecărei componente de interoperabilitate, eu-LISA este responsabilă de gestionarea tehnică a infrastructurii centrale a componentelor de interoperabilitate, inclusiv de întreținerea acestora și de evoluțiile 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 comunicații menționate la articolele 6, 12, 17, 25 și 39.

Gestionarea tehnică a componentelor de interoperabilitate cuprinde toate sarcinile și soluțiile tehnice necesare pentru a menține în funcțiune componentele de interoperabilitate și asigurând servicii neîntrerupte statelor membre și agențiilor Uniunii 24 de ore pe zi, șapte zile pe săptămână, în conformitate cu prezentul regulament. Gestionarea tehnică trebuie să includă lucrările de întreținere și dezvoltările tehnice necesare pentru a se asigura funcționarea 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 specificațiile 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 operaționale ale autorităților statelor membre și ale agențiilor Uniunii.

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

Fără a aduce atingere articolului 66, 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 întreține un mecanism și proceduri de verificare a calității 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

Responsabilitățile 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 naționale existente cu ESP, CIR și MID.

(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 alineatele (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 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 69.

CAPITOLUL IX

Modificarea altor instrumente ale Uniunii

Articolul 58

Modificarea Regulamentului (CE) nr. 767/2008

Regulamentul (CE) nr. 767/2008 se modifică după cum urmează:

1. La articolul 1 se adaugă următorul alineat:

„Prin faptul că stochează date de identitate, date privind documentele de călătorie și date biometrice în registrul comun de date de identitate (CIR) instituit prin articolul 17 alineatul (1) din Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului (*), VIS contribuie la facilitarea și acordarea de asistență în vederea identificării corecte a persoanelor înregistrate în VIS în condițiile și în scopurile de la articolul 20 din regulamentul menționat.

(*) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații 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).”

2. La articolul 4 se adaugă următoarele puncte:

„12. «date din VIS» înseamnă toate datele stocate în sistemul central al VIS și în CIR în conformitate cu articolele 9-14.

13. «date de identitate» înseamnă datele prevăzute la articolul 9 alineatul (4) literele (a) și (aa);

14. «date dactiloscopice» înseamnă datele privind cele cinci amprente digitale ale indexului, degetului mijlociu, degetului inelar, degetului mic și degetului mare de la mâna dreaptă și, dacă există, de la mâna stângă;”.

3. La articolul 5 se introduce următorul alineat:

„(1a) CIR conține datele menționate la articolul 9 alineatul (4) literele (a)-(c) și la articolul 9 alineatele (5) și (6). Celelalte date din VIS se stochează în sistemul central al VIS.”

4. La articolul 6, alineatul (2) se înlocuiește cu următorul text:

„(2) Accesul la VIS în vederea consultării datelor este rezervat exclusiv personalului autorizat în mod corespunzător din cadrul autorităților naționale ale fiecărui stat membru cu competențe în ceea ce privește scopurile prevăzute la articolele 15-22, și personalului autorizat în mod corespunzător din cadrul autorităților naționale ale fiecărui stat membru și al agențiilor Uniunii cu competențe în ceea ce privește scopurile prevăzute la articolele 20 și 21 din Regulamentul (UE) 2019/817. Acest acces este limitat la ceea ce este necesar pentru îndeplinirea sarcinilor care le revin, în scopurile menționate și este proporțional cu obiectivele urmărite.”

5. La articolul 9 alineatul (4), literele (a)-(c) se înlocuiesc cu următorul text:

„(a) numele (de familie); prenumele (numele de botez); data nașterii, sexul;

(aa) numele (de familie) la naștere [numele anterior (anterioare)] locul și țara nașterii; cetățenia actuală și cetățenia la naștere;

(b) tipul și numărul documentului sau documentelor de călătorie și codul din trei litere al țării emitente a documentului sau documentelor de călătorie;

(c) data expirării perioadei de valabilitate a documentului de călătorie;

(ca) autoritatea care a eliberat documentul de călătorie și data eliberării;".

Articolul 59

Modificarea Regulamentului (UE) 2016/399

La articolul 8 se introduce următorul alineat:

„(4a) În cazul în care, la intrare sau la ieșire, în urma consultării bazelor de date relevante, inclusiv a detectorului de identități multiple prin intermediul portalului european de căutare instituite prin articolul 25 alineatul (1) și, respectiv, articolul 6 alineatul (1) din Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului (*), rezultă o conexiune galbenă sau se detectează o conexiune roșie, polițistul de frontieră consultă registrul comun de date de identitate instituit prin articolul 17 alineatul (1) din regulamentul menționat sau SIS ori ambele pentru a evalua diferențele dintre datele de identitate conexate sau datele din documentele de călătorie conexate. Polițistul de frontieră efectuează verificările suplimentare necesare pentru a lua o decizie privind statutul și culoarea conexiunii.

În conformitate cu articolul 69 alineatul (1) din Regulamentul (UE) 2019/817, prezentul alineat se aplică numai de la punerea în funcțiune a detectorului de identități multiple în temeiul articolului 72 alineatul (4) din regulamentul menționat.

(*) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații 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)."

Articolul 60

Modificarea Regulamentului (UE) 2017/2226

Regulamentul (UE) 2017/2226 se modifică după cum urmează:

1. La articolul 1 se adaugă următorul alineat:

„(3) Prin faptul că stochează date de identitate, date privind documentele de călătorie și date biometrice în registrul comun de date de identitate (CIR) instituit prin articolul 17 alineatul (1) din Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului (*), EES contribuie la facilitarea și acordarea de asistență în vederea identificării corecte a persoanelor înregistrate în EES în condițiile și în scopurile de la articolul 20 din regulamentul menționat.

(*) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații 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)."

2. La articolul 3, alineatul (1) se modifică după cum urmează:

(a) punctul 22 se înlocuiește cu următorul text:

„22. «date din EES» înseamnă toate datele stocate în sistemul central al EES și în CIR, în conformitate cu articolele 15-20;";

(b) se introduce următorul punct:

„22a. «date de identitate» înseamnă datele menționate la articolul 16 alineatul (1) litera (a), precum și datele relevante menționate la articolul 17 alineatul (1) și la articolul 18 alineatul (1);";

(c) se adaugă următoarele puncte:

„32. «ESP» înseamnă portalul european de căutare instituit prin articolul 6 alineatul (1) din Regulamentul (UE) 2019/817;

33. «CIR» înseamnă registrul comun de date de identitate instituit prin articolul 17 alineatul (1) din Regulamentul (UE) 2019/817."

3. La articolul 6 alineatul (1) se adaugă următoarea literă:

„(j) a asigura identificarea corectă a persoanelor.”

4. Articolul 7 se modifică după cum urmează:

(a) alineatul (1) se modifică după cum urmează:

(i) se introduce următoarea literă:

„(as) infrastructura centrală a CIR, astfel cum este menționată la articolul 17 alineatul (2) litera (a) din Regulamentul (UE) 2019/817;”;

(ii) litera (f) se înlocuiește cu următorul text:

„(f) o infrastructură de comunicații securizată între sistemul central al EES și infrastructurile centrale ale ESP și ale CIR.”;

(b) se introduce următorul alineat:

„(1a) CIR conține datele menționate la articolul 16 alineatul (1) literele (a)-(d), la articolul 17 alineatul (1) literele (a), (b) și (c) și la articolul 18 alineatele (1) și (2). Celelalte date din EES sunt stocate în sistemul central al EES.”

5. La articolul 9 se adaugă următorul alineat:

„(4) Accesul la datele din EES stocate în CIR este rezervat exclusiv personalului autorizat în mod corespunzător din cadrul autorităților competente ale fiecărui stat membru și personalului autorizat în mod corespunzător din cadrul agențiilor Uniunii cu competențe în ceea ce privește scopurile prevăzute la articolele 20 și 21 din Regulamentul (UE) 2019/817. Acest acces este limitat la ceea ce este necesar pentru îndeplinirea sarcinilor care le revin, în scopurile menționate și este proporțional cu obiectivele urmărite.”

6. Articolul 21 se modifică după cum urmează:

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

„(1) În cazul în care este imposibil din punct de vedere tehnic să se introducă date în sistemul central al EES sau în CIR sau în cazul unei defecțiuni a sistemului central al EES sau a CIR, datele menționate la articolele 16-20 sunt stocate temporar în NUI. În cazul în care acest lucru nu este posibil, datele sunt stocate local, cu titlu temporar, în format electronic. În ambele cazuri, datele sunt introduse în sistemul central al EES sau în CIR de îndată ce imposibilitatea tehnică încetează sau defecțiunea este remediată. Statele membre iau măsurile adecvate și pun la dispoziție infrastructura, echipamentele și resursele necesare pentru a se asigura că o astfel de stocare locală temporară poate fi efectuată în orice moment și în oricare dintre punctele de trecere a frontierei.”;

(b) la alineatul (2), primul paragraf se înlocuiește cu următorul text:

„(2) Fără a aduce atingere obligației de a efectua verificări la frontiere în temeiul Regulamentului (UE) 2016/399, în situația excepțională în care este imposibil din punct de vedere tehnic să se introducă date fie în sistemul central al EES și în CIR, fie în NUI, iar stocarea locală temporară în format electronic a datelor este imposibilă din punct de vedere tehnic, autoritatea de frontieră stochează manual datele menționate la articolele 16-20 din prezentul regulament, cu excepția datelor biometrice, și aplică o ștampilă de intrare sau de ieșire în documentul de călătorie al resortisantului țării terțe. Datele respective sunt introduse în sistemul central al EES și în CIR de îndată ce acest lucru este posibil din punct de vedere tehnic.”;

7. Articolul 23 se modifică după cum urmează:

(a) se introduce următorul alineat:

„(2a) În scopul efectuării verificărilor în conformitate cu alineatul (1) din prezentul articol, autoritatea de frontieră lansează o interogare utilizând ESP pentru a compara datele privind resortisantul țării terțe cu datele relevante din EES și din VIS.”;

(b) la alineatul (4), primul paragraf se înlocuiește cu următorul text:

„(4) În cazul în care, în urma căutării cu ajutorul datelor alfanumerice prevăzute la alineatul (2) din prezentul articol, reiese că datele referitoare la resortisantul unei țări terțe nu sunt înregistrate în EES, iar o verificare a resortisantului țării terțe în temeiul alineatului (2) din prezentul articol nu dă rezultate sau când există îndoieli cu privire la identitatea resortisantului țării terțe, autoritățile de frontieră au acces la date în scopul identificării, în conformitate cu articolul 27, pentru a crea sau a actualiza un dosar individual în conformitate cu articolul 14.”

8. La articolul 32 se introduce următorul alineat:

„(1a) În cazurile în care autoritățile desemnate au lansat o interogare în CIR în conformitate cu articolul 22 din Regulamentul (UE) 2019/817, acestea pot accesa EES pentru consultare dacă sunt îndeplinite condițiile prevăzute la prezentul articol și dacă din răspunsul primit, astfel cum se menționează la articolul 22 alineatul (2) din Regulamentul (UE) 2019/817, rezultă că datele sunt stocate în EES."

9. La articolul 33 se introduce următorul alineat:

„(1a) În cazurile în care Europol a lansat o interogare în CIR în conformitate cu articolul 22 din Regulamentul (UE) 2019/817, acesta poate accesa EES pentru consultare dacă sunt îndeplinite condițiile prevăzute la prezentul articol și dacă din răspunsul primit, astfel cum se menționează la articolul 22 alineatul (2) din Regulamentul (UE) 2019/817, rezultă că datele sunt stocate în EES."

10. Articolul 34 se modifică după cum urmează:

(a) la alineatele (1) și (2), cuvintele „în sistemul central al EES" se înlocuiesc cu cuvintele „în CIR și în sistemul central al EES";

(b) la alineatul (5), cuvintele „din sistemul central al EES" se înlocuiesc cu cuvintele „din sistemul central al EES și din CIR".

11. La articolul 35, alineatul (7) se înlocuiește cu următorul text:

„(7) Sistemul central al EES și CIR informează de îndată toate statele membre cu privire la ștergerea datelor din EES sau CIR și, după caz, le elimină din lista persoanelor identificate menționată la articolul 12 alineatul (3)."

12. La articolul 36, cuvintele „a sistemului central al EES" se înlocuiesc cu cuvintele „a sistemului central al EES și a CIR";.

13. Articolul 37 se modifică după cum urmează:

(a) primul paragraf al alineatului (1) se înlocuiește cu următorul text:

„(1) eu-LISA este responsabilă pentru dezvoltarea sistemului central al EES și a CIR, a NUI, a infrastructurii de comunicații și a canalului securizat de comunicații dintre sistemul central al EES și sistemul central al VIS. eu-LISA este, de asemenea, responsabilă pentru dezvoltarea serviciului web menționat la articolul 13 în conformitate cu normele detaliate menționate la articolul 13 alineatul (7) și cu specificațiile și condițiile adoptate în temeiul articolului 36 primul paragraf litera (h) și pentru dezvoltarea registrului de date menționat la articolul 63 alineatul (2).";

(b) primul paragraf al alineatului (3) se înlocuiește cu următorul text:

„(3) eu-LISA este responsabilă de gestionarea operațională a sistemului central al EES și a CIR, a NUI, precum și a canalului securizat de comunicații dintre sistemul central al EES și sistemul central al VIS. Aceasta se asigură, în cooperare cu statele membre, că se utilizează în permanență cele mai bune tehnologii disponibile, sub rezerva unei analize costuri-beneficii, pentru sistemul central al EES și CIR, NUI, infrastructura de comunicații, canalul securizat de comunicații dintre sistemul central al EES și sistemul central al VIS, serviciul web menționat la articolul 13 și registrul de date menționat la articolul 63 alineatul (2). eu-LISA este, de asemenea, responsabilă de gestionarea operațională a infrastructurii de comunicații dintre sistemul central al EES și NUI, de serviciul web menționat la articolul 13 și de registrul de date menționat la articolul 63 alineatul (2)."

14. La articolul 46 alineatul (1), se adaugă următoarea literă:

„(f) o mențiune privind utilizarea ESP pentru a efectua interogări în EES, astfel cum se menționează la articolul 7 alineatul (2) din Regulamentul (UE) 2019/817."

15. Articolul 63 se modifică după cum urmează:

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

„(2) În sensul prezentului articol alineatul (1), eu-LISA stochează datele menționate la alineatul respectiv în registrul central de raportare și statistici menționat la articolul 39 din Regulamentul (UE) 2019/817.";

(b) la alineatul (4) se adaugă următorul paragraf:

„Statisticile zilnice sunt stocate în registrul central de raportare și statistici."

Articolul 61

Modificarea Regulamentului (UE) 2018/1240

Regulamentul (UE) 2018/1240 se modifică după cum urmează:

1. La articolul 1 se adaugă următorul alineat:

„(3) Prin faptul că stochează date de identitate și date privind documentele de călătorie în registrul comun de date de identitate (CIR) instituit prin articolul 17 alineatul (1) din Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului (*), ETIAS contribuie la facilitarea și acordarea de asistență în vederea identificării corecte a persoanelor înregistrate în ETIAS în condițiile și în scopurile de la articolul 20 din regulamentul menționat.

(*) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații 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).”

2. La articolul 3 alineatul (1) se adaugă următoarele litere:

„23. «CIR» înseamnă registrul comun de date de identitate instituit prin articolul 17 alineatul (1) din Regulamentul (UE) 2019/817;

24. «ESP» înseamnă portalul european de căutare instituit prin articolul 6 alineatul (1) din Regulamentul (UE) 2019/817;

25. «sistemul central al ETIAS» înseamnă sistemul central menționat la articolul 6 alineatul (2) litera (a) împreună cu CIR, în măsura în care CIR conține datele menționate la articolul 6 alineatul (2a);

26. «date de identitate» înseamnă datele prevăzute la articolul 17 alineatul 2) literele (a), (b) și (c);

27. «document de călătorie» înseamnă datele menționate la articolul 17 alineatul (2) literele (d) și (e) și codul din trei litere al țării care a eliberat documentul de călătorie, astfel cum se menționează la articolul 19 alineatul (3) litera (c).”

3. La articolul 4 se adaugă următoarea literă:

„(g) asigură identificarea corectă a persoanelor.”

4. Articolul 6 se modifică după cum urmează:

(a) alineatul (2) se modifică după cum urmează:

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

„(a) un sistem central, care include lista de supraveghere din ETIAS menționată la articolul 34;”;

(ii) se introduce următoarea literă:

„(aa) CIR;”;

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

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

(b) se introduce următorul alineat:

„(2a) CIR conține datele de identitate și datele privind documentele de călătorie. Celelalte date sunt stocate în sistemul central.”

5. Articolul 13 se modifică după cum urmează:

(a) se introduce următorul alineat:

„(4a) Accesul la datele de identitate din ETIAS și la datele privind documentele de călătorie stocate în CIR este rezervat, de asemenea, exclusiv membrilor personalului autorizat în mod corespunzător din cadrul autorităților naționale din fiecare stat membru și membrilor personalului autorizat în mod corespunzător din cadrul agențiilor Uniunii cu competențe în ceea ce privește scopurile prevăzute la articolele 20 și 21 din Regulamentul (UE) 2019/817. Acest acces este limitat la ceea ce este necesar pentru îndeplinirea sarcinilor care le revin, în scopurile menționate și este proporțional cu obiectivele urmărite.”;

(b) alineatul (5) se înlocuiește cu următorul text:

„(5) Fiecare stat membru desemnează autoritățile naționale competente menționate la alineatele (1), (2), (4) și (4a) din prezentul articol și comunică fără întârziere o listă a acestor autorități eu-LISA, în conformitate cu articolul 87 alineatul (2). În lista respectivă se specifică scopul în care personalul autorizat în mod corespunzător din cadrul fiecărei autorități are acces la datele din sistemul de informații al ETIAS în conformitate cu alineatele (1), (2), (4) și (4a) din prezentul articol."

6. La articolul 17, alineatul (2) se modifică după cum urmează:

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

„(a) numele (de familie), prenumele, numele (de familie) la naștere; data nașterii, locul nașterii, sexul, cetățenia actuală;";

(b) se introduce următoarea literă:

„(aa) țara de naștere, prenumele părinților solicitantului;".

7. La articolul 19 alineatul (4), cuvintele „articolul 17 alineatul (2) litera (a)" se înlocuiesc cu „articolul 17 alineatul (2) literele (a) și (aa)".

8. Articolul 20 se modifică după cum urmează:

(a) la alineatul (2), primul paragraf se înlocuiește cu următorul text:

„(2) Sistemul central al ETIAS lansează o interogare utilizând ESP pentru a compara datele relevante menționate la articolul 17 alineatul (2) literele (a), (aa), (b), (c), (d), (f), (g), (j), (k) și (m) și la articolul 17 alineatul (8) cu datele prezente într-o fișă, într-un dosar sau într-o semnalare înregistrată într-un dosar de cerere stocat în sistemul central al ETIAS, în SIS, în EES, în VIS, în Eurodac, în datele Europol și în bazele de date SLTD și TDAWN ale Interpol.";

(b) la alineatul (4), cuvintele „articolul 17 alineatul (2) literele (a), (b), (c), (d), (f), (g), (j), (k) și (m)" se înlocuiesc cu „articolul 17 alineatul (2) literele (a), (aa), (b), (c), (d), (f), (g), (j), (k) și (m)";

(c) la alineatul (5), cuvintele „articolul 17 alineatul (2) literele (a), (c), (f), (h), și (i)" se înlocuiesc cu „articolul 17 alineatul (2) literele (a), (aa), (c), (f), (h) și (i)".

9. La articolul 23, alineatul (1) se înlocuiește cu următorul text:

„(1) Sistemul central al ETIAS lansează o interogare utilizând ESP pentru a compara datele relevante menționate la articolul 17 alineatul (2) literele (a), (aa), (b) și (d) cu datele existente în SIS pentru a stabili dacă solicitantul face obiectul uneia dintre următoarele semnalări:

(a) o semnalare privind persoane dispărute;

(b) o semnalare privind persoane căutate în vederea participării la o procedură judiciară;

(c) o semnalare privind persoane supuse unor controale discrete sau al unor controale specifice."

10. La articolul 52 se introduce următorul alineat:

„(1a) În cazurile în care autoritățile desemnate au lansat o interogare în CIR în conformitate cu articolul 22 din Regulamentul (UE) 2019/817, acestea pot accesa dosarele de cerere stocate în sistemul central al ETIAS în conformitate cu prezentul articol pentru consultare în cazul în care, din răspunsul primit, astfel cum se menționează la articolul 22 alineatul (2) din Regulamentul (UE) 2019/817, rezultă că datele sunt stocate în dosarele de cerere stocate în sistemul central al ETIAS."

11. La articolul 53 se introduce următorul alineat:

„(1a) În cazurile în care Europol a lansat o interogare în CIR în conformitate cu articolul 22 din Regulamentul (UE) 2019/817, acesta poate accesa dosarele de cerere stocate în sistemul central al ETIAS în conformitate cu prezentul articol pentru consultare în cazul în care, din răspunsul primit, astfel cum se menționează la articolul 22 alineatul (2) din Regulamentul (UE) 2019/817, rezultă că datele sunt stocate în dosarele de cerere stocate în sistemul central al ETIAS."

12. La articolul 65 alineatul (3) al cincilea paragraf, cuvintele „articolul 17 alineatul (2) literele (a), (b), (d), (e) și (f)" se înlocuiesc cu „articolul 17 alineatul (2) literele (a), (aa), (b), (d), (e) și (f)".

13. La articolul 69 alineatul (1) se introduce următoarea literă:

„(ca) după caz, o mențiune privind utilizarea ESP pentru a efectua interogări în sistemul central al ETIAS, astfel cum se menționează la articolul 7 alineatul (2) din Regulamentul (UE) 2019/817;".

14. La articolul 73 alineatul (2), cuvintele „registrul central de date" se înlocuiesc cu „registrul central de raportare și statistici menționat la articolul 39 din Regulamentul (UE) 2019/817, în măsura în care acesta conține date obținute din sistemul central al ETIAS în temeiul articolului 84 din prezentul regulament."

15. La articolul 74 alineatul (1), primul paragraf se înlocuiește cu următorul text:

„(1) După punerea în funcțiune a ETIAS, eu-LISA este responsabilă cu gestionarea tehnică a sistemului central al ETIAS și a NUI. Aceasta este, de asemenea, responsabilă cu orice testare tehnică necesară pentru instituirea și actualizarea regulilor de verificare ale ETIAS. În cooperare cu statele membre, aceasta se asigură că se utilizează în permanență cea mai bună tehnologie existentă, sub rezerva unei analize cost-beneficiu. eu-LISA este, de asemenea, responsabilă cu gestionarea tehnică a infrastructurii de comunicații dintre sistemul central al ETIAS și NUI, precum și cu site-ul web public, aplicația pentru dispozitive mobile, serviciul de e-mail, serviciul de cont securizat, instrumentul de verificare pentru solicitanți, instrumentul pentru acordarea sau retragerea consimțământului pus la dispoziția solicitanților, instrumentul de evaluare pentru lista de supraveghere din ETIAS, portalul pentru operatorii de transport, serviciul web și software-ul pentru prelucrarea cererilor."

16. La articolul 84 alineatul (2), primul paragraf se înlocuiește cu următorul text:

„(2) În sensul alineatului (1) din prezentul articol, eu-LISA stochează datele menționate la alineatul respectiv în registrul central de raportare și statistici menționat la articolul 39 din Regulamentul (UE) 2019/817. În conformitate cu articolul 39 alineatul (1) din regulamentul respectiv, datele statistice utilizabile între sisteme și rapoartele analitice permit autorităților enumerate la alineatul (1) din prezentul articol să obțină rapoarte și statistici adaptabile pentru a sprijini aplicarea regulilor de verificare ale ETIAS menționate la articolul 33, a îmbunătăți evaluarea riscurilor în materie de securitate și de imigrație ilegală, precum și a riscurilor epidemice ridicate, a spori eficacitatea verificărilor la frontiere și a ajuta unitatea centrală a ETIAS și unitățile naționale ale ETIAS să prelucreze cererile de autorizații de călătorie."

17. La articolul 84 alineatul (4) se adaugă următorul paragraf:

„Statisticile zilnice sunt stocate în registrul central de raportare și statistici menționat la articolul 39 din Regulamentul (UE) 2019/817."

Articolul 62

Modificarea Regulamentului (UE) 2018/1726

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

1. Articolul 12 se înlocuiește cu următorul text:

„*Articolul 12*

Calitatea datelor

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

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

(*) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații 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 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. 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 funcționarea 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 aplicației de referință a ECRIS în temeiul articolului 36 alineatul (8) din Regulamentul (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, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Convenției 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, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești 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 dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor (ECRIS-TCN), destinat să completeze sistemul european de informații 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 observații formale referitoare la rapoartele Autorității Europene pentru Protecția 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 autorităților 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 naționale 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 autorităților competente în temeiul articolului 65 alineatul (2) din Regulamentul (UE) 2017/2226, lista autorităților competente în temeiul articolului 87 alineatul (2) din Regulamentul (UE) 2018/1240, lista autorităților 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 a 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:

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

„(da) Grupul consultativ privind interoperabilitatea;";

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

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

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

Agenția Europeană pentru Poliția 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 Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă pot numi fiecare câte un reprezentant în cadrul grupului consultativ privind interoperabilitatea."

Articolul 63

Modificarea Regulamentului (UE) 2018/1861

Regulamentul (UE) 2018/1861 se modifică după cum urmează:

1. La articolul 3 se adaugă următoarele puncte:

„22. «ESP» înseamnă portalul european de căutare instituit prin articolul 6 alineatul (1) din Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului (*);

23. «BMS comun» înseamnă serviciul comun de comparare a datelor biometrice instituit prin articolul 12 alineatul (1) din Regulamentul (UE) 2019/817;

24. «CIR» înseamnă registrul comun de date de identitate instituit prin articolul 17 alineatul (1) din Regulamentul (UE) 2019/817;

25. «MID» înseamnă detectorul de identități multiple instituit prin articolul 25 alineatul (1) din Regulamentul (UE) 2019/817.

(*) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații 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)."

2. Articolul 4 se modifică după cum urmează:

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

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

(c) o infrastructură de comunicații între CS-SIS, CS-SIS de rezervă și NI-SIS (denumită în continuare «infrastructura de comunicații») care furnizează o rețea virtuală criptată dedicată datelor din SIS și schimbului de date între birourile SIRENE, astfel cum sunt menționate la articolul 7 alineatul (2); și

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

(b) se adaugă următoarele alineate:

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

(9) Fără a se aduce atingere alineatelor (1)-(5) datele SIS pot fi transmise și prin intermediul infrastructurii de comunicare securizate menționate la alineatul (1) litera (d). Aceste transmisii se efectuează numai în măsura în care datele sunt necesare în scopul Regulamentului (UE) 2019/817."

3. La articolul 7 se introduce următorul alineat:

„(2a) Birourile SIRENE asigură, de asemenea, verificarea manuală a identităților diferite în conformitate cu articolul 29 din Regulamentul (UE) 2019/817. 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) 2019/817."

4. La articolul 12, alineatul (1) se înlocuiește cu următorul text:

„(1) Statele membre se asigură că fiecare accesare a datelor cu caracter personal și toate schimburile de date cu caracter personal din CS-SIS sunt înregistrate în sistemul lor N.SIS în scopul verificării legalității căutării, al monitorizării legalității prelucrării datelor, al automonitorizării, al asigurării funcționării corespunzătoare a N.SIS, precum și a integrității și securității datelor. Această cerință nu se aplică proceselor automate menționate la articolul 4 alineatul (6) literele (a), (b) și (c);

Statele membre se asigură că fiecare accesare a datelor cu caracter personal prin intermediul ESP este, de asemenea, înregistrată în scopul verificării legalității căutării, al monitorizării legalității prelucrării datelor, al automonitorizării și al asigurării integrității și securității datelor."

5. La articolul 34 alineatul (1) se adaugă următoarea literă:

„(g) verificarea identităților diferite și combaterea fraudei de identitate în conformitate cu capitolul V din Regulamentul (UE) 2019/817."

6. La articolul 60, alineatul (6) se înlocuiește cu următorul text:

„(6) În sensul articolului 15 alineatul (4) și al alineatelor (3), (4) și (5) din prezentul articol, eu-LISA stochează datele menționate 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 menționat la articolul 39 din Regulamentul (UE) 2019/817.

eu-LISA permite Comisiei și organismelor menționate la alineatul (5) din prezentul articol să obțină rapoarte și statistici personalizate. La cerere, eu-LISA acordă acces statelor membre, Comisiei, Europol și Agenției Europene pentru Poliția de Frontieră și Garda de Coastă la registrul central de raportare și statistici în conformitate cu articolul 39 din Regulamentul (UE) 2019/817."

Articolul 64

Modificarea Deciziei 2004/512/CE

La articolul 1 din Decizia 2004/512/CE, alineatul (2) se înlocuiește cu următorul text:

„(2) Sistemul de Informații privind Vizele se bazează pe o arhitectură centralizată și cuprinde:

(a) infrastructura centrală a registrului comun de date de identitate, astfel cum este menționată la articolul 17 alineatul (2) litera (a) din Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului (*);

(b) un sistem central de informații, denumit în continuare «Sistemul Central de Informații privind Vizele» (CS-VIS);

(c) o interfață în fiecare stat membru, denumită în continuare «interfața națională» (NI-VIS), care asigură conectarea la autoritatea centrală națională relevantă din statul membru respectiv;

(d) o infrastructură de comunicații între Sistemul Central de Informații privind Vizele și interfețele naționale;

(e) un canal de comunicații securizat între sistemul central al EES și CS-VIS;

(f) o infrastructură de comunicații securizată între sistemul central al EES și infrastructurile centrale ale portalului european de căutare instituit prin articolul 6 alineatul (1) din Regulamentul (UE) 2019/817 și serviciul comun de comparare a datelor biometrice instituit prin articolul 17 alineatul (1) din Regulamentul (UE) 2019/817.

(*) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații 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)."

Articolul 65

Modificarea Deciziei 2008/633/JAI

Decizia 2008/633/JAI se modifică după cum urmează:

1. La articolul 5 se adaugă următorul alineat:

„(1a) În cazurile în care autoritățile desemnate au lansat o interogare în registrul comun de date de identitate (CIR) în conformitate cu articolul 22 din Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului (*) și dacă sunt îndeplinite condițiile privind accesul prevăzute de prezentul articol, acestea pot accesa VIS pentru consultare în cazul în care din răspunsul primit, astfel cum se menționează la articolul 22 alineatul (2) din regulamentul menționat, rezultă că datele sunt stocate în VIS.

(*) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații 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)."

2. La articolul 7 se adaugă următorul alineat:

„(1a) În cazurile în care Europol a lansat o interogare în CIR în conformitate cu articolul 22 din Regulamentul (UE) 2019/817 și dacă sunt îndeplinite condițiile privind accesul prevăzute de prezentul articol, Europol poate accesa VIS pentru consultare în cazul în care din răspunsul primit, astfel cum se menționează la articolul 22 alineatul (2) din regulamentul menționat, rezultă că datele sunt stocate în VIS."

CAPITOLUL X

Dispoziții finale

Articolul 66

Întocmirea de rapoarte și de statistici

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

(a) numărul de interogări per profil de utilizator ESP;

(b) numărul de interogări pentru fiecare bază de date a Interpol.

Datele trebuie să nu permită identificarea persoanelor fizice.

(2) Personalul autorizat în mod corespunzător din cadrul autorităților 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) 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 autorităților 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 funcție de tip, și sistemele de informații ale UE care conțin 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 Agenției Europene pentru Poliția de Frontieră și Garda de Coastă are acces pentru a consulta datele menționate la alineatele (1), (2) și (3) din prezentul articol în scopul de a efectua analize de risc și evaluări ale vulnerabilității, astfel cum se menționează la articolele 11 și 13 din Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului ([40]).

(5) Personalul autorizat în mod corespunzător al Europol are acces pentru a consulta datele menționate la alineatele (2) și (3) din prezentul articol în scopul de a efectua analize strategice, tematice și operaționale, astfel cum se menționează 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 menționate la alineatele respective în CRRS. Datele incluse în CRRS trebuie să nu permită identificarea persoanelor fizice, dar permit autorităților enumerate la alineatele (1), (2) și (3) să obțină rapoarte și statistici adaptabile pentru a spori eficiența verificărilor la frontieră, a sprijini autoritățile să prelucreze cererile de viză și a sprijini elaborarea de politici bazate pe date concrete în materie de migrație și de securitate în Uniune.

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

Articolul 67

Perioada de tranziție pentru utilizarea portalului european de căutare

(1) Pentru o perioadă de doi ani de la data punerii în funcțiune a ESP, obligațiile menționate la articolul 7 alineatele (2) și (4) nu se aplică, iar utilizarea ESP este opțională.

(2) Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 73 pentru a modifica prezentul regulament prin prelungirea, o singură dată, a perioadei menționate 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 funcțiune a ESP asupra organizării și duratei verificărilor la frontiere.

Articolul 68

Perioada de tranziție aplicabilă dispozițiilor privind accesul la registrul comun de date de identitate în scopul prevenirii, depistării sau anchetării infracțiunilor de terorism sau a altor infracțiuni grave

Articolul 22, articolul 60 punctele 8 și 9, articolul 61 punctele 10 și 11 și articolul 65 se aplică de la data punerii în funcțiune a CIR menționată la articolul 72 alineatul (3).

([40]) 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).

Articolul 69

Perioada de tranziție aplicabilă detectorului de identități multiple

(1) Pentru o perioadă de un an de la notificarea de către eu-LISA a încheierii perioadei de testare a MID menționate la articolul 72 alineatul (4) litera (b) și înainte de punerea în funcțiune a MID, unitatea centrală a ETIAS este responsabilă de efectuarea unei detectări de identități multiple utilizând datele stocate în EES, VIS, Eurodac și SIS. Detectarea identităților multiple se efectuează folosind exclusiv date biometrice.

(2) În cazul în care, în urma interogărilor, se obțin una sau mai multe concordanțe 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 obțin una sau mai multe concordanțe 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 obțin mai multe concordanțe, se stabilește o conexiune între fiecare componentă a datelor care a generat corespondența.

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

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

(6) Unitatea centrală a ETIAS informează Comisia în conformitate cu articolul 71 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 73 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 70

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.

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

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

Articolul 71

Notificări

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

O listă consolidată a acestor autorități se publică în *Jurnalul Oficial al Uniunii Europene* în termen de trei luni de la data punerii în funcțiune a fiecărei componente de interoperabilitate în conformitate cu articolul 72. 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 menționate la articolul 72 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 tranziție prevăzute la articolul 69.

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

Articolul 72

Punerea în funcțiune

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

(a) au fost adoptate măsurile menționate 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 autoritățile statelor membre și cu agențiile Uniunii care pot folosi ESP;

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

ESP efectuează interogări în bazele de date ale Interpol numai odată ce condițiile 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 funcțiune a ESP.

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.

(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 78 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;

(d) unitatea centrală a ETIAS a trimis Comisiei notificarea în conformitate cu articolul 71 alineatul (3);

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

(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 calității datelor, indicatorii comuni de calitate a datelor și standardele minime de calitate a datelor, odată ce sunt îndeplinite următoarele condiții:

(a) au fost adoptate măsurile menționate 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 calității datelor, a indicatorilor comuni de calitate a datelor și a standardelor minime de calitate a datelor, pe care a efectuat-o în cooperare cu autoritățile statelor membre.

Comisia stabilește data menționată 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 funcționeze CRRS, odată ce sunt îndeplinite următoarele condiții:

(a) au fost adoptate măsurile menționate 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 autoritățile statelor membre;

(c) eu-LISA a validat modalitățile tehnice și juridice de colectare și transmitere a datelor menționate la articolul 39 și a notificat aceste modalități Comisiei.

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.

(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 73

Exercitarea delegării de competențe

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

(2) Competența de a adopta acte delegate menționată la articolul 28 alineatul (5), articolul 39 alineatul (5), articolul 49 alineatul (6), articolul 67 alineatul (2) și articolul 69 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 competențe cu cel puțin nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de timp identice, cu excepția cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puțin trei luni înainte de încheierea fiecărei perioade.

(3) Delegarea de competențe menționată la articolul 28 alineatul (5), articolul 39 alineatul (5), articolul 49 alineatul (6), articolul 67 alineatul (2) și articolul 69 alineatul (8) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe 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 menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional 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 67 alineatul (2) și al articolului 69 alineatul (8) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții 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 obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 74

Procedura comitetului

(1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul 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 75

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 76

Formare

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

Autoritățile statelor membre și agențiile Uniunii îi oferă personalului lor autorizat să prelucreze date utilizând componentele de interoperabilitate programe adecvate de formare legate de securitatea datelor, calitatea datelor, normele de protecție a datelor, procedurile aplicabile prelucrării datelor și obligațiile 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 autorităților statelor membre și cel al agențiilor Uniunii care sunt autorizate să prelucreze date utilizând componentele de interoperabilitate. Se acordă o atenție deosebită procesului de detectare a identităților multiple, inclusiv verificării manuale a identităților diferite și nevoii aferente de a oferi garanții adecvate de protecție a drepturilor fundamentale.

Articolul 77

Manual practic

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

Articolul 78

Monitorizare și evaluare

(1) eu-LISA se asigură că există proceduri pentru a monitoriza dezvoltarea componentelor de interoperabilitate și conectarea lor la interfața uniformă națională din perspectiva obiectivelor legate de planificare și costuri și pentru a monitoriza funcționarea 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 situația dezvoltării componentelor de interoperabilitate și legătura lor cu interfața uniformă națională. 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 funcțiune a fiecărei componente de interoperabilitate în conformitate cu articolul 72 și, ulterior, o dată la patru ani, eu-LISA prezintă Parlamentului European, Consiliului și Comisiei un raport privind funcționarea 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) o examinare a rezultatelor obținute 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 funcționării portalului web, inclusiv cifre privind utilizarea portalului web și numărul de cereri soluționate;

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

(e) o evaluare a securității componentelor de interoperabilitate;

(f) o evaluare a utilizării CIR pentru identificare;

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

(h) o evaluare a eventualelor implicații, inclusiv a impactului disproporționat asupra fluidității traficului la punctele de trecere a frontierelor și a implicațiilor cu un impact bugetar asupra bugetului general al Uniunii;

(i) o evaluare a căutării în bazele de date ale Interpolului prin intermediul ESP, inclusiv informații privind numărul de concordanțe în bazele de date ale Interpolului și informații 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, Autorității Europene pentru Protecția Datelor și Agenției 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 menționate la articolul 72, Comisia prezintă Parlamentului European și Consiliului un raport privind situația pregătirilor pentru a pune pe deplin în aplicare prezentul regulament. Raportul conține și informații detaliate cu privire la costurile aferente și la orice risc care poate afecta costurile totale.

(6) La doi ani de la punerea în funcțiune a MID în conformitate cu articolul 72 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 menționată la alineatul (4) litera (b) din prezentul articol.

(7) Statele membre și Europolul furnizează eu-LISA și Comisiei informațiile necesare pentru redactarea rapoartelor menționate la alineatele (3)-(6). Aceste informații nu afectează metodele de lucru și nici nu includ date care dezvăluie sursele, membrii personalului sau investigațiile autorităților desemnate.

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

(9) Respectând dispozițiile dreptului intern referitoare la publicarea informațiilor sensibile și fără a aduce atingere limitărilor necesare pentru protejarea securității și a ordinii publice, prevenirea infracțiunilor și a garanta că nicio anchetă națională 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 infracțiunilor de terorism sau a altor infracțiuni grave care conțin informații și statistici privind:

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

(b) motivele întemeiate invocate în sprijinul suspiciunii justificate că suspectul, autorul sau victima intră sub incidența Regulamentului (UE) 2017/2226, Regulamentului (CE) nr. 767/2008 sau a Regulamentului (UE) 2018/1240;

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

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

(e) necesitatea și utilizarea excepției justificate de urgență, precum și cazurile în care urgența 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 dispoziție o soluție tehnică pentru a gestiona cererile de acces ale utilizatorilor menționate la articolul 22 și a facilita colectarea informațiilor în temeiul alineatelor (7) și (9) din prezentul articol, în scopul generării rapoartelor și statisticilor menționate la alineatele respective. Comisia adoptă acte de punere în aplicare pentru a stabili specificațiile soluției tehnice. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 74 alineatul (2).

Articolul 79

Intrarea în vigoare și aplicabilitatea

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

Dispozițiile prezentului regulament referitoare la ESP se aplică de la data stabilită de Comisie în conformitate cu articolul 72 alineatul (1).

Dispozițiile prezentului regulament referitoare la BMS comun se aplică de la data stabilită de Comisie în conformitate cu articolul 72 alineatul (2).

Dispozițiile prezentului regulament referitoare la CIR se aplică de la data stabilită de Comisie în conformitate cu articolul 72 alineatul (3).

Dispozițiile prezentului regulament referitoare la MID se aplică de la data stabilită de Comisie în conformitate cu articolul 72 alineatul (4).

Dispozițiile prezentului regulament referitoare la mecanismele și procedurile automatizate de control al calității 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 72 alineatul (5).

Dispozițiile prezentului regulament referitoare la CRRS se aplică de la data stabilită de Comisie în conformitate cu articolul 72 alineatul (6).

Articolele 6, 12, 17, 25, 38, 42, 54, 56, 57, 70, 71, 73, 74, 75, 77 și articolul 78 alineatul (1) se aplică de la 11 iunie 2019.

Prezentul regulament se aplică în privința 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.

Adoptat la Bruxelles, 20 mai 2019.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*
A. TAJANI	G. CIAMBA

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

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16 alineatul (2), articolul 74, articolul 78 alineatul (2) litera (e), articolul 79 alineatul (2) litera (c), articolul 82 alineatul (1) litera (d), articolul 85 alineatul (1), articolul 87 alineatul (2) litera (a) și articolul 88 alineatul (2),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European ([1]),

după consultarea Comitetului Regiunilor,

hotărând în conformitate cu procedura legislativă ordinară ([2]),

întrucât:

(1) În comunicarea sa din 6 aprilie 2016 intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate", Comisia a subliniat faptul că arhitectura de gestionare a datelor din Uniune în materie de gestionare a frontierelor și de securitate trebuie îmbunătățită. În urma acestei comunicări a început un proces care vizează asigurarea interoperabilității dintre sistemele de informații ale UE în materie de securitate, frontiere și gestionarea migrației, în vederea abordării deficiențelor structurale legate de sistemele respective care împiedică autoritățile naționale să își desfășoare activitatea și în vederea accesului polițiștilor de frontieră, al autorităților vamale, al agenților de poliție și al autorităților judiciare la informațiile de care au nevoie.

(2) În Foaia de parcurs pentru a consolida schimbul de informații și gestionarea informațiilor, inclusiv soluțiile de interoperabilitate, în domeniul justiției și afacerilor interne din 6 iunie 2016, Consiliul a identificat diferite provocări juridice, tehnice și operaționale pe care le presupune asigurarea interoperabilității sistemelor de informații ale UE și a făcut apel la căutarea unor soluții.

(3) În Rezoluția sa din 6 iulie 2016 privind prioritățile strategice ale programului de lucru al Comisiei pentru 2017 ([3]), Parlamentul European a solicitat Comisiei să prezinte propuneri pentru îmbunătățirea și dezvoltarea sistemelor de informații existente, pentru abordarea lacunelor în materie de informații și pentru asigurarea tranziției către interoperabilitate, precum și propuneri privind obligativitatea schimbului de informații la nivelul UE, însoțite de garanțiile necesare în materie de protecție a datelor.

(4) În concluziile sale din 15 decembrie 2016, Consiliul European a îndemnat la continuarea asigurării interoperabilității sistemelor de informații și ale bazelor de date ale UE.

(5) În raportul său final din 11 mai 2017, Grupul de experți la nivel înalt pentru sistemele de informații și interoperabilitate a concluzionat că este necesar și posibil din punct de vedere tehnic să se găsească soluții practice pentru realizarea interoperabilității și că aceasta ar putea, în principiu, să ofere câștiguri operaționale, și, totodată, să fie instituite în conformitate cu cerințele în materie de protecție a datelor.

(6) În comunicarea sa din 16 mai 2017 intitulată Al șaptelea raport referitor la progresele înregistrate pentru realizarea unei uniuni a securității efective și reale, Comisia a prezentat, în conformitate cu comunicarea sa din 6 aprilie 2016 și cu constatările și recomandările Grupului de experți la nivel înalt pentru sistemele de informații și interoperabilitate, o nouă abordare privind gestionarea datelor în materie de frontiere, securitate și migrație, în care toate sistemele UE de informații privind securitatea, frontierele și gestionarea migrației urmau să fie interoperabile, într-o manieră care respectă în deplinătate drepturile fundamentale.

([1]) JO C 283, 10.8.2018, p. 48.
([2]) Poziția Parlamentului European din 16 aprilie 2019 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 14 mai 2019.
([3]) JO C 101, 16.3.2018, p. 116.

(7) În concluziile sale din 9 iunie 2017 privind calea de urmat pentru îmbunătățirea schimbului de informații și asigurarea interoperabilității sistemelor de informații ale UE, Consiliul a invitat Comisia să caute în continuare soluții pentru interoperabilitate, astfel cum a propus grupul de experți la nivel înalt.

(8) În concluziile sale din 23 iunie 2017, Consiliul European a subliniat necesitatea îmbunătățirii interoperabilității între bazele de date și a invitat Comisia să elaboreze un proiect legislativ pe baza propunerilor făcute de Grupul de experți la nivel înalt pentru sistemele de informații și interoperabilitate, cât mai curând posibil.

(9) Pentru îmbunătățirea eficacității și eficienței verificărilor la frontierele externe, pentru participarea la prevenirea și combaterea imigrației ilegale și la asigurarea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție al Uniunii, inclusiv menținerea securității și a ordinii publice și pentru garantarea securității pe teritoriul statelor membre, pentru a îmbunătăți punerea în aplicare a politicii comune a vizelor, pentru a facilita examinarea cererilor de protecție internațională, pentru a contribui la prevenirea, depistarea și investigarea infracțiunilor de terorism și a altor infracțiuni grave, pentru a facilita identificarea persoanelor cu identitate necunoscută care nu se pot legitima sau a rămășițelor umane neidentificate în cazul unui dezastru natural, al unui accident sau al unui atac terorist, cu scopul de a păstra încrederea publicului în sistemul Uniunii din domeniul migrației și al azilului, în măsurile Uniunii din domeniul securității și în capacitatea Uniunii de gestionare a frontierelor externe, ar trebui realizată interoperabilitatea dintre sistemele de informații ale Uniunii, și anume Sistemul de intrare/ieșire (EES), Sistemul de informații privind vizele (VIS), Sistemul european de informații și de autorizare privind călătoriile (ETIAS), Eurodac, Sistemul de informații Schengen (SIS) și Sistemul european de informații cu privire la cazierele judiciare pentru resortisanții țărilor terțe (ECRIS-TCN), astfel încât aceste sisteme de informații ale UE și datele pe care le conțin să se completeze reciproc, respectându-se totodată drepturile fundamentale ale persoanelor, în special dreptul la protecția datelor cu caracter personal. Pentru a realiza acest lucru, ar trebui instituite componentele de interoperabilitate: un portal european de căutare (ESP), un serviciu comun de comparare a datelor biometrice (BMS comun), un registru comun de date de identitate (CIR) și un detector de identități multiple (MID).

(10) Interoperabilitatea dintre sistemele de informații ale UE ar trebui să permită completarea reciprocă pentru a facilita identificarea corectă a persoanelor, inclusiv a persoanelor cu identitate necunoscută care nu se pot legitima sau a rămășițelor umane neidentificate, pentru a contribui la combaterea fraudelor de identitate, pentru a îmbunătăți și armoniza cerințele de calitate a datelor prevăzute în respectivele sisteme de informații ale UE, pentru a facilita implementarea tehnică și operațională a sistemelor de informații ale UE, pentru a consolida garanțiile în materie de securitate și protecție a datelor prevăzute de respectivele sisteme de informații ale UE, pentru a simplifica accesul în scopul prevenirii, depistării sau investigării infracțiunilor de terorism ori a altor infracțiuni grave la EES, VIS, ETIAS și Eurodac și pentru a îndeplini obiectivele EES, VIS, ETIAS, Eurodac, SIS și ale ECRIS-TCN.

(11) Componentele de interoperabilitate ar trebui să vizeze EES, VIS, ETIAS, Eurodac, SIS și ECRIS-TCN. Acestea ar trebui, de asemenea, să vizeze datele Europol, dar numai pentru a permite ca datele Europol să fie interogate în același timp prin intermediul respectivelor sisteme de informații ale UE.

(12) Componentele de interoperabilitate ar trebui să prelucreze datele personale ale persoanelor ale căror date cu caracter personal sunt prelucrate în sistemele de informații de bază ale UE și de către Europol.

(13) ESP ar trebui instituit pentru a facilita din punct de vedere tehnic accesul rapid, fără sincope, eficient, sistematic și controlat al autorităților statelor membre și al agențiilor Uniunii la sistemele de informații ale UE, datele Europol și bazele de date ale Organizației Internaționale de Poliție Criminală (Interpol), în măsura în care acest lucru este necesar pentru a-și îndeplini sarcinile în conformitate cu drepturile lor de acces. ESP ar trebui de asemenea instituit pentru a susține obiectivele EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN și ale datelor Europol. Permițând interogarea în paralel a tuturor sistemelor de informații ale UE relevante, a datelor Europol și a bazelor de date ale Interpol, ESP ar trebui să funcționeze ca un ghișeu unic sau ca un „broker de mesaje” prin care să se interogheze diverse sisteme centrale și să se extragă fără probleme informațiile necesare, cu respectarea deplină a cerințelor privind controlul accesului și protecția datelor care se aplică sistemelor de bază.

(14) Concepția ESP ar trebui să asigure faptul că, atunci când se lansează interogări în bazele de date ale Interpol, datele utilizate de către un utilizator ESP pentru a lansa o interogare nu sunt partajate cu proprietarii datelor Interpol. Modul în care este conceput ESP asigură, de asemenea, faptul că bazele de date ale Interpol sunt interogate doar în conformitate cu dreptul Uniunii și dreptul intern aplicabil.

(15) Utilizatorii ESP care au drept de acces la datele Europol în temeiul Regulamentului (UE) 2016/794 al Parlamentului European și al Consiliului ([4]) ar trebui să fie în măsură să efectueze simultan interogări în datele Europol și în sistemele de informații ale UE la care au acces. Orice prelucrare suplimentară a datelor în urma unei astfel de interogări ar trebui să aibă loc în conformitate cu Regulamentul (UE) 2016/794, inclusiv ținând cont de restricțiile privind accesul sau utilizarea impuse de furnizorul de date.

(16) ESP ar trebui astfel dezvoltat și configurat încât, pentru interogări, să nu permită utilizarea câmpurilor de date care nu sunt legate de persoane sau de documente de călătorie sau care nu sunt prezente într-un sistem de informații al UE, în datele Europol sau în baza de date a Interpol.

(17) Pentru a asigura utilizarea sistematică a sistemelor relevante de informații ale UE, ESP ar trebui utilizat pentru efectuarea de interogări în CIR, EES, VIS, ETIAS, Eurodac și în ECRIS-TCN. Cu toate acestea, o conexiune națională la diferitele sisteme de informații ale UE ar trebui menținută ca soluție tehnică alternativă. ESP ar trebui, de asemenea, să fie utilizat de către agențiile Uniunii pentru a efectua interogări în SIS central, cu respectarea drepturile lor de acces, pentru a-și îndeplini sarcinile. ESP ar trebui să fie un mijloc suplimentar de a efectua interogări în SIS central, în datele Europol și în bazele de date Interpol, care să completeze interfețele dedicate deja existente.

(18) Pentru identificarea unei persoane, datele biometrice, precum amprentele digitale și imaginile faciale, sunt unice și, prin urmare, mult mai fiabile decât datele alfanumerice. BMS comun ar trebui să fie un instrument tehnic care să consolideze și să faciliteze activitatea sistemelor de informații ale UE relevante și a celorlalte componente de interoperabilitate. Obiectivul esențial al BMS comun ar trebui să fie facilitarea identificării unei persoane care este înregistrată în mai multe baze de date, prin folosirea unei singure componente tehnologice pentru compararea datelor biometrice ale persoanei respective, în loc de mai multe componente. BMS comun ar trebui să contribuie la securitate și să aducă beneficii financiare, de întreținere și operaționale. Toate sistemele automate de identificare a amprentelor digitale, inclusiv cele utilizate în prezent pentru Eurodac, VIS și SIS, utilizează șabloane biometrice care conțin date ce provin dintr-o extragere de caracteristici a unor eșantioane biometrice efective. BMS comun ar trebui să regrupeze și să stocheze toate aceste șabloane biometrice, separate în mod logic, în funcție de sistemul de informații din care provin datele, în același loc, facilitând astfel comparațiile între sisteme prin utilizarea de șabloane biometrice și permițând obținerea unor economii de scară în dezvoltarea și întreținerea sistemelor centrale ale Uniunii.

(19) Șabloanele biometrice stocate în BMS comun, care ar trebui să conțină date ce provin dintr-o extragere de caracteristici a unor eșantioane biometrice efective, ar trebui să fie obținute în așa fel încât procesul de extragere să nu poată fi inversat. Șabloanele biometrice ar trebui obținute din datele biometrice, însă nu ar trebui să fie posibil să se obțină aceleași date biometrice plecând de la șabloanele biometrice. Întrucât datele privind amprentele palmare și profilurile ADN sunt stocate doar în SIS, și nu pot fi utilizate pentru a efectua verificări încrucișate cu datele existente în alte sisteme de informații, urmând principiile necesității și proporționalității, BMS comun nu ar trebui să stocheze profiluri ADN sau șabloane biometrice obținute din datele privind amprentele palmare.

(20) Datele biometrice reprezintă date cu caracter personal sensibile. Prezentul regulament ar trebui să stabilească baza și garanțiile privind prelucrarea unor astfel de date pentru identificarea univocă a persoanelor în cauză.

(21) EES, VIS, ETIAS, Eurodac și ECRIS-TCN necesită identificarea precisă a persoanelor ale căror date cu caracter personal sunt stocate în acestea. Prin urmare, CIR ar trebui să faciliteze identificarea corectă a persoanelor înregistrate în aceste sisteme.

(22) Datele cu caracter personal stocate în acele sisteme de informații ale UE pot face referire la aceleași persoane, dar cu identități diferite sau incomplete. Statele membre dispun de instrumente eficiente pentru identificarea cetățenilor sau a rezidenților permanenți înregistrați pe teritoriul lor. Interoperabilitatea dintre sistemele de informații ale UE ar trebui să contribuie la identificarea corectă a persoanelor prezente în sistemele respective. CIR ar trebui să stocheze datele cu caracter personal care sunt necesare pentru a permite o identificare mai precisă a persoanelor ale căror date sunt stocate în acele sisteme, inclusiv datele de identitate ale acestora, datele din documentul de călătorie al acestora și datele biometrice ale acestora, indiferent de sistemul în care au fost colectate inițial datele. În CIR ar trebui stocate doar datele cu caracter personal care sunt strict necesare pentru efectuarea unui control corect al identității. Datele cu caracter personal înregistrate în CIR nu ar trebui păstrate mai mult decât este strict necesar pentru îndeplinirea scopurilor pentru care au fost constituite sistemele de bază și ar trebui șterse în mod automat atunci când datele sunt șterse din sistemele de bază, respectându-se separarea lor logică.

([4]) Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 24.5.2016, p. 53).

(23) O nouă operațiune de prelucrare, care constă în stocarea acestor date în CIR și nu în fiecare dintre sistemele separate, este necesară pentru a face posibilă sporirea preciziei identificării, prin compararea automată a acestor date. Faptul că datele de identitate, datele din documentele de călătorie și datele biometrice sunt stocate în CIR nu ar trebui să împiedice în niciun fel prelucrarea datelor în EES, Eurodac, VIS, ETIAS, Eurodac sau ECRIS-TCN, întrucât CIR ar urma să fie o componentă comună nouă a acestor sisteme de bază.

(24) Prin urmare, este necesară crearea unui dosar individual în CIR pentru fiecare persoană înregistrată în EES, VIS, ETIAS, Eurodac sau ECRIS-TCN, pentru realizarea obiectivului de identificare corectă a persoanelor în spațiul Schengen și pentru sprijinirea MID atât pentru facilitarea controalelor de identitate pentru călătorii de bună credință, cât și pentru combaterea fraudelor de identitate. Dosarul individual ar trebui să stocheze toate informațiile privind identitatea legate de o persoană într-un singur loc și să le pună la dispoziția utilizatorilor finali autorizați în mod corespunzător.

(25) CIR ar trebui, așadar, să faciliteze și să eficientizeze accesul autorităților responsabile de prevenirea, depistarea sau investigarea infracțiunilor de terorism ori a altor infracțiuni grave la sistemele de informații ale UE care nu sunt instituite exclusiv în scopul prevenirii, detectării sau investigării infracțiunilor grave.

(26) CIR ar trebui să prevadă un sistem comun care să conțină datele de identitate, datele din documentele de călătorie și datele biometrice ale persoanelor care sunt înregistrate în EES, VIS, ETIAS, Eurodac și în ECRIS-TCN. Acesta ar trebui să facă parte din arhitectura tehnică a respectivelor sisteme și să servească drept componentă comună a acestora pentru stocarea și interogarea datelor de identitate, datelor din documentele de călătorie și a datelor biometrice pe care le prelucrează.

(27) Toate înregistrările din CIR ar trebui separate în mod logic prin atribuirea automată a unei etichete distinctive care să lege fiecare înregistrare de denumirea sistemului de bază care deține respectiva înregistrare. Sistemul de control al accesului la CIR ar trebui să utilizeze aceste etichete pentru a determina dacă permite accesul la înregistrarea respectivă.

(28) În cazul în care o autoritate de poliție a unui stat membru 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 sau în cazul în care există îndoieli cu privire la datele de identitate furnizate de persoana în cauză sau la autenticitatea documentului de călătorie ori la identitatea titularului său, sau în cazul în care persoana nu poate ori refuză să coopereze, respectiva autoritate de poliție ar trebui să poată lansa interogări în CIR pentru a identifica persoana. În aceste scopuri, autoritățile de poliție ar trebui să preleve amprente folosind tehnici de amprentare electronică prin scanare în timp real, cu condiția ca procedura să fi fost inițiată în prezența persoanei respective. Astfel de interogări în CIR nu ar trebui să fie permise pentru identificarea minorilor cu vârsta mai mică de 12 ani, cu excepția cazului în care se urmărește interesul superior al copilului.

(29) În cazul în care datele biometrice ale unei persoane nu pot fi utilizate sau în cazul în care, în urma unei interogări a datelor respective, nu se obține niciun răspuns, interogarea ar trebui efectuată cu datele de identitate ale persoanei în combinație cu datele din documentul de călătorie. În cazul în care din interogare reiese că datele referitoare la persoana respectivă sunt înregistrate în CIR, autoritățile statelor membre ar trebui să aibă acces să consulte datele de identitate și datele din documentul de călătorie ale persoanei respective, fără ca CIR să furnizeze vreun indiciu cu privire la sistemul de informații al UE de care aparțin datele.

(30) Statele membre ar trebui să adopte măsuri legislative naționale prin care să desemneze autoritățile competente care vor efectua controale de identitate folosind CIR și prin care să stabilească procedurile, condițiile și criteriile pentru aceste controale, care ar trebui să respecte principiul proporționalității. în special, competența de a colecta date biometrice în cursul unui control al identității unei persoane aflate în fața unui reprezentant al acestor autorități ar trebui să fie prevăzută de dreptul intern.

(31) Prezentul regulament ar trebui, de asemenea, să introducă o nouă soluție pentru simplificarea accesului autorităților responsabile de prevenirea, depistarea sau investigarea infracțiunilor de terorism ori a altor infracțiuni grave desemnate de statele membre și al Europol și la alte tipuri de date din EES, VIS, ETIAS sau Eurodac în afară de datele de identitate sau datele din documentele de călătorie. Astfel de date pot fi necesare pentru prevenirea, detectarea sau investigarea infracțiunilor de terorism sau a altor infracțiuni grave într-un anumit caz în care există motive întemeiate să se considere că consultarea acestora va contribui în mod semnificativ la prevenirea, depistarea sau investigarea infracțiunilor de terorism sau a altor infracțiuni grave, în special în cazurile în care există suspiciunea că suspectul, autorul sau victima unei infracțiuni de terorism sau altei infracțiuni grave este o persoană ale cărei date sunt stocate în EES, VIS, ETIAS și Eurodac.

(32) Accesul deplin la datele conținute în sistemele de informații ale UE care este necesar în scopul prevenirii, depistării sau investigării infracțiunilor cu caracter terorist sau a altor infracțiuni grave, în afara accesului la datele de identitate la datele din documentele de călătorie care sunt păstrate în CIR ar trebui să fie în continuare reglementat de instrumentele juridice aplicabile. Nici autoritățile responsabile de prevenirea, depistarea sau investigarea infracțiunilor de terorism ori a altor infracțiuni grave desemnate, nici Europol nu știu dinainte care dintre sistemele de informații ale UE cuprinde date referitoare la persoanele care fac obiectul unei interogări. Acest lucru duce la întârzieri și deficiențe. Utilizatorul final autorizat de autoritatea desemnată ar trebui să aibă posibilitatea să vadă în care dintre acele sisteme de informații ale UE sunt înregistrate datele corespunzătoare rezultatului unei interogări. Sistemul în cauză ar fi, prin urmare, marcat după verificarea automată a prezenței unei concordanțe în sistem [o așa-numită funcționalitate – marcaj privind concordanța („match-flag”)].

(33) În acest context, un răspuns de la CIR nu ar trebui interpretat sau utilizat ca motiv sau cauză pentru a trage concluzii despre o persoană sau pentru a lua măsuri în legătură cu o persoană, ci ar trebui folosit doar pentru a adresa o cerere de acces la sistemele de informații de bază ale UE, cu respectarea condițiilor și a procedurilor prevăzute de instrumentele juridice respective care reglementează un astfel de acces. O astfel de cerere de acces ar trebui să facă obiectul capitolului VII din prezentul regulament și, după caz, Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului ([5]), Directivei (UE) 2016/680 a Parlamentului European și a Consiliului ([6]) sau Regulamentului (UE) 2018/1725 al Parlamentului European și al Consiliului ([7]).

(34) De regulă, atunci când un marcaj privind concordanța arată că datele sunt înregistrate în Eurodac, autoritățile desemnate sau Europol ar trebui să solicite acces deplin la cel puțin unul dintre sistemele de informații ale UE în cauză. În cazul în care, în mod excepțional, nu se solicită un astfel de acces deplin, de exemplu pentru că autoritățile desemnate sau Europol au obținut deja datele prin alte mijloace, sau pentru că dreptul intern nu mai permite obținerea datelor, ar trebui să se înregistreze motivele pentru nesolicitarea accesului.

(35) Înregistrările interogărilor efectuate în CIR ar trebui să indice scopul acestora. În cazul în care o astfel de interogare a fost efectuată utilizându-se o abordare în două etape de consultare a datelor, înregistrările ar trebui să includă o trimitere la dosarul național al investigației sau al cazului, indicând astfel că interogarea a fost efectuată în scopul prevenirii, depistării sau investigării unor infracțiuni de terorism sau a altor infracțiuni grave.

(36) Efectuarea unei interogări în CIR de către autoritățile desemnate și de către Europol pentru a obține un răspuns de tip marcaj privind concordanța, prin care să se indice faptul că datele sunt înregistrate în EES, VIS, ETIAS sau în Eurodac, necesită prelucrarea automată a datelor cu caracter personal. Un marcaj privind concordanța ar trebui să nu dezvăluie datele cu caracter personal ale persoanei în cauză, ci numai să indice dacă anumite date referitoare la persoana respectivă sunt păstrate în vreunul dintre sisteme. Utilizatorul final autorizat nu ar trebui să ie nicio decizie în defavoarea persoanei în cauză bazându-se exclusiv pe apariția unui marcaj privind concordanța. Prin urmare, accesul utilizatorului final la un marcaj privind concordanța reprezintă o ingerință foarte limitată în dreptul persoanei vizate la protecția datelor cu caracter personal, permițând însă autorităților desemnate și Europol solicite acces la datele cu caracter personal într-un mod mai eficace.

(37) Ar trebui instituit MID pentru a sprijini funcționarea CIR și pentru a susține realizarea obiectivelor EES, VIS, ETIAS, Eurodac, SIS și ale ECRIS-TCN. Pentru a fi eficace în ceea ce privește îndeplinirea obiectivelor lor respective, toate aceste sisteme de informații ale UE necesită identificarea precisă a persoanelor ale căror date cu caracter personal sunt stocate în acestea.

(38) Pentru a realiza mai bine obiectivele sistemelor de informații ale UE, autoritățile care utilizează respectivele sisteme ar trebui să poată efectua verificări suficient de sigure cu privire la identitatea persoanelor ale căror date sunt înregistrate în diverse sisteme. Datele de identitate sau datele din documentele de călătorie stocate într-un

([5]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([6]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

([7]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

anumit sistem pot fi incorecte, incomplete sau frauduloase, și în prezent nu există nicio modalitate de detectare a datelor de identitate sau a datelor din documentele de călătorie incorecte, incomplete sau frauduloase prin comparație cu datele stocate într-un alt sistem. Pentru a remedia această situație, este necesar ca la nivelul Uniunii să existe un instrument tehnic care să permită identificarea precisă a persoanelor în aceste scopuri.

(39) MID ar trebui să creeze și să stocheze conexiunile dintre datele stocate în diferitele sisteme de informații ale UE în vederea detectării identităților multiple, cu scopul dublu de a facilita controalele de identitate pentru călătorii de bună credință și, în același timp, de a combate fraudele de identitate. MID ar trebui să conțină exclusiv conexiunile dintre datele privind persoanele care sunt prezente în mai mult de un sistem de informații al UE. Datele conexate ar trebui să se limiteze în mod strict la datele necesare pentru a verifica dacă o persoană este înregistrată în mod justificat sau nejustificat cu mai multe identități diferite în sisteme diferite sau pentru a clarifica dacă două persoane cu date de identitate similare nu sunt, de fapt, aceeași persoană. Prelucrarea datelor prin intermediul ESP și al BMS comun în vederea stabilirii de conexiuni între dosarele din diferite sisteme ar trebui menținută la un nivel minim absolut și, prin urmare, ar trebui să se limiteze la o detectare a identităților multiple care trebuie efectuată la momentul adăugării de date noi în unul dintre sistemele care conțin date stocate în CIR sau la momentul adăugării de date noi în SIS. MID ar trebui să includă garanții împotriva unor eventuale cazuri de discriminare sau a unor decizii nefavorabile care vizează persoane cu identități multiple legale.

(40) Prezentul regulament prevede noi operațiuni de prelucrare a datelor care vizează identificarea corectă a persoanelor în cauză. Aceasta constituie o ingerință în drepturile fundamentale ale acestora, astfel cum sunt protejate prin articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene. Întrucât implementarea efectivă a sistemelor de informații ale UE depinde de identificarea corectă a persoanelor în cauză, o astfel de ingerință este justificată prin invocarea acelorași obiective ca și cele care stau la baza instituirii fiecăruia dintre aceste sisteme: gestionarea eficace a frontierelor Uniunii, securitatea internă a Uniunii și punerea în aplicare eficace a politicilor Uniunii în materie de azil și vize.

(41) Atunci când o autoritate națională sau o agenție a UE creează sau încarcă noi înregistrări, ESP și BMS comun ar trebui să compare datele privind persoanele în CIR și în SIS. O astfel de comparație ar trebui să fie automatizată. CIR și SIS ar trebui să utilizeze BMS comun pentru a detecta posibilele conexiuni pe baza datelor biometrice. CIR și SIS ar trebui să utilizeze ESP pentru a detecta posibilele conexiuni pe baza datelor alfanumerice. CIR și SIS ar trebui să fie în măsură să identifice datele care sunt aceleași sau similare privind o persoană stocate în mai multe sisteme. Dacă este cazul, ar trebui creată o conexiune care să indice că este vorba de aceeași persoană. CIR și SIS ar trebui astfel configurate încât greșelile minore de ortografie sau de transcriere să fie detectate, în așa fel încât să nu se creeze obstacole nejustificate pentru persoana în cauză.

(42) Autoritatea națională sau agenția Uniunii care a înregistrat datele respective în sistemul de informații ar trebui să confirme sau să modifice conexiunile. Această autoritate națională sau agenție a Uniunii ar trebui să aibă acces la datele stocate în CIR sau în SIS, precum și în MID, în scopul verificării manuale a identităților diferite.

(43) O verificare manuală a identităților diferite ar trebui asigurată de către autoritatea care a creat sau actualizat datele care au generat o concordanță, în urma căreia s-a stabilit o conexiune cu date înregistrate în alt sistem de informații al UE. Autoritatea responsabilă de verificarea manuală a identităților diferite ar trebui să evalueze dacă există mai multe identități care se referă la aceeași persoană într-un mod justificat sau nejustificat. Această evaluare ar trebui efectuată, acolo unde este posibil, în prezența persoanelor în cauză, solicitându-se, dacă este necesar, clarificări sau informații suplimentare. Evaluarea ar trebui efectuată fără întârziere, în conformitate cu cerințele legale privind exactitatea informațiilor în temeiul dreptului Uniunii și al dreptului intern.

(44) Pentru conexiunile obținute prin intermediul SIS referitoare la semnalări privind persoane căutate în vederea arestării în scopul predării sau al extrădării, privind persoane dispărute sau vulnerabile, privind persoane căutate în vederea participării la o procedură judiciară sau privind persoane vizate pentru controale discrete, controale prin interviu sau controale specifice, autoritatea responsabilă cu verificarea manuală a identităților diferite ar trebui să fie biroul SIRENE din statul membru care a creat semnalarea. Aceste categorii de semnalări SIS sunt

sensibile și nu ar trebui neapărat să facă obiectul unui schimb cu autoritățile care au creat sau actualizat datele care sunt în conexiune cu acestea din unul dintre celelalte sisteme de informații ale UE. Crearea unei conexiuni cu datele din SIS nu ar trebui să aducă atingere măsurilor care urmează să fie adoptate în conformitate cu Regulamentele (UE) 2018/1860 ([8]), (UE) 2018/1861 ([9]) și (UE) 2018/1862 ([10]) ale Parlamentului European și ale Consiliului.

(45) Crearea acestor conexiuni necesită transparență față de persoanele în cauză. Pentru a facilita punerea în aplicare a garanțiilor necesare în conformitate cu normele aplicabile ale Uniunii în materie de protecție a datelor, persoanele care sunt vizate de o conexiune roșie sau de o conexiune albă ca urmare a unei verificări manuale a identităților diferite ar trebui să fie informate în scris, fără a aduce atingere restricțiilor pentru protejarea securității și a ordinii publice, pentru prevenirea infracțiunilor și pentru garantarea faptului că nicio anchetă națională nu este pusă în pericol. Persoanele respective ar trebui să primească un număr unic de identificare, care să le permită să identifice autoritatea căreia ar trebui să i se adreseze pentru a-și exercita drepturile.

(46) În cazul în care se creează o conexiune galbenă, autoritatea responsabilă cu verificarea manuală a identităților diferite ar trebui să aibă acces la MID. În cazul în care există o conexiune roșie, autoritățile statelor membre și agențiile Uniunii care au acces la cel puțin un sistem de informații al UE inclus in CIR sau la SIS ar trebui să aibă acces la MID. O conexiune roșie ar trebui să indice faptul că o persoană utilizează identități diferite în mod nejustificat sau că o persoană utilizează identitatea unei alte persoane.

(47) Când există o conexiune albă sau verde între datele din două sisteme de informații ale UE, autoritățile statelor membre și agențiile Uniunii ar trebui să aibă acces la MID atunci când respectiva autoritate sau agenție are acces la ambele sisteme de informații. Acest acces ar trebui să se acorde exclusiv pentru a permite respectivei autorități sau agenții să detecteze cazurile potențiale în care datele au fost conexate incorect sau prelucrate în MID, CIR și SIS cu încălcarea prezentului regulament și pentru a lua măsurile pentru a remedia situația și a actualiza sau șterge conexiunea.

(48) Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA) ar trebui să instituie mecanisme automatizate de control al calității datelor și indicatori comuni de calitate a datelor. În plus, ar trebui să fie responsabilă de dezvoltarea unei capacități centrale de monitorizare pentru calitatea datelor și de prezentarea în mod regulat de rapoarte de analiză a datelor în vederea îmbunătățirii controlului în ceea ce privește implementarea și utilizarea sistemelor de informații ale UE de către statele membre. Indicatorii comuni de calitate a datelor ar trebui să includă standarde minime de calitate pentru stocarea datelor în sistemele de informații ale UE sau în componentele de interoperabilitate. Scopul standardelor de calitate privind datele ar trebui să fie, pentru sistemele de informații ale UE sau pentru componentele de interoperabilitate, acela de a identifica într-un mod automatizat datele care par a fi incorecte sau inconsecvente, astfel încât statul membru din care provin să fie în măsură să le verifice și să ia măsurile necesare pentru a le corecta.

(49) Comisia ar trebui să evalueze rapoartele privind calitatea întocmite de eu-LISA și, după caz, ar trebui să formuleze recomandări adresate statelor membre. Statele membre ar trebui să fie responsabile cu pregătirea unui plan de acțiune care să descrie măsurile care vizează remedierea eventualelor deficiențe în ceea ce privește calitatea datelor și ar trebui să prezinte periodic progresele înregistrate.

(50) Formatul universal de mesaje (UMF) ar trebui să reprezinte un standard pentru schimburile de informații transfrontaliere structurate între sistemele de informații, autoritățile sau organizațiile din domeniul justiției și afacerilor interne. UMF ar trebui să definească un vocabular comun și structuri logice pentru informațiile care fac frecvent obiectul schimburilor, cu scopul de a facilita interoperabilitatea, permițând crearea și citirea conținutului în mod coerent și cu asigurarea echivalenței semantice.

(51) Aplicarea standardului UMF poate fi avută în vedere în VIS, SIS și în orice alt model de schimb transfrontalier de informații și sistem de informații în domeniul justiției și afacerilor interne, nou sau existent, elaborat de statele membre.

([8]) Regulamentul (UE) 2018/1860 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind utilizarea Sistemului de informații Schengen pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală (JO L 312, 7.12.2018, p. 1).

([9]) Regulamentul (UE) 2018/1861 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Convenției 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).

([10]) Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare și de 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).

(52) Ar trebui înființat un registru central de raportare și statistici (CRRS) care să genereze date statistice între sisteme și rapoarte analitice în scopuri strategice, operaționale și de asigurare a calității datelor, în conformitate cu instrumentele juridice aplicabile. eu-LISA ar trebui să instituie, să implementeze și să găzduiască CRRS în amplasamentele sale tehnice. CRRS ar trebui să conțină date statistice anonime din sistemele de informații ale UE, CIR, MID și BMS comun. Datele conținute în CRRS nu ar trebui să permită identificarea persoanelor. eu-LISA ar trebui să anonimizeze într-un mod automat datele și ar trebui să înregistreze aceste date anonimizate în CRRS. Procesul de anonimizare a datelor ar trebui să fie automatizat, iar personalul eu-LISA nu ar trebui să aibă acces direct la datele cu caracter personal stocate în sistemele de informații ale UE sau în componentele de interoperabilitate.

(53) Regulamentul (UE) 2016/679 se aplică prelucrării datelor cu caracter personal în scopul interoperabilității efectuate în temeiul prezentului regulament de către autoritățile naționale, cu excepția cazului în care această prelucrare este efectuată de către autoritățile desemnate sau de către punctele centrale de acces din statele membre în scopul prevenirii, depistării sau investigării infracțiunilor de terorism sau a altor infracțiuni grave.

(54) În cazul în care prelucrarea datelor cu caracter personal de către statele membre în scopul interoperabilității în temeiul prezentului regulament este efectuată de către autoritățile competente în scopul prevenirii, depistării sau investigării infracțiunilor de terorism sau a altor infracțiuni grave, se aplică Directiva (UE) 2016/680.

(55) Regulamentul (UE) 2016/679, Regulamentul (UE) 2018/1725 sau, după caz, Directiva (UE) 2016/680 se aplică oricărui transfer de date cu caracter personal către state terțe sau organizații internaționale, efectuate în temeiul prezentului regulament. Fără a aduce atingere motivelor de transfer în temeiul capitolului V din Regulamentul (UE) 2016/679 sau, după caz, al Directivei (UE) 2016/680, orice hotărâre a unei instanțe sau a unui tribunal și orice decizie a unei autorități administrative a unei țări terțe care impun unui operator sau persoanei împuternicite de operator să transfere sau să divulge date cu caracter personal ar trebui să fie recunoscută sau executorie în orice fel numai dacă se bazează pe un acord internațional în vigoare între țara terță solicitantă și Uniune sau un stat membru.

(56) Dispozițiile specifice privind protecția datelor din Regulamentul (UE) 2018/1862 și Regulamentul (UE) 2019/816 al Parlamentului European și al Consiliului ([11]) se aplică prelucrării datelor cu caracter personal în sistemele guvernate de respectivele regulamente.

(57) Regulamentul (UE) 2018/1725 se aplică în cazul prelucrării datelor cu caracter personal de către eu-LISA și de către alte instituții și organisme ale Uniunii atunci când își exercită responsabilitățile care le revin în temeiul prezentului regulament, fără a aduce atingere dispozițiilor Regulamentului (UE) 2016/794, care se aplică prelucrării datelor cu caracter personal de către Europol.

(58) Autoritățile de supraveghere prevăzute în Regulamentul (UE) 2016/679 sau Directiva (UE) 2016/680 ar trebui să monitorizeze legalitatea prelucrării datelor cu caracter personal de către statele membre. Autoritatea Europeană pentru Protecția Datelor ar trebui să monitorizeze activitățile instituțiilor și organelor Uniunii în ceea ce privește prelucrarea datelor cu caracter personal. Autoritatea Europeană pentru Protecția Datelor și autoritățile de supraveghere ar trebui să coopereze între ele în cadrul activităților de monitorizare a prelucrării datelor de către componentele de interoperabilitate. Pentru ca Autoritatea Europeană pentru Protecția Datelor să îndeplinească sarcinile care i-au fost încredințate în temeiul prezentului regulament, sunt necesare resurse suficiente, atât umane, cât și financiare.

(59) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([12]) și a emis un aviz la 16 aprilie 2018 ([13]).

(60) Grupul de lucru instituit prin articolul 29 a emis un aviz la 11 aprilie 2018.

(61) Atât statele membre, cât și eu-LISA ar trebui să dispună de planuri de securitate pentru a facilita îndeplinirea obligațiilor privind securitatea și ar trebui să coopereze între ele pentru a aborda chestiunile legate de securitate. eu-LISA ar trebui, de asemenea, să se asigure că sunt valorificate permanent cele mai recente evoluții tehnologice pentru a asigura integritatea datelor în contextul dezvoltării, proiectării și gestionării componentelor de interoperabilitate. Printre obligațiile eu-LISA în acest sens ar trebui să se numere adoptarea măsurilor necesare pentru

([11]) 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 dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor (ECRIS-TCN), destinat să completeze sistemul european de informații cu privire la cazierele judiciare și de modificare a Regulamentului (UE) 2018/1726 (a se vedea pagina 1 din prezentul Jurnal Oficial).

([12]) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

([13]) JO C 233, 4.7.2018, p. 12.

a împiedica accesul persoanelor neautorizate, cum ar fi angajații prestatorilor externi de servicii, la datele personale prelucrate prin intermediul componentelor de interoperabilitate. Atunci când atribuie contracte pentru prestarea de servicii, statele membre și eu-LISA ar trebui să ia în considerare toate măsurile necesare pentru a asigura respectarea actelor cu putere de lege și a reglementărilor referitoare la protecția datelor personale și la viața privată a persoanelor sau pentru a proteja interesele esențiale de securitate, în temeiul Regulamentului (UE) 2018/1046 al Parlamentului European și al Consiliului ([14]) și cu convențiile internaționale aplicabile. eu-LISA ar trebui să aplice principiile protejării vieții private începând cu momentul conceperii și în mod implicit pe parcursul dezvoltării componentelor de interoperabilitate.

(62) În vederea sprijinirii întocmirii de statistici și rapoarte, este necesar ca personalul autorizat al autorităților competente, al instituțiilor și al agențiilor Uniunii menționate în prezentul regulament să aibă acces la anumite date referitoare la anumite componente de interoperabilitate, dar nu și la date care ar permite identificarea persoanelor.

(63) Pentru ca autoritățile din statele membre și agențiile Uniunii să se poată adapta noilor cerințe privind utilizarea ESP, este necesar să se prevadă o perioadă de tranziție. În mod similar, pentru a se asigura coerența și funcționarea optimă a MID, ar trebui stabilite măsuri tranzitorii pentru punerea în funcțiune a acestuia.

(64) Întrucât obiectivul prezentului regulament, și anume instituirea unui cadru de interoperabilitate între sistemele de informații ale Uniunii, nu poate fi realizat într-o măsură suficientă de statele membre, dar, având în vedere amploarea și efectele acțiunii, poate fi îndeplinit mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană (TUE). În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea acestui obiectiv.

(65) Suma rămasă din bugetul alocat frontierelor inteligente în Regulamentul (UE) nr. 515/2014 al Parlamentului European și al Consiliului ([15]) ar trebui realocată prezentului regulament, în temeiul articolului 5 alineatul (5) litera (b) din Regulamentul (UE) nr. 515/2014, pentru a acoperi costurile dezvoltării componentelor de interoperabilitate.

(66) Pentru a completa anumite aspecte tehnice detaliate ale prezentului regulament, competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene (TFUE) ar trebui să fie delegată Comisiei în ceea ce privește:

— prelungirea perioadei de tranziție pentru utilizarea ESP;

— prelungirea perioadei de tranziție pentru detectarea identităților multiple efectuată de unitatea centrală a ETIAS;

— procedurile de identificare a cazurilor în care datele de identitate pot fi considerate ca fiind aceleași sau similare;

— normele privind funcționarea CRRS, inclusiv garanții specifice pentru prelucrarea datelor cu caracter personal și normele de securitate aplicabile registrului;

— normele detaliate privind funcționarea portalului web.

Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare ([16]). În special, pentru a se asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(67) Pentru a asigura condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui conferite competențe de executare Comisiei în vederea stabilirii datelor de la care ESP, BMS comun, CIR, MID și CRRS trebuie să fie puse în funcțiune.

([14]) Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 privind normele financiare aplicabile bugetului general al Uniunii, de modificare a Regulamentelor (UE) nr. 1296/2013, (UE) nr. 1301/2013, (UE) nr. 1303/2013, (UE) nr. 1304/2013, (UE) nr. 1309/2013, (UE) nr. 1316/2013, (UE) nr. 223/2014, (UE) nr. 283/2014 și a Deciziei nr. 541/2014/UE și de abrogare a Regulamentului (UE, Euratom) nr. 966/2012 (JO L 193, 30.7.2018, p. 1).

([15]) Regulamentul (UE) nr. 515/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 de instituire, în cadrul Fondului pentru securitate internă, a instrumentului de sprijin financiar pentru frontiere externe și vize și de abrogare a Deciziei nr. 574/2007/CE (JO L 150, 20.5.2014, p. 143).

([16]) JO L 123, 12.5.2016, p. 1.

(68) De asemenea, ar trebui conferite competențe de executare Comisiei în vederea adoptării unor norme detaliate privind: detaliile tehnice ale profilurilor utilizatorilor ESP; specificațiile soluției tehnice menite să permită interogarea sistemelor de informații ale UE, a datelor Europol și a bazelor de date ale Interpol prin ESP și formatul răspunsurilor ESP; normele tehnice de creare a unor conexiuni în MID între datele provenite de la diferitele sisteme de informații ale Uniunii; conținutul și prezentarea formularului care trebuie utilizat pentru informarea persoanei vizate în cazul în care este creată o conexiune roșie; cerințele în materie de performanță și monitorizarea performanței BMS comun; mecanismele și procedurile automatizate de control al calității datelor și indicatorii aferenți; dezvoltarea standardului UMF; procedura de cooperare în cazul unor incidente de securitate; și specificațiile soluției tehnice care dă statelor membre posibilitatea de a gestiona cererile de acces ale utilizatorilor. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([17]).

(69) Întrucât componentele de interoperabilitate vor presupune prelucrarea unor volume semnificative de date cu caracter personal sensibile, este important ca persoanele ale căror date sunt prelucrate prin intermediul acestor componente să își poată exercita în mod efectiv drepturile în calitate de persoane vizate, astfel cum se prevede în Regulamentul (UE) 2016/679, în Directiva (UE) 2016/680 și în Regulamentul (UE) 2018/1725. Persoanelor vizate ar trebui să li se pună la dispoziție un portal web care să le înlesnească exercitarea drepturilor de acces, de rectificare, de ștergere și de restricționare a prelucrării datelor lor cu caracter personal. eu-LISA ar trebui să creeze și să gestioneze un astfel de portal web.

(70) Unul dintre principiile de bază ale protecției datelor este reducerea la minimum a datelor: în temeiul articolului 5 alineatul (1) litera (c) din Regulamentul (UE) 2016/679, prelucrarea datelor cu caracter personal trebuie să fie adecvată, relevantă și limitată la ceea ce este necesar în raport cu scopurile în care sunt prelucrate. Din acest motiv, componentele de interoperabilitate ar trebui să nu prevadă stocarea oricăror date cu caracter personal noi, cu excepția conexiunilor care vor fi stocate în MID și care sunt minimumul necesar în scopul prezentului regulament.

(71) Prezentul regulament ar trebui să cuprindă dispoziții clare privind răspunderea și dreptul la despăgubiri în cazul prelucrării ilegale a datelor cu caracter personal sau al oricărui alt act incompatibil cu acesta. Astfel de dispoziții nu ar trebui să aducă atingere dreptului la despăgubiri ori răspunderii operatorului sau a persoanei împuternicite de operator în conformitate cu Regulamentul (UE) 2016/679, cu Directiva (UE) 2016/680 și cu Regulamentul (UE) 2018/1725. eu-LISA ar trebui să răspundă pentru orice prejudiciu pe care l-a cauzat în calitatea sa de persoană împuternicită de operator în cazul în care nu a respectat obligațiile care îi sunt impuse în mod specific de prezentul regulament sau în cazul în care a acționat în afara sau în contradicție cu instrucțiunile legale ale statului membru care este operator.

(72) Prezentul regulament nu aduce atingere aplicării Directivei 2004/38/CE a Parlamentului European și a Consiliului ([18]).

(73) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la TUE și la TFUE, Danemarca nu participă la adoptarea prezentului regulament, acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică. Deoarece prezentul regulament constituie o dezvoltare a acquis-ului Schengen, în privința dispozițiilor sale referitoare la SIS, astfel cum este reglementat prin Regulamentul (UE) 2018/1862, Danemarca decide, în conformitate cu articolul 4 din protocolul respectiv, în termen de șase luni de la data la care Consiliul decide cu privire la prezentul regulament dacă îl va pune în aplicare în legislația sa națională.

(74) În privința dispozițiilor sale referitoare la SIS, astfel cum este reglementat prin Regulamentul (UE) 2018/1862, Regatul Unit participă la prezentul regulament, în conformitate cu articolul 5 alineatul (1) din Protocolul nr. 19 privind acquis-ul Schengen integrat în cadrul Uniunii Europene, anexat la TUE și la TFUE, și cu articolul 8 alineatul (2) din Decizia 2000/365/CE a Consiliului ([19]). De asemenea, în privința dispozițiilor sale referitoare la Eurodac și la ECRIS-TCN, în conformitate cu articolul 3 din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la TUE și la TFUE, Regatul Unit a notificat, prin scrisoarea din 18 mai 2018, intenția sa de a participa la adoptarea și la aplicarea prezentului regulament.

([17]) Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

([18]) Directiva 2004/38/CE a Parlamentului European și a Consiliului din 29 aprilie 2004 privind dreptul la liberă circulație și ședere pe teritoriul statelor membre pentru cetățenii Uniunii și membrii familiilor acestora, de modificare a Regulamentului (CEE) nr. 1612/68 și de abrogare a Directivelor 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE și 93/96/CEE (JO L 158, 30.4.2004, p. 77).

([19]) Decizia 2000/365/CE a Consiliului din 29 mai 2000 privind solicitarea Regatului Unit al Marii Britanii și Irlandei de Nord de a participa la unele dintre dispozițiile acquis-ului Schengen (JO L 131, 1.6.2000, p. 43).

(75) În privința dispozițiilor sale referitoare la SIS, astfel cum este reglementat prin Regulamentul (UE) 2018/1862, Irlanda ar putea, în principiu, participa la prezentul regulament, în conformitate cu articolul 5 alineatul (1) din Protocolul nr. 19 privind acquis-ul Schengen integrat în cadrul Uniunii Europene, anexat la TUE și la TFUE, și cu articolul 6 alineatul (2) din Decizia 2002/192/CE a Consiliului ([20]). De asemenea, în privința dispozițiilor sale referitoare la Eurodac și la ECRIS-TCN, în conformitate cu articolele 1 și 2 din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la TUE și la TFUE, și fără a aduce atingere articolului 4 din protocolul respectiv, Irlanda nu participă la adoptarea prezentului regulament și acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică. Având în vedere că nu este posibil, în circumstanțele actuale, să se garanteze că prezentul regulament este aplicabil în întregime Irlandei, în conformitate cu articolul 288 din TFUE, Irlanda nu participă la adoptarea prezentului regulament și acesta nu este obligatoriu pentru respectivul stat membru și nu i se aplică, fără a se aduce atingere drepturilor sale în temeiul Protocoalelor nr. 19 și nr. 21.

(76) În ceea ce privește Islanda și Norvegia, prezentul regulament constituie, în privința dispozițiilor sale referitoare la SIS, astfel cum este reglementat prin Regulamentul (UE) 2018/1862, o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Acordului încheiat de Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei privind asocierea acestora din urmă la implementarea, aplicarea și dezvoltarea acquis-ului Schengen ([21]), care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE a Consiliului ([22]).

(77) În ceea ce privește Elveția, prezentul regulament constituie, în privința dispozițiilor sale referitoare la SIS, astfel cum este reglementat prin Regulamentul (UE) 2018/1862, o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Acordului dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen ([23]), care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE, coroborat cu articolul 3 din Decizia 2008/149/JAI a Consiliului ([24]).

(78) În ceea ce privește Liechtenstein, prezentul regulament constituie, în privința dispozițiilor sale referitoare la SIS, astfel cum este reglementat prin Regulamentul (UE) 2018/1862, o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Protocolului dintre Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen ([25]), care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE, coroborat cu articolul 3 din Decizia 2011/350/UE a Consiliului ([26]).

(79) Prezentul regulament respectă drepturile fundamentale și se conformează principiilor recunoscute, în special, de Carta drepturilor fundamentale a Uniunii Europene, și ar trebui să fie pus în aplicare în conformitate cu aceste drepturi și principii.

(80) Pentru ca prezentul regulament să se încadreze în cadrul juridic existent, Regulamentul (UE) 2018/1726 al Parlamentului European și al Consiliului ([27]) și Regulamentele (UE) 2018/1862 și (UE) 2019/816 ar trebui modificate în consecință,

---

([20]) Decizia 2002/192/CE a Consiliului din 28 februarie 2002 privind solicitarea Irlandei de a participa la unele dintre dispozițiile acquis-ului Schengen (JO L 64, 7.3.2002, p. 20).

([21]) JO L 176, 10.7.1999, p. 36.

([22]) Decizia 1999/437/CE a Consiliului din 17 mai 1999 privind anumite modalități de aplicare a Acordului încheiat între Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei în ceea ce privește asocierea acestor două state în vederea punerii în aplicare, a asigurării respectării și dezvoltării acquis-ului Schengen (JO L 176, 10.7.1999, p. 31).

([23]) JO L 53, 27.2.2008, p. 52.

([24]) Decizia 2008/149/JAI a Consiliului din 28 ianuarie 2008 privind încheierea, în numele Uniunii Europene, a Acordului între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen (JO L 53, 27.2.2008, p. 50).

([25]) JO L 160, 18.6.2011, p. 21.

([26]) Decizia 2011/350/UE a Consiliului din 7 martie 2011 privind încheierea, în numele Uniunii Europene, a Protocolului dintre Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen, în ceea ce privește eliminarea controalelor la frontierele interne și circulația persoanelor (JO L 160, 18.6.2011, p. 19).

([27]) Regulamentul (UE) 2018/1726 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA) și de modificare a Regulamentului (CE) nr. 1987/2006 și a Deciziei 2007/533/JAI a Consiliului, precum și de abrogare a Regulamentului (UE) nr. 1077/2011 (JO L 295, 21.11.2018, p. 99).

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

Dispoziții generale

Articolul 1

Obiect

(1) Prezentul regulament, împreună cu Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului ([28]), stabilește un cadru pentru a asigura interoperabilitatea dintre Sistemul de intrare/ieșire (EES), Sistemul de informații privind vizele (VIS), Sistemul european de informații și de autorizare privind călătoriile (ETIAS), Eurodac, Sistemul de informații Schengen (SIS) și Sistemul european de informații cu privire la cazierele judiciare ale resortisanților țărilor terțe (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 identități multiple (MID).

(3) Prezentul regulament cuprinde, de asemenea, dispoziții privind cerințele de calitate a datelor, formatul universal pentru mesaje (UMF), registrul central de raportare și statistici (CRRS) și responsabilitățile statelor membre și ale Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA) în ceea ce privește conceperea, dezvoltarea și funcționarea componentelor de interoperabilitate.

(4) Prezentul regulament adaptează totodată procedurile și condițiile în care autoritățile desemnate și Agenția 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 infracțiunilor de terorism sau a altor infracțiuni grave.

(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;

([28]) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații 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).

(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;

(f) raționalizarea condițiilor de acces al autorităților desemnate la EES, VIS, ETIAS și Eurodac, asigurând totodată condiții necesare și proporționale 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 informații ale UE menționate la alineatul (1).

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

Articolul 4

Definiții

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 ([29]);

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 polițistul de frontieră desemnat în conformitate cu dreptul intern să efectueze verificări la frontiere;

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

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

6. „identificare” înseamnă procesul de determinare a identității 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);

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

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

9. „date dactiloscopice” înseamnă imagini de amprente digitale și imagini de amprente digitale latente care, datorită unicității lor și punctelor de referință pe care le conțin, permit comparații fiabile și concludente referitoare la identitatea unei persoane;

([29]) 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).

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

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

12. „șablon biometric” înseamnă o reprezentare matematică obținută 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, țara care l-a eliberat, data expirării perioadei de valabilitate a documentului de călătorie și codul din trei litere al țării care a eliberat documentul de călătorie;

15. „sisteme de informații 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 menționate 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 notițe (baza de date TDAWN);

18. „concordanță” înseamnă existența unei corespondențe 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 informații sau într-o bază de date;

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

20. „autorități desemnate” înseamnă autoritățile desemnate de statele membre, definite la articolul 3 alineatul (1) punctul 26 din Regulamentul (UE) 2017/2226 al Parlamentului European și al Consiliului ([30]), la articolul 2 alineatul (1) litera (e) din Decizia 2008/633/JAI a Consiliului ([31]) și la articolul 3 alineatul (1) punctul 21 din Regulamentul (UE) 2018/1240 al Parlamentului European și al Consiliului ([32]);

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 ([33]) 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 ([34]) 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 ([35]);

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;

([30]) Regulamentul (UE) 2017/2226 al Parlamentului European și al Consiliului din 30 noiembrie 2017 de instituire a Sistemului de intrare/ieșire (EES) pentru înregistrarea datelor de intrare și de ieșire și a datelor referitoare la refuzul intrării ale resortisanților țărilor terțe care trec frontierele externe ale statelor membre, de stabilire a condițiilor de acces la EES în scopul aplicării legii și de modificare a Convenției de punere în aplicare a Acordului Schengen și a Regulamentelor (CE) nr. 767/2008 și (UE) nr. 1077/2011 (Regulamentul EES) (JO L 327, 9.12.2017, p. 20).

([31]) Decizia 2008/633/JAI a Consiliului din 23 iunie 2008 privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave (JO L 218, 13.8.2008, p. 129).

([32]) Regulamentul (UE) 2018/1240 al Parlamentului European și al Consiliului din 12 septembrie 2018 de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS) și de modificare a Regulamentelor (UE) nr. 1077/2011, (UE) nr. 515/2014, (UE) 2016/399, (UE) 2016/1624 și (UE) 2017/2226 (JO L 236, 19.9.2018, p. 1).

([33]) 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).

([34]) 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).

([35]) 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).

26. „Eurodac" înseamnă Eurodac, instituit de Regulamentul (UE) nr. 603/2013 al Parlamentului European și al Consiliului ([36]);

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.

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, apartenență la o minoritate națională, situație 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 vieții private și la protecția datelor cu caracter personal. Se acordă o atenție specială copiilor, persoanelor în vârstă, persoanelor cu handicap și persoanelor care au nevoie de protecție internațională. 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 autorităților statelor membre și al agențiilor Uniunii la sistemele de informații 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 comunicații între ESP, statele membre și agențiile Uniunii care au dreptul să utilizeze ESP;

(c) o infrastructură de comunicații 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.

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

Articolul 7

Utilizarea portalului european de căutare

(1) Utilizarea ESP este rezervată autorităților statelor membre și agențiilor Uniunii care au acces la cel puțin unul dintre sistemele de informații ale UE, în conformitate cu instrumentele juridice care reglementează aceste sisteme de informații 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 autorități ale statelor membre și agenții ale Uniunii pot utiliza ESP și datele furnizate de acesta exclusiv pentru obiectivele și scopurile prevăzute de instrumentele juridice care reglementează respectivele sisteme de informații ale UE, de Regulamentul (UE) 2016/794 și de prezentul regulament.

([36]) 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).

(2) Autoritățile statelor membre și agențiile Uniunii menționate 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 informații 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 menționate la articolele 20, 21 și 22.

(3) Autoritățile statelor membre menționate la alineatul (1) pot utiliza ESP pentru a căuta date referitoare la persoane sau la documentele de călătorie ale acestora în SIS central menționat în Regulamentul (UE) 2018/1860 și în Regulamentul (UE) 2018/1861.

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

(5) Autoritățile statelor membre și agențiile Uniunii menționate 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 menționate la alineatul (2). Fiecare profil cuprinde, în conformitate cu dreptul Uniunii și dreptul intern următoarele informații:

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

(b) sistemele de informații 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 informații 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 menționate la alineatul (1), în conformitate cu drepturile de acces ale utilizatorilor ESP în temeiul instrumentelor juridice care reglementează sistemele de informații ale UE și în temeiul dreptului intern. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 70 alineatul (2).

(3) Profilurile menționate la alineatul (1) sunt revizuite cu regularitate de către eu-LISA în cooperare cu statele membre, cel puțin 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 funcție 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 informații 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 interfeței pe baza UMF menționat 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 conțin.

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

ESP nu furnizează nicio informație referitoare la datele din sistemele de informații 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.

(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.

(2) În cazul în care, din cauza unei disfuncționalități a infrastructurii naționale 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 informații ale UE sau în CIR, statul membru respectiv notifică eu-LISA și Comisia în mod automat.

(3) În cazurile menționate la alineatele (1) și (2) din prezentul articol și până la remedierea problemei tehnice, obligația menționată la articolul 7 alineatele (2) și (4) nu se aplică, iar statele membre au acces la sistemele de informații 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 disfuncționalități a infrastructurii unei agenții 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 informații ale Uniunii sau în CIR, agenția 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 obținute pe baza datelor biometrice menționate la articolul 13 care sunt stocate în CIR și în SIS și permite efectuarea de interogări folosind date biometrice în mai multe sisteme de informații 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 comunicații 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 obține din următoarele date biometrice:

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

(b) datele menționate la articolul 5 alineatul (1) litera (b) și alineatul (2) din Regulamentul (UE) 2019/816.

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

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

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

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

(5) Prin intermediul unui act de punere în aplicare, Comisia stabilește cerințele de performanță pentru BMS comun și modalitățile practice de monitorizare a performanței 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 menționată 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 menționate 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.

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.

(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 menționate la articolul 18;

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

(c) o infrastructură de comunicații 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 disfuncționalități 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 identități multiple în temeiul articolului 21 sau al prevenirii, depistării ori investigării infracțiunilor de terorism sau a altor infracțiuni grave în temeiul articolului 22, utilizatorii CIR sunt notificați în mod automat de către eu-LISA.

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

Articolul 18

Datele din registrul comun de date de identitate

(1) CIR stochează următoarele date, separate în mod logic, în funcție de sistemul de informații din care provin datele menționate la articolul 5 alineatul (1) litera (b) și alineatul (2), precum și următoarele date enumerate la articolul 5 alineatul (1) litera (a) din Regulamentul (UE) 2019/816: numele (de familie), prenumele, data nașterii, locul nașterii (localitatea și țara), cetățenia sau cetățeniile, genul, numele anterioare, dacă este cazul, pseudonimele sau numele de împrumut, dacă sunt disponibile, precum și, dacă sunt disponibile, informațiile privind documentele de călătorie.

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

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

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

(5) Stocarea datelor menționate 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 menționate 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 informații 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 poliție, în conformitate cu alineatele (2) și (5), numai în următoarele circumstanțe:

(a) în cazul în care o autoritate de poliție 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.

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

(2) În cazul în care survine una dintre circumstanțele enumerate la alineatul (1) și o autoritate de poliție are competențe în acest sens în temeiul unor măsuri legislative naționale, astfel cum se menționează 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 condiția ca această procedură să fie inițiată în prezența persoanei respective.

(3) În cazul în care, în urma interogării, reiese că în CIR sunt stocate date referitoare la persoana respectivă, autoritatea de poliție are acces să consulte datele menționate 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 combinație 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 poliție are competențe în acest sens în temeiul unor măsuri legislative naționale, 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 rămășițelor 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 naționale. Cu această ocazie, statele membre iau în considerare necesitatea de a evita orice discriminare împotriva resortisanților țărilor terțe. Aceste măsuri legislative precizează scopurile precise ale identificării din cele menționate la articolul 2 alineatul (1) literele (b) și (c). Statele membre desemnează autoritățile de poliție competente și stabilesc procedurile, condițiile și criteriile aferente acestor controale.

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

Articolul 21

Accesul la registrul comun de date de identitate în scopul detectării de identități 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 identităților diferite în conformitate cu articolul 29 are acces, exclusiv în scopul verificării respective, la datele menționate la articolul 18 alineatele (1) și (2) stocate în CIR conexate printr-o conexiune galbenă.

(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.

(2) Dosarul individual este stocat în CIR numai atât timp cât datele corespondente sunt stocate cel puțin într-unul din sistemele de informații 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 operațiunilor de prelucrare a datelor efectuate în CIR, în conformitate cu alineatele (2), (3) și (4) din prezentul articol.

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

(a) statul membru sau agenția 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 operațiunilor de prelucrare a datelor efectuate în CIR în temeiul articolului 21. În aceste înregistrări sunt incluse următoarele informații:

(a) statul membru sau agenția 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 informații al UE de la care s-au primit datele.

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

(a) data și ora efectuării interogării;

(b) datele utilizate pentru lansarea interogării;

(c) rezultatele interogării;

(d) statul membru sau agenția 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 Protecția 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 condițiile prevăzute la articolul 22 alineatele (1) și (2) din prezentul regulament.

(5) Fiecare stat membru păstrează înregistrările interogărilor efectuate de autoritățile sale și de personalul acestora autorizat în mod corespunzător să utilizeze CIR în temeiul articolelor 20, 21 și 22. Fiecare agenție 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) referința dosarului național;

(b) scopul accesării;

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

(7) Înregistrările menționate la alineatele (2)-(6) 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.

(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 identități multiple

Articolul 25

Detectorul de identități multiple

(1) Pentru a susține funcționarea CIR și a sprijini realizarea obiectivelor EES, VIS, ETIAS, Eurodac, SIS și ECRIS-TCN, se instituie un detector de identități multiple (MID), care creează și stochează dosare de confirmare a identității, astfel cum se menționează la articolul 34, și 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 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.

(4) 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 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 identității menționat 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 informații ale UE. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 70 alineatul (2).

Articolul 29

Verificarea manuală a identităților diferite și autoritățile responsabile

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

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

(b) autoritățile centrale ale statului membru de condamnare în cazul concordanțelor obținute 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 identităților diferite în dosarul de confirmare a identității.

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

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

(b) cu privire la persoane dispărute sau vulnerabile, menționată 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.

(3) Autoritatea responsabilă de verificarea manuală a identităților diferite are acces la datele conexate conținute 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 identitățile 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 identităților diferite evaluează fiecare conexiune separat.

(5) În cazul în care datele care au generat concordanța erau deja conexate, autoritatea responsabilă de verificarea manuală a identităților diferite ține 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 identităților diferite, o conexiune între datele din două sau mai multe sisteme de informații 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 puțin unul dintre sistemele de informații ale UE nu conține 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 informații 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 identităților 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 identităților diferite a ajuns la concluzia că datele conexate se referă la două persoane diferite;

(c) datele conexate au date de identitate diferite, dar au în comun aceleași date privind documentele de călătorie, cel puțin unul dintre sistemele de informații ale UE nu conține date biometrice privind persoana în cauză, iar autoritatea responsabilă de verificarea manuală a identităților 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 informații 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 deține 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 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.

Articolul 32

Conexiune roșie

(1) O conexiune între datele din două sau mai multe sisteme de informații 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 identităților 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 identităților diferite a ajuns la concluzia că datele conexate se referă la două persoane diferite dintre care cel puțin 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 identităților 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 puțin unul dintre sistemele de informații ale UE nu conține date biometrice privind persoana în cauză, iar autoritatea responsabilă de verificarea manuală a identităților diferite a ajuns la concluzia că datele conexate se referă în mod nejustificat la aceeași persoană.

(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 informații ale UE, MID indică datele menționate la articolul 34. Măsurile subsecvente creării unei conexiuni roșii se iau în conformitate cu dreptul Uniunii și cu dreptul intern, orice consecință juridică pentru persoana în cauză bazându-se exclusiv pe datele relevante privind persoana respectivă. Din simpla existență a unei conexiuni roșii nu derivă nicio consecință 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 dispozițiilor referitoare la gestionarea semnalărilor în SIS din Regulamentele (UE) 2018/1860, (UE) 2018/1861 și (UE) 2018/1862 și fără a aduce atingere restricțiilor necesare pentru protejarea securității și a ordinii publice, pentru prevenirea infracțiunilor și pentru garantarea faptului că nicio anchetă națională nu va fi pusă în pericol, în cazul în care se creează o conexiune roșie, autoritatea responsabilă de verificarea manuală a identităților diferite informează persoana în cauză cu privire la prezența unor date de identitate multiple ilegale și pune la dispoziția persoanei în cauză un număr de identificare unic, astfel cum este menționat la articolul 34 litera (c) din prezentul regulament, o trimitere la autoritatea responsabilă de verificarea manuală a identităților diferite, astfel cum este menționată 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) Informațiile menționate la 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).

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

(7) În cazul în care o autoritate a unui stat membru sau o agenție 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 dispozițiilor prezentului regulament, autoritatea sau agenția respectivă verifică datele relevante stocate în CIR și SIS și:

(a) în cazul în care conexiunea se referă la una dintre semnalările SIS menționate 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 agenția Uniunii și, dacă este cazul, rectifică sau șterge conexiunea din MID imediat.

Autoritatea competentă a statului membru care obține dovezile informează fără întârziere autoritatea statului membru responsabil de verificarea manuală a identităților 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 informații 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 puțin unul dintre sistemele de informații 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 identităților 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 informații ale UE, MID indică faptul că datele de identitate ale datelor conexe corespund aceleiași persoane. Sistemele de informații ale UE în care s-a lansat interogarea răspund indicând, după caz, toate datele conexate referitoare la persoana respectivă și generând, prin urmare, o concordanță 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 dispozițiilor referitoare la gestionarea semnalărilor în SIS din Regulamentele (UE) 2018/1860, (UE) 2018/1861 și (UE) 2018/1862 și fără a aduce atingere restricțiilor necesare pentru protejarea securității și a ordinii publice, pentru prevenirea infracțiunilor și pentru garantarea faptului că nicio anchetă națională nu va fi pusă în pericol, în cazul în care este creată o conexiune albă în urma unei verificări manuale a unor identități diferite, autoritatea responsabilă de verificarea manuală a identităților diferite informează persoana în cauză cu privire la prezența unor date de identitate similare sau diferite și furnizează persoanei în cauză un număr de identificare unic, astfel cum este menționat la articolul 34 litera (c) din prezentul regulament, o trimitere către la autoritatea responsabilă de verificarea manuală a identităților diferite, astfel cum este menționată 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) 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;

(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).

(5) La un an de la instituirea mecanismelor și procedurilor automatizate de control al calității 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 dispoziția Comisiei un plan de acțiune pentru remedierea deficiențelor identificate în raportul de evaluare și, în special, a problemelor de calitate a datelor cauzate de datele eronate din sistemele de informații ale UE. Statele membre raportează regulat Comisiei cu privire la progresele înregistrate în funcție de acest plan de acțiune până în momentul în care acesta este pus în aplicare pe deplin.

Comisia transmite raportul de evaluare Parlamentului European, Consiliului, Autorității Europene pentru Protecția Datelor, Comitetului european pentru protecția datelor și Agenției pentru Drepturi Fundamentale a Uniunii Europene instituită prin Regulamentul (CE) nr. 168/2007 al Consiliului ([37]).

Articolul 38

Formatul universal pentru mesaje

(1) Se instituie un format universal pentru mesaje (UMF). UMF definește standardele pentru anumite elemente de conținut ale schimbului transfrontalier de informații între sistemele de informații, autoritățile sau organizațiile participante din domeniul justiției și afacerilor interne.

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

(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 agenție a Uniunii a unor noi modele de schimb de informații și sisteme de informații în domeniul justiției și afacerilor interne.

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

Articolul 39

Registrul central de raportare și statistici

(1) Se instituie un registru central de raportare și statistici (CRRS) în scopul de a susține obiectivele SIS, Eurodac și ECRIS-TCN, în conformitate cu instrumentele juridice respective care reglementează sistemele menționate, și de a furniza date statistice utilizabile între sisteme și rapoarte analitice în scop operațional, de elaborare a politicilor și de asigurare a calității datelor.

(2) eu-LISA creează, implementează și găzduiește în amplasamentele sale tehnice CRRS care conține datele și statisticile menționate la articolul 74 din Regulamentul (UE) 2018/1862 și la articolul 32 din Regulamentul (UE) 2019/816, separate în mod logic pe sisteme de informații ale UE. 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, autorităților menționate la articolul 74 din Regulamentul (UE) 2018/1862 și la articolul 32 din Regulamentul (UE) 2019/816.

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

Datele conținute 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 comunicații 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 funcționarea CRRS, inclusiv garanții specifice pentru prelucrarea datelor cu caracter personal în temeiul alineatelor (2) și (3) din prezentul articol și norme de securitate aplicabile registrului.

CAPITOLUL VII

Protecția datelor

Articolul 40

Operatorul de date

(1) În ceea ce privește prelucrarea datelor în BMS comun, autoritățile 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 obținute din datele menționate 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, autoritățile 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 menționate 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.

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

(a) Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă este operator de date în înțelesul 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) autoritățile statelor membre care introduc sau modifică date în dosarul de confirmare a identității 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 protecției datelor, inclusiv pentru verificarea admisibilității unei interogări și a legalității prelucrării datelor, operatorii de date au acces la înregistrările menționate la articolele 10, 16, 24 și 36 pentru automonitorizarea menționată 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 înțelesul 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 autoritățile din statele membre asigură securitatea prelucrărilor de date cu caracter personal efectuate în temeiul prezentului regulament. eu-LISA, unitatea centrală a ETIAS, Europol și autoritățile 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 comunicații aferente.

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

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

(b) a interzice accesul persoanelor neautorizate la echipamentele și instalațiile 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;

(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.

(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:

(a) orice persoană sau stat membru care a suferit prejudicii materiale sau morale ca urmare a unei operațiuni ilegale de prelucrare a datelor cu caracter personal sau a oricărei alte acțiuni 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 acțiuni realizate de către Europol, Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă sau eu-LISA care este incompatibilă cu prezentul regulament are dreptul de a primi despăgubiri din partea agenției respective.

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

(2) Dacă orice nerespectare de către un stat membru a obligațiilor în temeiul prezentului regulament provoacă prejudicii componentelor de interoperabilitate, răspunderea aparține statului membru respectiv, cu excepția cazului în care eu-LISA sau un alt stat membru care are obligații 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 menționate 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 menționate la alineatele (1) și (2) fac obiectul condițiilor 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 dispoziția persoanelor ale căror date sunt colectate informațiile 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 informațiile la momentul colectării acestor date.

(2) Informațiile sunt furnizate într-un limbaj clar și simplu, într-o limbă pe care persoana în cauză o înțelege sau despre care se poate presupune în mod rezonabil că o înțelege. Aceasta trebuie să includă furnizarea de informații 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 protecție 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 restricționarea 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 (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 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 model de e-mail pentru a facilita comunicarea între utilizatorul portalului și autoritatea competentă a statului membru responsabil de verificarea manuală a identităților diferite. Acest e-mail trebuie să includă un spațiu dedicat numărului de identificare unic menționat la articolul 34 litera (c) pentru a permite autorității competente a statului membru responsabil de verificarea manuală a identităților diferite să identifice datele în cauză.

(4) Statele membre comunică eu-LISA datele de contact ale tuturor autorităților care sunt competente să examineze și să răspundă oricărei cereri menționate 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 funcționarea portalului web, inclusiv a interfeței pentru utilizatori, limbile în care acesta este disponibil și modelul de e-mail.

Articolul 50

Comunicarea datelor cu caracter personal către țări terțe, organizații internaționale și părți 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 dispoziția unei țări terțe, a unei organizații internaționale sau a unei părți private.

Articolul 51

Supravegherea de către autoritățile de supraveghere

(1) Fiecare stat membru se asigură că autoritățile 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 naționale adoptate în temeiul Directivei (UE) 2016/680 sunt aplicabile, dacă este relevant, accesului autorităților polițienești și autorităților desemnate la componentele de interoperabilitate, inclusiv în ceea ce privește drepturile persoanelor ale căror date sunt accesate în acest mod.

(3) Autoritățile de supraveghere garantează că, cel puțin la fiecare patru ani, se realizează un audit al operațiunilor de prelucrare a datelor cu caracter personal de către autoritățile naționale responsabile, în sensul prezentului regulament, în conformitate cu standardele internaționale de audit relevante.

Autoritățile de supraveghere publică anual numărul solicitărilor de rectificare sau ștergere a datelor cu caracter personal sau de restricționare a prelucrării datelor cu caracter personal, acțiunile întreprinse ulterior și numărul rectificărilor, ștergerilor și restricționărilor prelucrării efectuate în urma solicitărilor depuse de persoanele în cauză.

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

(5) Statele membre oferă toate informațiile solicitate de autoritatea de supraveghere menționată la articolul 51 alineatul (1) din Regulamentul (UE) 2016/679 și, în special, îi comunică informații privind activitățile desfășurate în conformitate cu responsabilitățile lor, în temeiul prezentului regulament. Statele membre acordă autorităților de supraveghere menționate la articolul 51 alineatul (1) din Regulamentul (UE) 2016/679 acces la înregistrările lor menționate la articolele 10, 16, 24 și 36 din prezentul regulament, la motivele menționate la articolul 22 alineatul (2) din prezentul regulament și le permit în orice moment accesul în toate localurile proprii utilizate pentru asigurarea interoperabilității.

Articolul 52

Auditurile efectuate de Autoritatea Europeană pentru Protecția Datelor

Autoritatea Europeană pentru Protecția Datelor garantează că cel puțin o dată la patru ani se realizează un audit al operațiunilor 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 internaționale de audit relevante. Un raport al acestui audit se trimite Parlamentului European, Consiliului, eu-LISA, Comisiei, statelor membre și agenției Uniunii în cauză. eu-LISA, unității centrale ETIAS și Europol li se oferă posibilitatea de a face observații înainte de adoptarea rapoartelor.

eu-LISA, unitatea centrală a ETIAS și Europol pun la dispoziția Autorității Europene pentru Protecția Datelor informațiile solicitate de aceasta, oferă Autorității Europene pentru Protecția Datelor acces la toate documentele solicitate de aceasta și la înregistrările lor menționate la articolele 10, 16, 24 și 36, precum și la toate localurile proprii, în orice moment.

Articolul 53

Cooperarea dintre autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor

(1) Autoritățile de supraveghere și Autoritatea Europeană pentru Protecția Datelor, fiecare acționând în limitele competențelor sale, cooperează activ în cadrul responsabilităților lor și asigură o supraveghere coordonată a utilizării componentelor de interoperabilitate și aplicarea celorlalte dispoziții ale prezentului regulament, în special dacă Autoritatea Europeană pentru Protecția Datelor sau o autoritate de supraveghere identifică discrepanțe majore între practicile statelor membre sau transferuri potențial ilegale efectuate prin canalele de comunicare ale componentelor de interoperabilitate.

(2) În cazurile menționate 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 protecția datelor transmite Parlamentului European, Consiliului, Comisiei, Europol, Agenției Europene pentru Poliția de Frontieră și Garda de Coastă și eu-LISA un raport comun privind activitățile 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

Responsabilități

Articolul 54

Responsabilitățile 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 funcționalitățile prevăzute în prezentul regulament, în conformitate cu condițiile de securitate, disponibilitate, calitate și performanță prevăzute la articolul 55 alineatul (1).

(3) eu-LISA este responsabilă de dezvoltarea componentelor de interoperabilitate, de orice adaptare necesară pentru asigurarea interoperabilității 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 comunicații, precum și specificațiile tehnice și evoluția acestora în ceea ce privește infrastructura centrală și infrastructura de comunicații securizată, care sunt adoptate de către Consiliul de administrație, 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 interoperabilității 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 specificațiilor tehnice, efectuarea de teste și gestionarea și coordonarea generală a proiectului.

(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.

Articolul 55

Responsabilitățile eu-LISA după punerea în funcțiune

(1) După punerea în funcțiune a fiecărei componente de interoperabilitate, eu-LISA este responsabilă de gestionarea tehnică a infrastructurii centrale a componentelor de interoperabilitate, inclusiv de întreținerea acestora și de evoluțiile 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 comunicații menționate la articolele 6, 12, 17, 25 și 39.

Gestionarea tehnică a componentelor de interoperabilitate cuprinde toate sarcinile și soluțiile tehnice necesare pentru a menține în funcțiune componentele de interoperabilitate și asigurând servicii neîntrerupte statelor membre și agențiilor Uniunii 24 de ore pe zi, 7 zile pe săptămână, în conformitate cu prezentul regulament. Gestionarea tehnică trebuie să includă lucrările de întreținere și dezvoltările tehnice necesare pentru a se asigura funcționarea 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 specificațiile 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 operaționale ale autorităților statelor membre și ale agențiilor Uniunii.

(2) Fără a aduce atingere articolului 17 din Statutul funcționarilor Uniunii Europene, eu-LISA aplică norme corespunzătoare privind secretul profesional sau alte obligații echivalente de confidențialitate membrilor personalului său care lucrează cu date stocate în componentele de interoperabilitate. Această obligație se aplică și după ce persoanele respective au încetat să mai ocupe o anumită funcție 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 întreține un mecanism și proceduri de verificare a calității 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

Responsabilitățile 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 naționale existente cu ESP, CIR și MID.

(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:

1. Articolul 12 se înlocuiește cu următorul text:

„*Articolul 12*

Calitatea datelor

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

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

(*) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații 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 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. 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 funcționarea 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 aplicației de referință a ECRIS în temeiul articolului 36 alineatul (8) din Regulamentul (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, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Convenției 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, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești 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 dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor (ECRIS-TCN), destinat să completeze sistemul european de informații 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 observații formale referitoare la rapoartele Autorității Europene pentru Protecția 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 autorităților 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 naționale 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 autorităților competente în temeiul articolului 65 alineatul (2) din Regulamentul (UE) 2017/2226, lista autorităților competente în temeiul articolului 87 alineatul (2) din Regulamentul (UE) 2018/1240, lista autorităților 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:

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

„(da) Grupul consultativ privind interoperabilitatea;”;

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

„(3) Europol, Eurojust și Agenția Europeană pentru Poliția 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.

Agenția Europeană pentru Poliția 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 Agenția Europeană pentru Poliția 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 identități 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 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 4 se modifică după cum urmează:

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

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

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

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

(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 menționate 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 identităților 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 legalității căutării, al monitorizării legalității prelucrării datelor, al automonitorizării și al asigurării integrității și securității datelor.";

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

„(f) verificarea identităților 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 menționate 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 menționat la articolul 39 din Regulamentul (UE) 2019/818.

eu-LISA permite Comisiei și organismelor menționate la alineatul (6) din prezentul articol să obțină rapoarte și statistici personalizate. La cerere, eu-LISA acordă acces statelor membre, Comisiei, Europol și Agenției Europene pentru Poliția 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) condițiile în care ECRIS-TCN contribuie la facilitarea și acordarea de asistență în vederea identificării corecte a persoanelor înregistrate în ECRIS-TCN în condițiile și în 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:

„(1) Pentru fiecare resortisant al unei țări terțe 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 conține datele menționate la alineatul (1) litera (b) și următoarele date de la alineatul (1) litera (a): numele (de familie), prenumele, data nașterii, locul nașterii (localitatea și țara), cetățenia sau cetățeniile, genul, numele anterioare, dacă este cazul, pseudonimele sau numele de împrumut, dacă sunt disponibile, tipul și numărul documentelor de călătorie ale persoanei și denumirea autorității emitente, dacă sunt disponibile. CIR poate conține și datele menționate 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 menționate 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 dețin informații privind cazierele judiciare ale resortisanților țărilor terțe. 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) 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 autorităților naționale din fiecare stat membru și personalului autorizat în mod corespunzător din cadrul agențiilor Uniunii cu competențe 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 menționate și este proporțional 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 menționate la alineatul respectiv în registrul central de raportare și statistici menționat 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 pronunțate înainte de data începerii introducerii datelor în conformitate cu articolul 35 alineatul (1), autoritățile 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 menționate 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 funcțiune în conformitate cu articolul 35 alineatul (4)."

CAPITOLUL IX

Dispoziții finale

Articolul 62

Întocmirea de rapoarte și de statistici

(1) Personalul autorizat în mod corespunzător din cadrul autorităților 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 autorităților 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) 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 autorităților 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 funcție de tip, și sistemele de informații ale UE care conțin 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 Agenției Europene pentru Poliția de Frontieră și Garda de Coastă are acces pentru a consulta datele menționate la alineatele (1), (2) și (3) din prezentul articol în scopul de a efectua analize de risc și evaluări ale vulnerabilității, astfel cum se menționează la articolele 11 și 13 din Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului ([38]).

(5) Personalul autorizat în mod corespunzător al Europol are acces pentru a consulta datele menționate la alineatele (2) și (3) din prezentul articol în scopul de a efectua analize strategice, tematice și operaționale, astfel cum se menționează 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 menționate la alineatele respective în CRRS. Datele incluse în CRRS trebuie să nu permită identificarea persoanelor fizice, dar permit autorităților enumerate la alineatele (1), (2) și (3) să obțină rapoarte și statistici adaptabile pentru a spori eficiența verificărilor la frontieră, a sprijini autoritățile să prelucreze cererile de viză și a sprijini elaborarea de politici bazate pe date concrete în materie de migrație și de securitate în Uniune.

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

([38]) 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).

Articolul 63

Perioada de tranziție pentru utilizarea portalului european de căutare

(1) Pentru o perioadă de doi ani de la data punerii în funcțiune a ESP, obligațiile menționate la articolul 7 alineatele (2) și (4) nu se aplică, iar utilizarea ESP este opțională.

(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 menționate 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 funcțiune a ESP asupra organizării și duratei verificărilor la frontiere.

Articolul 64

Perioada de tranziție aplicabilă dispozițiilor privind accesul la registrul comun de date de identitate în scopul prevenirii, depistării sau anchetării infracțiunilor de terorism sau a altor infracțiuni grave

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

Articolul 65

Perioada de tranziție aplicabilă detectorului de identități multiple

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

(2) În cazul în care, în urma interogărilor, se obțin una sau mai multe concordanțe 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 obțin una sau mai multe concordanțe 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 obțin mai multe concordanțe, se stabilește o conexiune între fiecare componentă a datelor care a generat corespondența.

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

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

(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.

(5) Costurile aferente autorităților desemnate sunt suportate în mod corespunzător de către fiecare stat membru de desemnare. Costurile aferente conectării fiecărei autorități 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 autoritățile menționate la articolele 7, 20, 21 și 26 care pot utiliza sau avea acces la ESP, CIR și, respectiv, MID.

O listă consolidată a acestor autorități se publică în *Jurnalul Oficial al Uniunii Europene* în termen de trei luni de la data punerii în funcțiune 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 menționate 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 tranziție prevăzute la articolul 65.

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

Articolul 68

Punerea în funcțiune

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

(a) au fost adoptate măsurile menționate 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 autoritățile statelor membre și cu agențiile Uniunii care pot folosi ESP;

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

ESP efectuează interogări în bazele de date ale Interpol numai odată ce condițiile 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 funcțiune a ESP.

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.

(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;

(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 menționate la alineatul (1) litera (b), alineatul (2) litera (b), alineatul (3) litera (b) și alineatul (4) 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.

(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 calității datelor, indicatorii comuni de calitate a datelor și standardele minime de calitate a datelor, odată ce sunt îndeplinite următoarele condiții:

(a) au fost adoptate măsurile menționate 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 calității datelor, a indicatorilor comuni de calitate a datelor și a standardelor minime de calitate a datelor, pe care a efectuat-o în cooperare cu autoritățile statelor membre.

Comisia stabilește data menționată 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 funcționeze CRRS, odată ce sunt îndeplinite următoarele condiții:

(a) au fost adoptate măsurile menționate 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 autoritățile statelor membre;

(c) eu-LISA a validat modalitățile tehnice și juridice de colectare și transmitere a datelor menționate la articolul 39 și a notificat aceste modalități Comisiei.

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.

(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 competențe

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

(2) Competența de a adopta acte delegate menționată 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 competențe cu cel puțin nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de timp identice, cu excepția cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puțin trei luni înainte de încheierea fiecărei perioade.

(3) Delegarea de competențe menționată 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 competențe 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 menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional 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 obiecții 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 obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 70

Procedura comitetului

(1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul 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 atribuții legate de furnizarea de cursuri de formare privind utilizarea tehnică a componentelor de interoperabilitate în conformitate cu Regulamentul (UE) 2018/1726.

Autoritățile statelor membre și agențiile Uniunii îi oferă personalului lor autorizat să prelucreze date utilizând componentele de interoperabilitate programe adecvate de formare legate de securitatea datelor, calitatea datelor, normele de protecție a datelor, procedurile aplicabile prelucrării datelor și obligațiile 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 autorităților statelor membre și cel al agențiilor Uniunii care sunt autorizate să prelucreze date utilizând componentele de interoperabilitate. Se acordă o atenție deosebită procesului de detectare a identităților multiple, inclusiv verificării manuale a identităților diferite și nevoii aferente de a oferi garanții adecvate de protecție a drepturilor fundamentale.

Articolul 73

Manual practic

Comisia, în strânsă cooperare cu statele membre, cu eu-LISA și cu alte agenții relevante ale Uniunii, pune la dispoziție un manual practic pentru implementarea și gestionarea componentelor de interoperabilitate. Manualul practic furnizează orientări, recomandări și bune practici de natură tehnică și operațională. 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 interfața uniformă națională din perspectiva obiectivelor legate de planificare și costuri și pentru a monitoriza funcționarea 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 situația dezvoltării componentelor de interoperabilitate și legătura lor cu interfața uniformă națională. 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 funcțiune 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 funcționarea 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) o examinare a rezultatelor obținute 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 funcționării portalului web, inclusiv cifre privind utilizarea portalului web și numărul de cereri soluționate;

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

(e) o evaluare a securității componentelor de interoperabilitate;

(f) o evaluare a utilizării CIR pentru identificare;

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

(h) o evaluare a eventualelor implicații, inclusiv a impactului disproporționat asupra fluidității traficului la punctele de trecere a frontierelor și a implicațiilor cu un impact bugetar asupra bugetului general al Uniunii;

(i) o evaluare a căutării în bazele de date ale Interpolului prin intermediul ESP, inclusiv informații privind numărul de concordanțe în bazele de date ale Interpolului și informații 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, Autorității Europene pentru Protecția Datelor și Agenției 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 menționate la articolul 68, Comisia prezintă Parlamentului European și Consiliului un raport privind situația pregătirilor pentru a pune pe deplin în aplicare prezentul regulament. Raportul conține și informații detaliate cu privire la costurile aferente și la orice risc care poate afecta costurile totale.

(6) La doi ani de la punerea în funcțiune 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 menționată la alineatul (4) litera (b) din prezentul articol.

(7) Statele membre și Europolul furnizează eu-LISA și Comisiei informațiile necesare pentru redactarea rapoartelor menționate la alineatele (3)-(6). Aceste informații nu afectează metodele de lucru și nici nu includ date care dezvăluie sursele, membrii personalului sau investigațiile autorităților desemnate.

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

(9) Respectând dispozițiile dreptului intern referitoare la publicarea informațiilor sensibile și fără a aduce atingere limitărilor necesare pentru protejarea securității și a ordinii publice, prevenirea infracțiunilor și a garanta că nicio anchetă națională 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 infracțiunilor de terorism sau a altor infracțiuni grave care conțin informații și statistici privind:

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

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

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

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

(e) necesitatea și utilizarea excepției justificate de urgență, precum și cazurile în care urgența 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 dispoziție o soluție tehnică pentru a gestiona cererile de acces ale utilizatorilor menționate la articolul 22 și a facilita colectarea informațiilor în temeiul alineatelor (7) și (9) din prezentul articol, în scopul generării rapoartelor și statisticilor menționate la alineatele respective. Comisia adoptă acte de punere în aplicare pentru a stabili specificațiile soluției tehnice. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată 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*.

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

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

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

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

Dispozițiile prezentului regulament referitoare la mecanismele și procedurile automatizate de control al calității 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).

Dispozițiile 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 privința 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.

Adoptat la Bruxelles, 20 mai 2019.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*
A. TAJANI	G. CIAMBA

ISSN 1977-0782 (ediție electronică)
ISSN 1830-3625 (ediție tipărită)

Oficiul pentru Publicații al Uniunii Europene
2985 Luxemburg
LUXEMBURG

RO