

# Az Európai Unió Hivatalos Lapja

# L 135



Magyar nyelvű kiadás

## Jogszabályok

62. évfolyam

2019. május 22.

Tartalom

### I Jogalkotási aktusok

#### RENDELETEK

- ★ Az Európai Parlament és a Tanács (EU) 2019/816 rendelete (2019. április 17.) az Európai Bűnügyi Nyilvántartási Információs Rendszer kiegészítése érdekében a harmadik országbeli állampolgárokkal és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval rendelkező tagállamok azonosítására szolgáló központosított rendszer (ECRIS-TCN) létrehozásáról, valamint az (EU) 2018/1726 rendelet módosításáról ..... 1
- ★ Az Európai Parlament és a Tanács (EU) 2019/817 rendelete (2019. május 20.) az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízumügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról ..... 27
- ★ Az Európai Parlament és a Tanács (EU) 2019/818 rendelete (2019. május 20.) az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a rendőrségi és igazságügyi együttműködés, a menekültügy és a migráció területén, valamint az (EU) 2018/1726, az (EU) 2018/1862 és az (EU) 2019/816 rendelet módosításáról ..... 85

# HU

Azok a jogi aktusok, amelyek címe normál szedéssel jelenik meg, a mezőgazdasági ügyek napi intézésére vonatkoznak, és rendszerint csak korlátozott ideig maradnak hatályban.

Valamennyi más jogszabály címét vastagon szedik, és előtte csillag szerepel.



## I

(Jogalkotási aktusok)

## RENDELETEK

## AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/816 RENDELETE

(2019. április 17.)

**az Európai Bűnügyi Nyilvántartási Információs Rendszer kiegészítése érdekében a harmadik országbeli állampolgárokkal és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval rendelkező tagállamok azonosítására szolgáló központosított rendszer (ECRIS-TCN) létrehozásáról, valamint az (EU) 2018/1726 rendelet módosításáról**

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 82. cikke (1) bekezdése második albekezdésének d) pontjára,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

rendes jogalkotási eljárás keretében <sup>(1)</sup>,

mivel:

- (1) Az Unió célul tűzte ki maga elé, hogy egy belső határok nélküli, a szabadságon, a biztonságon és a jog érvényesülésén alapuló olyan térséget kínáljon polgárai számára, amelyben biztosított a személyek szabad mozgása. Ezt a célt többek között a bűnmegelőzésre és a bűnüldözésre irányuló – köztük a szervezett bűnözés és a terrorizmus elleni – megfelelő intézkedések révén kell megvalósítani.
- (2) E cél szükségessé teszi, hogy a tagállamokban hozott ítéletekre vonatkozó információkat az ítélethozatal szerinti tagállamon kívül is figyelembe vegyék – a 2008/675/IB tanácsi kerethatározatban <sup>(2)</sup> megállapítottaknak megfelelően – az új büntetőeljárások során, valamint új bűncselekmények elkövetésének megelőzése érdekében.
- (3) Ez a cél előfeltételezi a bűnügyi nyilvántartásokból származó információk cseréjét a tagállamok illetékes hatóságai között. Ezen információcsere megszervezésére és elősegítésére a 2009/315/IB tanácsi kerethatározatban <sup>(3)</sup> meghatározott szabályok, valamint a 2009/316/IB tanácsi határozattal <sup>(4)</sup> létrehozott Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS) révén kerül sor.
- (4) Az ECRIS hatályos jogi kerete azonban nem veszi kellőképpen figyelembe a harmadik országbeli állampolgárokkal kapcsolatos megkeresések sajátosságait. Jóllehet az ECRIS-en keresztül már jelenleg is lehetőség van a harmadik országbeli állampolgárokra vonatkozó információcserére, ennek hatékony, gyors és pontos kivitelezésére nem áll rendelkezésre közös uniós eljárás vagy mechanizmus.
- (5) Az Unión belül a harmadik országbeli állampolgárokra vonatkozó információkat nem gyűjtik össze, mint a tagállami állampolgárok esetében az állampolgárság szerinti tagállamokban, hanem azokat csak azokban a tagállamokban tárolják, ahol az ítéletet meghozták. Ezért kizárólag akkor nyerhető teljeskörű áttekintés egy harmadik országbeli állampolgár bűnügyi előéletéről, ha minden tagállamhoz ilyen információk iránti megkeresést intéznek.

<sup>(1)</sup> Az Európai Parlament 2019. március 12-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2019. április 9-i határozata.

<sup>(2)</sup> A Tanács 2008/675/IB kerethatározata (2008. július 24.) az Európai Unió más tagállamaiban hozott ítéleteknek egy új büntetőeljárásban való figyelembevételéről (HL L 220., 2008.8.15., 32. o.).

<sup>(3)</sup> A Tanács 2009/315/IB kerethatározata (2009. február 26.) a bűnügyi nyilvántartásból származó információk tagállamok közötti cseréjének megszervezéséről és azok tartalmáról (HL L 93., 2009.4.7., 23. o.).

<sup>(4)</sup> A Tanács 2009/316/IB határozata (2009. április 6.) a 2009/315/IB kerethatározat 11. cikke alkalmazásában az Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS) létrehozásáról (HL L 93., 2009.4.7., 33. o.).

- (6) Az ilyen általános megkeresések aránytalan adminisztratív terhet rónak minden tagállamra, beleértve azokat is, amelyek nem rendelkeznek információval az adott harmadik országbeli állampolgárról. Ez a teher a gyakorlatban visszatartja a tagállamokat attól, hogy harmadik országbeli állampolgárokra vonatkozó információkat kérjenek más tagállamoktól, ami súlyosan hátráltatja közöttük az információk cseréjét, a bűnügyi nyilvántartási információkhoz való hozzáférésüket pedig a nemzeti nyilvántartásban tárolt információkra korlátozza. Ennek következményeként nő annak a kockázata, hogy a tagállamok közötti információcsere nem hatékony és nem teljeskörű, ami pedig hatással van a polgárok és az Unióban tartózkodó személyek biztonságára és védelmére.
- (7) A helyzet javítása érdekében létre kell hozni egy olyan rendszert, amelynek segítségével a tagállamok központi hatóságai gyorsan és hatékonyan kideríthetik, hogy mely más tagállamok rendelkeznek bűnügyi nyilvántartási információkkal egy adott harmadik országbeli állampolgárra vonatkozóan (a továbbiakban: az ECRIS-TCN). Ezt követően a bűnügyi nyilvántartási információk a 2009/315/IB kerethatározattal összhangban a jelenlegi ECRIS-keret felhasználásával kérhetők az adott tagállamoktól.
- (8) Ezért e rendelettel meg kell állapítani egy uniós szinten központosított, személyes adatokat tartalmazó rendszert létrehozó szabályokat, és a tagállamok, valamint a központosított rendszer kifejlesztéséért és karbantartásáért felelős szervezet közötti feladatmegosztásra vonatkozó szabályokat, valamint minden olyan különös adatvédelmi rendelkezést, amely a meglévő adatvédelmi szabályozás kiegészítéséhez, valamint az adatvédelem, az adatbiztonság és az érintett személyek alapvető jogai védelme megfelelő általános szintjének biztosításához szükséges.
- (9) Az a cél, amely szerint az uniós polgárok számára egy belső határok nélküli, a szabadságon, a biztonságon és a jog érvényesülésén alapuló olyan térséget lehessen kialakítani, amelyben biztosított a személyek szabad mozgása, szükségessé teszi azt is, hogy teljeskörű információk álljanak rendelkezésre az olyan uniós polgárokkal szemben hozott ítéletekre vonatkozóan, akik valamely harmadik ország állampolgárságával is rendelkeznek. Tekintettel arra, hogy ezek a személyek egy vagy több állampolgársággal rendelkezőként mutakozhatnak be, valamint arra, hogy különböző ítéleteket tárolhatnak az ítélethozatal szerinti tagállamban és az állampolgárság szerinti tagállamban, e rendelet hatálya alá kell vonni azokat az olyan uniós polgárokat, akik valamely harmadik ország állampolgárságával is rendelkeznek. Ezeknek a személyeknek e rendelet hatálya alóli kizárása azt eredményezné, hogy az ECRIS-TCN-ben tárolt információk nem lennének teljeskörűek. Ez veszélyeztetné a rendszer megbízhatóságát. Mivel azonban ezek a személyek uniós polgársággal rendelkeznek, azoknak a feltételeknek, amelyek mellett ezekre a személyekre vonatkozóan ujjnyomatadatokat lehet bevinni az ECRIS-TCN-be, hasonlóan kell lenniük azokhoz a feltételekhez, amelyek mellett a tagállamok az uniós polgárokra vonatkozóan ujjnyomatadatokat cserélnék egymással a 2009/315/IB kerethatározattal és a 2009/316/IB határozattal létrehozott ECRIS-en keresztül. Ezért az olyan uniós polgárok ujjnyomatadatait, akik valamely harmadik ország állampolgárságával is rendelkeznek, csak akkor lehet bevinni az ECRIS-TCN-be, ha azokat a nemzeti joggal összhangban büntetőeljárások során gyűjtötték be, ugyanakkor a tagállamok számára nyitva kell állnia a lehetőségnek, hogy a büntetőeljárástól eltérő célokból begyűjtött ujjnyomatadatokat is felhasználhassanak, amennyiben e felhasználást a nemzeti jog megengedi.
- (10) Az ECRIS-TCN-nek lehetővé kell tennie ujjnyomatadatokat kezelését harmadik országbeli állampolgárra vonatkozóan bűnügyi nyilvántartási információval rendelkező tagállamok azonosítása céljából. Továbbá lehetővé kell tennie az arcképmások kezelését a személyazonosság megerősítése érdekében. Alapvető fontosságú, hogy az ujjnyomatadatokat és az arcképmások feltöltése és felhasználása során ne lépjék túl a cél eléréséhez feltétlenül szükséges mértéket, tiszteletben tartsák az alapvető jogokat és a gyermekek mindenek felett álló érdekét, valamint megfeleljenek az alkalmazandó uniós adatvédelmi szabályoknak.
- (11) Az ECRIS-TCN kifejlesztésének és üzemeltetésének feladatával az (EU) 2018/1726 európai parlamenti és tanácsi rendelettel <sup>(5)</sup> létrehozott, a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai uniós ügynökséget (eu-LISA) kell megbízni, tekintettel annak a bel- és igazságügy területén működő más nagyméretű rendszerek igazgatásával kapcsolatos tapasztalataira. Az eu-LISA megbízatását módosítani kell, hogy az tükrözze az említett új feladatokat.
- (12) Az eu-LISA számára megfelelő finanszírozást és személyzetet kell biztosítani az e rendeletben előírt feladatai ellátásához.
- (13) mivel szoros műszaki kapcsolatokat kell létesíteni az ECRIS-TCN és az ECRIS között, az eu-LISA-t meg kell megbízni az ECRIS referenciaalkalmazás továbbfejlesztésének és karbantartásának feladatával is, és ennek megjelenítése érdekében módosítani kell az eu-LISA megbízatását.
- (14) Négy tagállam fejlesztett ki saját nemzeti ECRIS alkalmazási szoftvert a 2009/316/IB határozattal összhangban, és a tagállamok az ECRIS referenciaalkalmazás helyett ezt használják a bűnügyi nyilvántartási információk cseréjére. Tekintettel az érintett tagállamok rendszereinek nemzeti használatra bevezetett sajátosságaira, illetve az e tagállamok által eszközölt beruházásokra, lehetővé kell tenni számukra, hogy az e rendeletben foglalt feltételeknek való megfelelés mellett az ECRIS-TCN céljaira is használhassák nemzeti ECRIS alkalmazási szoftverüket.

<sup>(5)</sup> Az Európai Parlament és a Tanács (EU) 2018/1726 rendelete (2018. november 14.) a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai uniós ügynökségről (eu-LISA), az 1987/2006/EK rendelet és a 2007/533/IB tanácsi határozat módosításáról, valamint az 1077/2011/EU rendelet hatályon kívül helyezéséről (HL L 295., 2018.11.21., 99. o.).

- (15) Az ECRIS-TCN kizárólag az Unióban működő büntetőbíróóságok által elítélt harmadik országbeli állampolgárokra vonatkozó személyazonosító adatokat tartalmazhatja. E személyazonosító adatoknak alfanumerikus és ujnyomatadatokat kell magukban foglalniuk. Lehetővé kell tenni azt is, hogy arcképmásokat foglaljanak magukban, ha az ítéletet hozó tagállam joga megengedi az elítélt személyek arcképmásainak gyűjtését és tárolását.
- (16) A tagállamok által a központi rendszerbe feltöltendő alfanumerikus adatok között szerepelnie kell az elítélt személy vezetéknevének (családi nevének) és utóneveinek (keresztneveinek), valamint álneveinek vagy felvett neveinek, amennyiben ez az információ a központi hatóság rendelkezésére áll. Ha eltérő személyes adat – például a név írásmódjának egy másik ábécé szerinti eltérő változata – is ismert az adott tagállam számára, akkor lehetővé kell tenni annak a központi rendszerbe kiegészítő információként való feltöltését.
- (17) Az alfanumerikus adatoknak kiegészítő információként tartalmazniuk kell a személy személyazonosító számát, illetve személyazonosító okmányainak típusát és számát, valamint az ezen okmányokat kiállító hatóság nevét is, amennyiben ez az információ a központi hatóság rendelkezésére áll. A tagállamnak törekednie kell arra, hogy a vonatkozó információk a központi rendszerbe való feltöltése előtt ellenőrizze a személyazonosító okmányok hitelességét. Mivel ezek az adatok megbízhatatlanok lehetnek, felhasználásuk során körültekintően kell eljárni.
- (18) A központi hatóságoknak az ECRIS-TCN-t kell használniuk a harmadik országbeli állampolgárokra vonatkozó bűnügyi nyilvántartási információval rendelkező tagállamok azonosítására, ha az érintett tagállamban az adott személyre vonatkozóan bűnügyi nyilvántartási információkat kérnek az e személlyel szembeni büntetőeljárás céljából vagy az e rendeletben említett célokból. Bár főszabály szerint minden ilyen esetben az ECRIS-TCN-t kell használni, a büntetőeljárás lefolytatásáért felelős hatóság dönthet úgy is, hogy ha az ügy körülményei miatt nem lenne helyénvaló, akkor az ECRIS-TCN-t ne használják, így például sürgősen lefolytatandó büntetőeljárás bizonyos típusai esetén, tranzit esetén, ha a bűnügyi nyilvántartási információkat nemrégiben beszerezték az ECRIS-en keresztül, illetve kisebb súlyú jogsértések, különösen kisebb súlyú közlekedési jogsértések, az általános önkormányzati rendeletekkel kapcsolatos kisebb súlyú jogsértések és a közrend elleni kisebb súlyú jogsértések esetén.
- (19) A tagállamok számára az e rendeletben foglaltaktól eltérő célokra is lehetővé kell tenni az ECRIS-TCN használatát, amennyiben a nemzeti jog így rendelkezik, és azzal összhangban. Annak érdekében azonban, hogy minél átláthatóbb legyen az ECRIS-TCN használata, a tagállamoknak az említett egyéb célokról értesíteniük kell a Bizottságot, amelynek pedig gondoskodnia kell az összes értesítésnek az *Európai Unió Hivatalos Lapjában* való közzétételéről.
- (20) A bűnügyi nyilvántartási információkat kérő egyéb hatóságok számára azt is lehetővé kell tenni, hogy úgy dönthessenek, hogy ha az ügy körülményei miatt nem lenne helyénvaló, akkor az ECRIS-TCN-t ne használják, például, ha egy személy szakmai képzéseire vonatkozóan bizonyos standard adminisztratív ellenőrzéseket kell elvégezni, különösen ha ismert, hogy az ECRIS-TCN-ben végzett lekérdezés eredményétől függetlenül más tagállamoktól nem fognak bűnügyi nyilvántartási információkat kérni. Azonban az ECRIS-TCN-t mindig használni kell olyankor, ha a bűnügyi nyilvántartási információk iránti kérelmet olyan személy kezdeményezte, aki a 2009/315/IB kerethatározattal összhangban a bűnügyi nyilvántartásban rá vonatkozó adatokról kér információt, vagy ha az információk iránti megkeresésre a 2011/93/EU európai parlamenti és tanácsi irányelvvel <sup>(6)</sup> összhangban bűnügyi nyilvántartási információk megszerzése céljából kerül sor.
- (21) A harmadik országbeli állampolgárok számára biztosítani kell a jogot, hogy a bűnügyi nyilvántartásokban rájuk vonatkozó adatokról írásbeli tájékoztatást kapjanak azon tagállam jogával összhangban, amelyben az információt kérik, valamint a 2009/315/IB kerethatározattal összhangban. Az ilyen információ harmadik országbeli állampolgárnak való átadását megelőzően az érintett tagállamnak le kell kérdeznie az ECRIS-TCN-t.
- (22) A valamely harmadik ország állampolgárságával is rendelkező uniós polgárok csak akkor fognak szerepelni az ECRIS-TCN-ben, ha az illetékes hatóságok tudnak arról, hogy ezek a személyek valamely harmadik országnak az állampolgárságával rendelkeznek. Attól, hogy az illetékes hatóságok nem tudnak arról, hogy uniós polgárok valamely harmadik ország állampolgárságával is rendelkeznek, még előfordulhat, hogy ezeket a személyeket korábban harmadik országbeli állampolgárként elítélték. Annak biztosítása érdekében, hogy az illetékes hatóságoknak teljeskörű áttekintése legyen a bűnügyi nyilvántartási információkról, lehetővé kell tenni az ECRIS-TCN lekérdezését annak ellenőrzésére, hogy van-e olyan tagállam, amely az adott uniós polgárra mint harmadik országbeli állampolgárra vonatkozóan bűnügyi nyilvántartási információval rendelkezik.
- (23) Abban az esetben, ha egyezés van a központi rendszerben rögzített adatok és a tagállam által a lekérdezéshez használt adatok között (a továbbiakban: a találat), a találattal együtt a találat tekintetében rögzített adatokat is megadják. A lekérdezés eredményét a központi hatóságok csak az ECRIS-en keresztüli megkeresések céljára,

<sup>(6)</sup> Az Európai Parlament és a Tanács 2011/93/EU irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról (HL L 335., 2011.12.17., 1. o.).

illetve az (EU) 2018/1727 európai parlamenti és tanácsi rendelettel <sup>(7)</sup> létrehozott Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége (a továbbiakban: az Eurojust), az (EU) 2016/794 európai parlamenti és tanácsi rendelettel <sup>(8)</sup> létrehozott Bűnüldözési Együttműködés Európai Unió Ügynöksége (a továbbiakban: az Europol) és az (EU) 2017/1939 tanácsi rendelettel <sup>(9)</sup> létrehozott Európai Ügyészség csak az e rendeletben említett, ítéletekkel kapcsolatos információk iránti megkeresések céljára használhatják.

- (24) Az ECRIS-TCN-ben rögzített arcképmások kezdetben kizárólag a harmadik országbeli állampolgárok személyazonosságának megerősítése céljából használhatók fel, annak azonosítása érdekében, hogy mely tagállamok rendelkeznek az adott harmadik országbeli állampolgárral szemben hozott korábbi ítéletekre vonatkozó információval. A jövőben az arcképmások felhasználhatók kell, hogy legyenek automatizált biometrikus megfeleltetés céljára is, feltéve, hogy teljesülnek az erre vonatkozó műszaki és szakpolitikai követelmények. A Bizottságnak – a szükségesség és az arányosság, valamint az arcfelismerő szoftverek terén végbemenő műszaki fejlődés figyelembevételével – értékelnie kell a szükséges technológia rendelkezésre állását és alkalmazhatóságát, mielőtt elfogadná az arcképmások harmadik országbeli állampolgárok azonosítása céljából történő felhasználására vonatkozó felhatalmazáson alapuló jogi aktust annak azonosítása érdekében, hogy mely tagállamok rendelkeznek az adott személyekkel szemben hozott korábbi ítéletekre vonatkozó információval.
- (25) A biometrikus azonosításra szükség van, mivel ez a legmegbízhatóbb módszer a tagállamok területén tartózkodó, gyakran sem okmányokkal, sem más személyazonosító eszközökkel nem rendelkező harmadik országbeli állampolgárok személyazonosságának megállapítására, valamint a harmadik országbeli állampolgárok adatainak megbízhatóbb megfeleltetése céljából.
- (26) A tagállamoknak fel kell tölteniük a központi rendszerbe az elítélt harmadik országbeli állampolgároknak a büntetőeljárás során a nemzeti joggal összhangban begyűjtött ujjnyomatadatait. Annak érdekében, hogy a központi rendszerben a személyazonosító adatok lehető legteljesebb köre álljon rendelkezésre, lehetővé kell tenni, hogy a tagállamok olyan ujjnyomatadatokat is feltölthessenek a központi rendszerbe, amelyeket a büntetőeljárás céljaitól eltérő célokból gyűjtöttek be, feltéve, hogy ezen ujjnyomatadatok a büntetőeljárás során a nemzeti joggal összhangban felhasználhatók.
- (27) Ennek a rendeletnek a tagállamok által a központi rendszerbe feltöltendő ujjnyomatadatok tekintetében minimumkövetelményeket kell megállapítania. A tagállamok választására kell bízni, hogy azon harmadik országbeli állampolgárok ujjnyomatadatait töltsék fel, akikkel szemben legalább 6 hónap szabadságvesztés büntetést szabtak ki, vagy azon harmadik országbeli állampolgárok ujjnyomatadatait, akiket olyan bűncselekmény miatt ítélték el, amely esetében az érintett tagállam joga alapján a büntetési tétel felső határa legalább 12 hónap szabadságvesztés.
- (28) A tagállamoknak az elítélt harmadik országbeli állampolgárokra vonatkozóan adatrekordokat kell létrehozniuk az ECRIS-TCN-ben. Ezt lehetőség szerint automatikusan és indokolatlan késedelem nélkül kell elvégezni, azt követően, hogy az elítélés tényét feltöltötték a nemzeti bűnügyi nyilvántartásokba. A tagállamoknak az ECRIS-TCN-be történő adatfeltöltés kezdő időpontját követően hozott ítéletek vonatkozásában – e rendelettel összhangban – alfanumerikus adatokat és ujjnyomatadatokat kell feltölteniük a központi rendszerbe. A tagállamok számára lehetőséget kell biztosítani arra, hogy ugyanezen időponttól kezdve, és azt követően bármikor arcképmásokat töltsenek fel a központi rendszerbe.
- (29) A rendszer maximális hatékonyságának biztosítása érdekében a tagállamoknak – e rendelettel összhangban – az ECRIS-TCN-ben adatrekordokat kell létrehozniuk az adatfeltöltés kezdő időpontja előtt elítélt harmadik országbeli állampolgárokra vonatkozóan is. A tagállamok azonban nem kötelezhetők arra, hogy ebből a célból olyan információkat gyűjtsenek, amelyek az adatfeltöltés kezdő időpontja előtt még nem szerepeltek a bűnügyi nyilvántartásaikban. Harmadik országbeli állampolgárok ilyen korábbi ítéletek kapcsán begyűjtött ujjnyomatadatait kizárólag abban az esetben kell bevinni, ha azok büntetőeljárás során kerültek begyűjtésre, és ha az érintett tagállam azt állapítja meg, hogy azok egyértelműen megfeleltethetők a bűnügyi nyilvántartásokban szereplő más személyazonosító adatoknak.
- (30) Az ítéletekre vonatkozó információcseré javításának segítenie kell a tagállamokat a 2008/675/IB kerethatározat végrehajtásában, amely arra kötelezi a tagállamokat, hogy az új büntetőeljárások során figyelembe vegyék a más tagállamokban hozott korábbi ítéleteket annyiban, amennyiben a korábbi nemzeti ítéleteket a nemzeti jognak megfelelően figyelembe veszik.

<sup>(7)</sup> Az Európai Parlament és a Tanács (EU) 2018/1727 rendelete (2018. november 14.) az Európai Unió Büntető Igazságügyi Együttműködési Ügynökségéről (Eurojust) és a 2002/187/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről (HL L 295., 2018.11.21., 138. o.).

<sup>(8)</sup> Az Európai Parlament és a Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Unió Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről (HL L 135., 2016.5.24., 53. o.).

<sup>(9)</sup> A Tanács (EU) 2017/1939 rendelete (2017. október 12.) az Európai Ügyészség létrehozására vonatkozó megerősített együttműködés bevezetéséről (HL L 283., 2017.10.31., 1. o.).

- (31) Az ECRIS-TCN által jelzett találat önmagában nem jelenti azt, hogy a harmadik országbeli állampolgárt elítélték a jelzett tagállamokban. A korábbi ítélet megléte kizárólag az érintett tagállamok bünyügyi nyilvántartásaiból kapott információ alapján erősíthető meg.
- (32) Nem érintve az uniós pénzügyi programok alkalmazandó szabályokkal összhangban való felhasználásának lehetőségét, minden tagállamnak viselnie kell a bünyügyi nyilvántartási adatbázisa és nemzeti ujjnyomat-adatbázisai – ideértve azok nemzeti központi hozzáférési ponthoz való kapcsolatait is – megvalósításával, kezelésével, használatával és karbantartásával, valamint az ECRIS-TCN használatának lehetővé tételéhez szükséges technikai kiigazítások megvalósításával, kezelésével, használatával és karbantartásával kapcsolatban felmerülő saját költségeit.
- (33) Az Eurojustnak, az Europolnak és az Európai Ügyészségnek hozzá kell férnie az ECRIS-TCN-hez abból a célból, hogy jogszabályban előírt feladataik elősegítése érdekében azonosítsák a harmadik országbeli állampolgárokra vonatkozó bünyügyi nyilvántartási információval rendelkező tagállamokat. A büntetőügyekben folytatott igazságügyi együttműködés elvei – például a kölcsönös jogsegélyre vonatkozó szabályok – alkalmazásának sérelme nélkül az Eurojust számára is közvetlen hozzáférést kell biztosítani az ECRIS-TCN-hez az e rendeletben előírt azon feladatának elvégzése céljából, hogy harmadik országok és nemzetközi szervezetek kapcsolattartó-jaként járjon el. Azzal együtt, hogy figyelembe kell venni az Európai Ügyészséget létrehozó megerősített együttműködésben részt nem vevő tagállamok álláspontját, az ítéletekre vonatkozó információhoz való hozzáférés nem tagadható meg az Európai Ügyészségtől pusztaán azon az alapon, hogy az érintett tagállam nem vesz részt az említett megerősített együttműködésben.
- (34) Ez a rendelet állapítja meg az ECRIS-TCN-hez való hozzáférés szigorú szabályait és a szükséges biztosítékokat, beleértve a tagállamoknak az adatok gyűjtésével és felhasználásával kapcsolatos felelősségét. Ezen túlmenően meghatározza azt is, hogy az egyének miként gyakorolhatják a kártérítéshez, a hozzáféréshez, a helyesbítéshez, a törléshez és a jogorvoslathoz – különösen a hatékony jogorvoslathoz – való jogukat, valamint rendelkezik az adatkezelési műveletek független közjogi hatóságok általi felügyeletéről. Ezáltal tiszteletben tartja a különösen az Európai Unió Alapjogi Chartájában elismert alapvető jogokat és szabadságokat, többek között a személyes adatok védelméhez való jogot, a törvény előtti egyenlőség elvét és a hátrányos megkülönböztetés általános tilalmát. E tekintetben figyelembe veszi továbbá az emberi jogok és alapvető szabadságok védelméről szóló európai egyezményt, a Polgári és Politikai Jogok Nemzetközi Egyezségokmányát és a nemzetközi jog szerint fennálló más emberi jogi kötelezettségeket.
- (35) A személyes adatok illetékes nemzeti hatóságok általi, a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása – többek között a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése – céljából végzett kezelésére az (EU) 2016/680 európai parlamenti és tanácsi irányelv<sup>(10)</sup> kell alkalmazni. A személyes adatok nemzeti hatóságok általi kezelésére az (EU) 2016/679 európai parlamenti és tanácsi rendeletet<sup>(11)</sup> kell alkalmazni abban az esetben, ha az ilyen adatkezelés nem az (EU) 2016/680 irányelv hatálya alá tartozik. Az (EU) 2018/1725 európai parlamenti és tanácsi rendelettel<sup>(12)</sup> összhangban koordinált felügyeletet kell biztosítani, amely rendeletet a személyes adatok eu-LISA általi kezelésére is alkalmazni kell.
- (36) A korábbi ítéletek tekintetében a központi hatóságoknak az alfanumerikus adatokat az adatfeltöltésre e rendeletben megállapított időtartam végéig, az ujjnyomatadatokat pedig az ECRIS-TCN működése megkezdésének időpontjától számított két éven belül fel kell tölteniük. A tagállamoknak lehetőségük van minden adat egyszerre történő feltöltésére, feltéve, hogy betartják az említett határidőket.
- (37) Az e rendelet bármiféle megsértéséből adódó károk tekintetében meg kell határozni a tagállamok, az Eurojust, az Europol, az Európai Ügyészség és az eu-LISA felelősségére vonatkozó szabályokat.
- (38) A harmadik országbeli állampolgárokkal szemben hozott korábbi ítéletekre vonatkozó információval rendelkező tagállamok jobb azonosítása érdekében a Bizottságot fel kell hatalmazni arra, hogy az Európai Unió működéséről szóló szerződés (EUMSZ) 290. cikkének megfelelően jogi aktusokat fogadjon el e rendelet kiegészítésére vonatkozóan, amelyekben előírja az arcképmások harmadik országbeli állampolgárok azonosítása céljából történő felhasználását annak azonosítása érdekében, hogy mely tagállamok rendelkeznek a korábbi ítéletekre vonatkozó információval. Különösen fontos, hogy a Bizottság az előkészítő munkája során megfelelő konzultációkat folytasson, többek között szakértői szinten is, és hogy e konzultációkra a jogalkotás minőségének javításáról

<sup>(10)</sup> Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (HL L 119., 2016.5.4., 89. o.).

<sup>(11)</sup> Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

<sup>(12)</sup> Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o.).

szóló, 2016. április 13-i intézményközi megállapodásnak <sup>(13)</sup> megfelelően kerüljön sor. A felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg kap kézhez minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein.

- (39) Az ECRIS-TCN létrehozása és üzemeltetési igazgatása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek <sup>(14)</sup> megfelelően kell gyakorolni.
- (40) A tagállamoknak meg kell hozniuk a szükséges intézkedéseket, hogy ennek a rendeletnek a lehető leghamarabb megfeleljenek az ECRIS-TCN megfelelő működésének biztosítása érdekében, figyelembe véve az ahhoz szükséges időt, hogy az eu-LISA kifejlessze és üzembe helyezze az ECRIS-TCN-t. A tagállamok számára azonban e rendelet hatálybalépését követően legalább 36 hónapnak kell rendelkezésre állnia ahhoz, hogy meg hozzák az e rendeletnek való megfeleléshez szükséges intézkedéseket.
- (41) mivel e rendelet célját, nevezetesen a harmadik országbeli állampolgárokra vonatkozó pontos bűnügyi nyilvántartási információk gyors és hatékony cseréjének lehetővé tételét, a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban közös szabályok bevezetésével e cél jobban megvalósítható, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés (EUSZ) 5. cikkében foglalt szubszidiaritás elvének megfelelően. Az említett cikkben foglalt arányosság elvének megfelelően ez a rendelet nem lépi túl az e cél eléréséhez szükséges mértéket.
- (42) Az EUSZ-hez és az EUMSZ-hez csatolt, Dánia helyzetéről szóló 22. jegyzőkönyv 1. és 2. cikke értelmében Dánia nem vesz részt ennek a rendeletnek az elfogadásában, az rá nézve nem kötelező és nem alkalmazandó.
- (43) Az EUSZ-hez és az EUMSZ-hez csatolt, az Egyesült Királyságnak és Írországnak a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség tekintetében fennálló helyzetéről szóló 21. jegyzőkönyv 1. és 2. cikkével és 4a. cikkének (1) bekezdésével összhangban, az említett jegyzőkönyv 4. cikkének sérelme nélkül, Írország nem vesz részt ennek a rendeletnek az elfogadásában, az rá nézve nem kötelező és nem alkalmazandó.
- (44) A 21. jegyzőkönyv 3. cikkével és 4a. cikkének (1) bekezdésével összhangban az Egyesült Királyság bejelentette, hogy részt kíván venni ennek a rendeletnek az elfogadásában és alkalmazásában.
- (45) Az európai adatvédelmi biztossal a 45/2001/EK európai parlamenti és tanácsi rendelet <sup>(15)</sup> 28. cikkének (2) bekezdésével összhangban konzultációra került sor, és a biztos 2017. december 12-én véleményt nyilvánított <sup>(16)</sup>,

ELFOGADTA EZT A RENDELETET:

#### I. FEJEZET

### Általános rendelkezések

#### 1. cikk

#### Tárgy

Ez a rendelet:

- a) létrehozza a harmadik országbeli állampolgárokkal szemben hozott korábbi ítéletekre vonatkozó információval rendelkező tagállamok azonosítására szolgáló rendszert (a továbbiakban: az ECRIS-TCN);
- b) megállapítja azokat a feltételeket, amelyek mellett a központi hatóságoknak a 2009/316/IB határozattal létrehozott Európai Bűnügyi Nyilvántartási Információs Rendszeren (a továbbiakban: az ECRIS) keresztül az ilyen korábbi ítéletekre vonatkozó információk megszerzése érdekében az ECRIS-TCN-t használniuk kell, továbbá azokat a feltételeket, amelyek mellett az Eurojustnak, az Europolnak és az Európai Ügyészségnek az ECRIS-TCN-t használnia kell.

<sup>(13)</sup> HL L 123., 2016.5.12., 1. o.

<sup>(14)</sup> Az Európai Parlament és a Tanács 182/2011/EU rendelete (2011. február 16.) a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról (HL L 55., 2011.2.28., 13. o.).

<sup>(15)</sup> Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról (HL L 8., 2001.1.12., 1. o.).

<sup>(16)</sup> HL C 55., 2018.2.14., 4. o.



## 2. cikk

### Hatály

Ez a rendelet a tagállamokban hozott ítéletek hatálya alá tartozó harmadik országbeli állampolgárok személyazonosító adatainak az ítélethozatal szerinti tagállamok azonosítása céljából történő kezelésére alkalmazandó. Az 5. cikk (1) bekezdése b) pontjának ii. alpontja kivételével e rendelet harmadik országbeli állampolgárokra vonatkozó rendelkezéseit azokra az uniós polgárokra is alkalmazni kell, akik valamely harmadik ország állampolgárságával is rendelkeznek és a tagállamokban hozott ítéletek hatálya alá tartoznak.

## 3. cikk

### Fogalom meghatározások

E rendelet alkalmazásában:

1. „ítélet”: büntetőbíróság által valamely természetes személy ellen bűncselekmény elkövetése miatt hozott jogerős határozat, amennyiben e határozatot felveszik az ítélethozatal szerinti tagállam bűnügyi nyilvántartásaiba;
2. „büntetőeljárás”: a tárgyalást megelőző szakasz, a tárgyalási szakasz, valamint az ítélet végrehajtása;
3. „bűnügyi nyilvántartás”: olyan nemzeti nyilvántartás vagy nyilvántartások, amelyek az ítéleteket a nemzeti joggal összhangban tartalmazzák;
4. „ítélethozatal szerinti tagállam”: az a tagállam, ahol az ítéletet meghozták;
5. „központi hatóság”: a 2009/315/IB kerethatározat 3. cikkének (1) bekezdésével összhangban kijelölt hatóság;
6. „illetékes hatóságok”: e rendelettel összhangban az ECRIS-TCN-hez való hozzáférésre vagy annak lekérdezésére hatáskörrel rendelkező központi hatóságok, valamint az Eurojust, az Europol és az Európai Ügyészség;
7. „harmadik országbeli állampolgár”: olyan személy, aki az EUMSZ 20. cikkének (1) bekezdése értelmében nem uniós polgár, vagy hontalan személy, vagy olyan személy, akinek az állampolgársága nem ismert;
8. „központi rendszer”: a tagállamokban hozott ítéletek hatálya alá tartozó harmadik országbeli állampolgárok személyazonosító adatait tartalmazó, az eu-LISA által kifejlesztett és karbantartott adatbázis vagy adatbázisok;
9. „interfész szoftver”: az illetékes hatóságoknál telepített szoftver, amely lehetővé teszi számukra, hogy a 4. cikk (1) bekezdésének d) pontjában említett kommunikációs infrastruktúrán keresztül hozzáférjenek a központi rendszerhez;
10. „személyazonosító adatok”: alfanumerikus adatok, ujjnyomatadatok és arcképmások, amelyek rendeltetése, hogy ezen adatokat összekapcsolják valamely természetes személlyel;
11. „alfanumerikus adatok”: betűkből, számokból, speciális karakterekből, szóközökből és központozási jelekből álló adatok;
12. „ujjnyomatadatok”: valamely személy összes ujjának sík és átfogatott nyomatára vonatkozó adatok;
13. „arcképmás”: valamely személy arcáról készített digitális felvétel;
14. „találat”: a központi rendszerben rögzített személyazonosító adatok és a lekérdezéshez használt személyazonosító adatok összehasonlításával megállapított egyezés vagy egyezések;
15. „nemzeti központi hozzáférési pont”: a 4. cikk (1) bekezdésének d) pontjában említett kommunikációs infrastruktúrához való nemzeti csatlakozási pont;
16. „ECRIS referenciaalkalmazás”: a bűnügyi nyilvántartási információknak az ECRIS-en keresztül történő cseréje céljából a Bizottság által kifejlesztett és a tagállamok rendelkezésére bocsátott szoftver;
17. „nemzeti felügyeleti hatóság”: egy tagállam által az alkalmazandó uniós adatvédelmi szabályok értelmében létrehozott független közhatalmi szerv;
18. „felügyeleti hatóságok”: az európai adatvédelmi biztos és a nemzeti felügyeleti hatóságok.

## 4. cikk

**Az ECRIS-TCN műszaki architektúrája**

- (1) Az ECRIS-TCN a következőkből áll:
- központi rendszer, amely tárolja az elítélt harmadik országbeli állampolgárok személyazonosító adatait;
  - az egyes tagállamok nemzeti központi hozzáférési pontja;
  - interfész szoftver, amely lehetővé teszi az illetékes hatóságok kapcsolódását a központi rendszerhez a nemzeti központi hozzáférési ponton és a d) pontban említett kommunikációs infrastruktúrán keresztül;
  - kommunikációs infrastruktúra a központi rendszer és a nemzeti központi hozzáférési pontok között.
- (2) A központi rendszer elhelyezését az eu-LISA biztosítja a műszaki telephelyein.
- (3) Az interfész szoftvert integrálni kell az ECRIS referenciaalkalmazásba. A tagállamok az ECRIS referenciaalkalmazást vagy a (4)–(8) bekezdésben meghatározott helyzetekben és feltételek mellett a nemzeti ECRIS alkalmazási szoftvert használják az ECRIS-TCN lekérdezésére és a bűnügyi nyilvántartási információk iránti megkeresések ezt követő elküldésére.
- (4) Azok a tagállamok, amelyek saját nemzeti ECRIS alkalmazási szoftverüket használják, felelősek annak biztosításáért, hogy nemzeti ECRIS alkalmazási szoftverük lehetővé tegye a bűnügyi nyilvántartásokat vezető nemzeti hatóságoknak, hogy e rendelettel összhangban – az interfész szoftver kivételével – használhassák az ECRIS-TCN-t. E célból ezek a tagállamok az ECRIS-TCN működésének a 35. cikk (4) bekezdése szerinti kezdő időpontja előtt biztosítják, hogy nemzeti ECRIS alkalmazási szoftverük a 10. cikkben említett végrehajtási jogi aktusokban meghatározott protokolloknak és műszaki előírásoknak, valamint az eu-LISA által e rendelet alapján meghatározott, az említett végrehajtási jogi aktusokon alapuló további műszaki követelményeknek megfelelően működjön.
- (5) Amíg nem használják az ECRIS referenciaalkalmazást, a saját nemzeti ECRIS alkalmazási szoftverüket használó tagállamok biztosítják azt is, hogy indokolatlan késedelem nélkül elvégezzék nemzeti ECRIS alkalmazási szoftverük minden olyan későbbi műszaki kiigazítását, amelyet a 10. cikkben említett végrehajtási jogi aktusokban meghatározott műszaki előírások vagy az eu-LISA által e rendelet alapján meghatározott, az említett végrehajtási jogi aktusokon alapuló további műszaki követelmények tesznek szükségessé.
- (6) Azok a tagállamok, amelyek saját nemzeti ECRIS alkalmazási szoftverüket használják, viselik a nemzeti ECRIS alkalmazási szoftverük alkalmazásával, karbantartásával és továbbfejlesztésével, valamint az ECRIS-TCN-nel való összeköttetésének biztosításával kapcsolatban felmerülő költségeket, az interfész szoftver kivételével.
- (7) Ha egy olyan tagállam, amely saját nemzeti ECRIS alkalmazási szoftverét használja, nem tudja teljesíteni e cikk szerinti kötelezettségeit, az ECRIS-TCN igénybevételehez köteles az ECRIS referenciaalkalmazást használni, az integrált interfész szoftvert is beleértve.
- (8) A 36. cikk (10) bekezdésének b) pontja szerinti, a Bizottság által elvégzendő értékelésre tekintettel az érintett tagállamok minden szükséges információt a Bizottság rendelkezésére bocsátanak.

## II. FEJEZET

**A központi hatóságok általi adatfeltöltés és -felhasználás**

## 5. cikk

**Adatfeltöltés az ECRIS-TCN-be**

- (1) Az ítélethozatal szerinti tagállam központi hatósága minden elítélt harmadik országbeli állampolgár esetében adatrekordot hoz létre a központi rendszerben. Az adatrekordnak a következőket kell tartalmaznia:
- az alfanumerikus adatok tekintetében:
    - a következő információk, kivéve, ha egyedi esetekben a központi hatóság számára ezek az információk nem ismertek (kötelező információk):
      - vezetéknev (családi név),
      - utónevek (keresztnevek),

- születési idő,
  - születési hely (város és ország),
  - állampolgárság vagy állampolgárságok,
  - nem,
  - adott esetben korábbi nevek,
  - az ítélethozatal szerinti tagállam kódja;
- ii. a következő információk, ha szerepelnek a büntügyi nyilvántartásban (opcionális információk):
- szülők neve;
- iii. a következő információk, ha a központi hatóság számára rendelkezésre állnak (kiegészítő információk):
- személyazonosító szám, vagy a személy személyazonosító okmányainak típusa és száma, valamint a kiállító hatóság neve,
  - álnevek vagy felvett nevek;
- b) az ujjnyomatatok tekintetében:
- i. a büntetőeljárás során a nemzeti joggal összhangban gyűjtött ujjnyomatatok;
- ii. legalább az alábbi kritériumok alapján gyűjtött ujjnyomatatok:
- ha a harmadik országbeli állampolgárra legalább 6 hónap szabadságvesztés büntetést szabtak ki;
- vagy
- ha a harmadik országbeli állampolgárt olyan bűncselekmény miatt ítélték el, amellyel kapcsolatban a tagállam joga alapján kiszabható büntetési tétel felső határa legalább 12 hónap szabadságvesztés.
- (2) Az e cikk (1) bekezdése b) pontjában említett ujjnyomatatokra a 10. cikk (1) bekezdésének b) pontjában említett végrehajtási jogi aktusban meghatározott, az ujjnyomatatok minőségére, felbontására és feldolgozására vonatkozó műszaki előírásokat kell alkalmazni. Az elítélt személy ujjnyomatadatai referenciaszámának tartalmaznia kell az ítélethozatal szerinti tagállam kódját.
- (3) Az adatrekord az elítélt harmadik országbeli állampolgár arcképmásait is tartalmazhatja, ha az ítélethozatal szerinti tagállam joga lehetővé teszi az elítélt személyek arcképmásainak gyűjtését és tárolását.
- (4) Az ítélethozatal szerinti tagállam lehetőség szerint automatikusan, és az ítéletnek a büntügyi a nyilvántartásokba való bekerülését követően indokolatlan késedelem nélkül létrehozza az adatrekordot.
- (5) Az ítélethozatal szerinti tagállamok emellett az adatfeltöltésnek a 35. cikk (1) bekezdésével összhangban meghatározott kezdő időpontja előtt hozott ítéletek vonatkozásában is létrehozzák az adatrekordokat, amennyiben nemzeti adatbázisaikban tárolják az elítélt személyekkel kapcsolatos adatokat. Ezekben az esetekben az ujjnyomatadatokat csak akkor kell bevinni, ha büntetőeljárás során a nemzeti joggal összhangban kerültek begyűjtésre, és amennyiben egyértelműen megfeleltethetők a büntügyi nyilvántartásokban szereplő más személyazonosító adatoknak.
- (6) Az (1) bekezdés b) pontjának i. és ii. alpontjában, valamint az (5) bekezdésben meghatározott kötelezettségek teljesítése érdekében a tagállamok büntetőeljárástól eltérő célokból begyűjtött ujjnyomatadatokat is felhasználhatnak, amennyiben e felhasználást a nemzeti jog megengedi.

## 6. cikk

### Arcképmások

- (1) A (2) bekezdésben meghatározott felhatalmazáson alapuló jogi aktus hatálybalépéséig az arcképmások kizárólag az alfanumerikus lekérdezés vagy ujjnyomatadatokat alkalmazó lekérdezés eredményeként azonosított harmadik országbeli állampolgár személyazonosságának megerősítésére használhatók fel.
- (2) A Bizottság felhatalmazást kap arra, hogy – amint az műszakilag lehetségessé válik – a 37. cikknek megfelelően az e rendeletet kiegészítő felhatalmazáson alapuló jogi aktusokat fogadjon el az arcképmások harmadik országbeli állampolgárok azonosítása céljából történő felhasználására vonatkozóan, annak azonosítása érdekében, hogy mely tagállamok rendelkeznek az említett személyekkel szemben hozott korábbi ítéletekre vonatkozó információval. E felhatalmazás gyakorlását megelőzően a Bizottság – a szükségesség és az arányosság, valamint az arcfelismerő szoftverek terén végbemenő műszaki fejlődés figyelembevételével – értékeli a szükséges technológia rendelkezésre állását és alkalmazhatóságát.

## 7. cikk

**A bűnügyi nyilvántartási információval rendelkező tagállamok azonosítására szolgáló ECRIS-TCN használata**

(1) A központi hatóságoknak az ECRIS-TCN-t kell használniuk a harmadik országbeli állampolgárokra vonatkozó bűnügyi nyilvántartási információval rendelkező tagállamok azonosítására annak érdekében, hogy az ECRIS-en keresztül korábbi ítéletekre vonatkozóan információkat szerezzenek, ha az érintett tagállamban az adott személyre vonatkozóan bűnügyi nyilvántartási információkat kérnek az e személlyel szembeni büntetőeljárás céljából vagy valamely alábbi célból, amennyiben a nemzeti jog így rendelkezik, és azzal összhangban:

- valamely személy kérelmére a bűnügyi nyilvántartásban rá vonatkozóan szereplő adatok ellenőrzése,
- biztonsági ellenőrzés,
- engedély szerzése,
- foglalkoztatás ellenőrzése,
- ellenőrzés gyermekekkel vagy különleges bánásmódot igénylő személyekkel való közvetlen és rendszeres kapcsolat-tartással járó önkéntes tevékenységek végzéséhez,
- vízumeljárások, állampolgárság megszerzésére irányuló eljárások és migrációs eljárások, a menekültügyi eljárásokat is beleértve, valamint
- közbeszerzési szerződésekkel és állami vizsgálatokkal összefüggő ellenőrzések.

Mindazonáltal egyedi esetekben a bűnügyi nyilvántartási információkat kérő hatóság dönthet úgy, hogy az ECRIS-TCN használata nem helyénvaló, kivéve, ha valamely harmadik országbeli állampolgár a bűnügyi nyilvántartásokban rá vonatkozóan szereplő adatokról kér információt a központi hatóságtól, vagy ha az információ iránti megkeresésre a 2011/93/EU irányelv 10. cikke (2) bekezdése alapján bűnügyi nyilvántartási információk megszerzése céljából kerül sor.

(2) Bármely tagállam, amely – amennyiben a nemzeti jog így rendelkezik, és azzal összhangban – az ECRIS-TCN-nek az (1) bekezdésben meghatározottaktól eltérő célokra történő használatáról határoz annak érdekében, hogy az ECRIS-en keresztül korábbi ítéletekre vonatkozóan információkat szerezzen, ezekről az egyéb célokról és az ilyen célok bármilyen változásairól a rendszer működésének a 35. cikk (4) bekezdésében említett kezdő időpontjáig vagy azt követően bármikor értesíti a Bizottságot. A Bizottság ezeket az értesítéseket a kézhezvételüket követő 30 napon belül közzéteszi az *Európai Unió Hivatalos Lapjában*.

(3) Az Eurojust, az Europol valamint az Európai Ügyészség a 14–18. cikkel összhangban jogosultak lekérdezni az ECRIS-TCN-t a harmadik országbeli állampolgárokra vonatkozó bűnügyi nyilvántartási információval rendelkező tagállamok azonosítása céljából. Ugyanakkor ezek az ECRIS-TCN-be nem tölthetnek fel adatokat, azokat nem helyesbíthetik és nem törölhetik.

(4) Az (1), a (2) és a (3) bekezdésben említett célokból az illetékes hatóságok az ECRIS-TCN-t lekérdezhetik egy uniós polgárra vonatkozóan annak ellenőrzése céljából is, hogy bármely tagállam rendelkezik-e bűnügyi nyilvántartási információkkal erre a személyre vonatkozóan úgy, mint harmadik országbeli állampolgár.

(5) Az ECRIS-TCN lekérdezésekor az illetékes hatóságok felhasználhatják az 5. cikk (1) bekezdésében említett adatok mindegyikét vagy csak egy részét. A rendszer lekérdezéséhez minimálisan szükséges adatokat a 10. cikk (1) bekezdésének g) pontjával összhangban elfogadott végrehajtási jogi aktusban kell meghatározni.

(6) Az illetékes hatóságok arcképmások felhasználásával is lekérdezhetik az ECRIS-TCN-t, amennyiben ezt a funkciót a 6. cikk (2) bekezdésével összhangban bevezették.

(7) Találat esetén a központi rendszer automatikusan megadja az illetékes hatóságnak a harmadik országbeli állampolgárra vonatkozó bűnügyi nyilvántartási információval rendelkező tagállamokra vonatkozó információt, a kapcsolódó referenciaszámokkal és a megfelelő személyazonosító adatokkal együtt. Ezek a személyazonosító adatok kizárólag az érintett harmadik országbeli állampolgár személyazonosságának ellenőrzése céljára használhatók fel. A központi rendszer lekérdezésének eredményét csak a 2009/315/IB kerethatározat 6. cikke szerinti vagy az e rendelet 17. cikkének (3) bekezdése szerinti megkeresések céljára lehet felhasználni.

(8) Abban az esetben, ha nincs találat, a központi rendszer erről automatikusan tájékoztatja az illetékes hatóságot.

## III. FEJEZET

**Az adatok megőrzése és módosítása**

## 8. cikk

**Az adatok megőrzésének időtartama**

(1) Minden adatrekordot addig kell tárolni a központi rendszerben, amíg az érintett személlyel kapcsolatos ítéletekre vonatkozó adatokat a bűnügyi nyilvántartásokban tárolják.

(2) Az (1) bekezdésben említett adatmegőrzési időtartam lejártakor az ítéletozatal szerinti tagállam központi hatóságának törölnie kell a központi rendszerből az adatrekordot, beleértve az ujjnyomatadatokat és az arcképmásokat is. Ezt a törlést lehetőség szerint automatikusan, de minden esetben legkésőbb egy hónappal a megőrzési időtartam lejártát követően el kell végezni.

#### 9. cikk

### **Az adatok módosítása és törlése**

(1) A tagállamok módosíthatják vagy törölhetik az ECRIS-TCN-be általuk feltöltött adatokat.

(2) A bünyügyi nyilvántartásokban szereplő, az 5. cikkel összhangban az adatrekord létrehozására vezető információk bármely módosítása maga után vonja a központi rendszerben található említett adatrekordban tárolt információk ítéletozatal szerinti tagállam általi, indokolatlan késedelem nélküli azonos módosítását.

(3) Ha az ítéletozatal szerinti tagállam okkal feltételezi, hogy a központi rendszerben általa rögzített adatok pontatlanok, vagy hogy az adatok központi rendszeren belüli kezelése e rendeletet sértő módon történt:

a) azonnal elindítja az érintett adatok pontosságának vagy adott esetben az azok jogszerű kezelésének ellenőrzésére irányuló eljárást;

b) szükség esetén indokolatlan késedelem nélkül helyesbíti az adatokat vagy törli azokat a központi rendszerből.

(4) Ha az adatokat feltöltő, az ítéletozatal szerinti tagállamtól eltérő valamely tagállam okkal feltételezi, hogy a központi rendszerben rögzített adatok pontatlanok, vagy hogy az adatok központi rendszeren belüli kezelése e rendeletet sértő módon történt, indokolatlan késedelem nélkül kapcsolatba lép az ítéletozatal szerinti tagállam központi hatóságával.

Az ítéletozatal szerinti tagállam:

a) azonnal elindítja az érintett adatok pontosságának vagy adott esetben az azok jogszerű kezelésének ellenőrzésére irányuló eljárást;

b) szükség esetén indokolatlan késedelem nélkül helyesbíti az adatokat vagy törli azokat a központi rendszerből;

c) indokolatlan késedelem nélkül tájékoztatja a másik tagállamot az adatok helyesbítéséről vagy törléséről, vagy arról, hogy az adatok helyesbítésére vagy törlésére miért nem került sor.

#### IV. FEJEZET

### **Kifejlesztés, üzemeltetés és feladatok**

#### 10. cikk

### **Végrehajtási jogi aktusok Bizottság általi elfogadása**

(1) A Bizottság a lehető leghamarabb elfogadja az ECRIS-TCN műszaki kifejlesztéséhez és kivitelezéséhez szükséges végrehajtási jogi aktusokat és különösen az alábbiakra vonatkozó jogi aktusokat:

a) az alfanumerikus adatok kezelésére vonatkozó műszaki előírások;

b) az ujjnyomatatok minőségére, felbontására és kezelésére vonatkozó műszaki előírások;

c) az interfész szoftver műszaki leírása;

d) az arcképmások minőségére, felbontására és a 6. cikkben meghatározott célokból és feltételekkel történő kezelésére vonatkozó műszaki előírások;

e) az adatminőség, beleértve az adatminőség-ellenőrzések elvégzésére szolgáló mechanizmust és eljárásokat is;

f) az adatok feltöltése az 5. cikkel összhangban;

g) az ECRIS-TCN-hez való hozzáférés és a rendszer lekérdezése a 7. cikkel összhangban;

h) az adatok módosítása és törlése a 8. és a 9. cikkel összhangban;

- i) a naplók vezetése és az azokhoz való hozzáférés a 31. cikkel összhangban;
  - j) a központi adattár üzemeltetése és az adattárra alkalmazandó adatbiztonsági és adatvédelmi szabályok a 32. cikkel összhangban;
  - k) statisztikák biztosítása a 32. cikkel összhangban;
  - l) az ECRIS-TCN teljesítményére és rendelkezésre állására vonatkozó követelmények, beleértve az ECRIS-TCN biometrikus teljesítményére vonatkozó minimális előírásokat és követelményeket is, különös tekintettel a hamis pozitív találati arány és a hamis negatív találati arány tekintetében meghatározott követelményszintre.
- (2) Az (1) bekezdésben említett végrehajtási jogi aktusokat a 38. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

### 11. cikk

#### Az ECRIS-TCN kifejlesztése és üzemeltetési igazgatása

- (1) Az ECRIS-TCN kifejlesztése – a beépített és az alapértelmezett adatvédelem elvével összhangban – az eu-LISA feladata. Emellett az ECRIS-TCN üzemeltetési igazgatása is az eu-LISA feladata. A kifejlesztés a műszaki előírások kidolgozását és végrehajtását, a tesztelést és az átfogó projektkoordinációt foglalja magában.
- (2) Az ECRIS referenciaalkalmazás továbbfejlesztése és karbantartása is az eu-LISA feladata.
- (3) Az eu-LISA meghatározza az ECRIS-TCN fizikai architektúrájának tervét, beleértve annak műszaki előírásait és továbbfejlesztését a központi rendszer, a nemzeti központi hozzáférési pont, valamint az interfész szoftver tekintetében. Az említett tervet a Bizottság kedvező véleményét követően az igazgatótanácsnak kell elfogadnia.
- (4) Az eu-LISA e rendelet hatálybalépését és a 10. cikkben meghatározott végrehajtási jogi aktusok Bizottság általi elfogadását követően a lehető leghamarabb kifejleszti és üzembe helyezi az ECRIS-TCN-t.
- (5) Az ECRIS-TCN tervezési és kifejlesztési szakaszát megelőzően az eu-LISA igazgatótanácsa létrehoz egy tíz tagból álló programirányítási tanácsot.

A programirányítási tanács az igazgatótanács által kinevezett nyolc tagból, a 39. cikkben említett tanácsadó csoport elnökéből, valamint a Bizottság által kinevezett egy tagból áll. Az igazgatótanács kizárólag olyan tagállamokból nevezhet ki tagokat, amelyekre nézve az uniós jog értelmében teljes mértékben kötelezők az ECRIS-t szabályozó jogalkotási eszközök, és amelyek részt fognak venni az ECRIS-TCN-ben. Az igazgatótanácsnak gondoskodnia kell arról, hogy az általa a programirányítási tanácsba kinevezett tagok rendelkezzenek az igazságügyi és a bűnügyi nyilvántartó hatóságokat támogató IT-rendszerek kifejlesztése és igazgatása terén szükséges tapasztalattal és szakértelemmel.

Az eu-LISA részt vesz a programirányítási tanács munkájában. Ennek érdekében az eu-LISA képviselői részt vesznek a programirányítási tanács ülésein, hogy beszámoljanak az ECRIS-TCN tervezésével és kifejlesztésével kapcsolatban végzett munkáról, valamint bármely egyéb kapcsolódó munkáról és tevékenységekről.

A programirányítási tanácsnak legalább háromhavonta, szükség esetén pedig gyakrabban kell üléseznie. Biztosítani kell az ECRIS-TCN tervezési és kifejlesztési szakaszának megfelelő irányítását, továbbá biztosítani kell, hogy az ECRIS-TCN-nel kapcsolatos központi és nemzeti projektek összhangban legyenek egymással, és a nemzeti ECRIS alkalmazási szoftverrel. A programirányítási tanácsnak rendszeresen és lehetőleg havonta, írásbeli jelentést kell benyújtania az eu-LISA igazgatótanácsa számára a projekt előrehaladásáról. A programirányítási tanács nem rendelkezik döntéshozatali hatáskörrel, és nem képviselheti az igazgatótanács tagjait.

- (6) A programirányítási tanácsnak meg kell határoznia saját eljárási szabályzatát, amely különösen a következőkről rendelkezik:
- a) az elnökség;
  - b) az ülések helyszíne;
  - c) az ülések előkészítése;
  - d) szakértők részvétele az üléseken;
  - e) az igazgatótanácsban részt nem vevő tagállamok számára való teljeskörű tájékoztatást biztosító kommunikációs tervek.

(7) A programirányítási tanács elnökségét olyan tagállamnak kell betöltenie, amelyre nézve az uniós jog értelmében teljes mértékben kötelezők az ECRIS-t szabályozó jogalkotási eszközök és az eu-LISA által üzemeltetett összes nagyméretű IT-rendszer kifejlesztését, létrehozását, működtetését és használatát szabályozó jogalkotási eszközök.

(8) A programirányítási tanács tagjainak valamennyi utazási és ellátási költségét az eu-LISA fedezi. Az eu-LISA eljárási szabályzatának 10. cikke értelemszerűen alkalmazandó. A programirányítási tanács titkárságát az eu-LISA biztosítja.

(9) A tervezési és kifejlesztési szakaszban a 39. cikkben említett tanácsadó csoport az ECRIS-TCN-nel kapcsolatos nemzeti projektek projektmenedzsereiből áll, elnöki tisztét pedig az eu-LISA tölti be. A tervezési és kifejlesztési szakaszban a tanácsadó csoportnak az ECRIS-TCN működésének megkezdéséig rendszeresen, lehetőleg havonta legalább egyszer üléseznie kell. A tanácsadó csoportnak minden ülés után be kell számolnia a programirányítási tanácsnak. A tanácsadó csoportnak biztosítania kell a programirányítási tanács tevékenységét segítő szakértelmet, valamint nyomon kell követnie a tagállami előkészületek alakulását.

(10) Az ECRIS-TCN-ben tárolt adatok titkosságának és sérthetlenségének állandó biztosítása érdekében az eu-LISA – a tagállamokkal együttműködve – megfelelő műszaki és szervezési intézkedésekről gondoskodik, figyelembe véve a technika állását, a megvalósítás költségét és az adatkezeléssel járó kockázatokat.

(11) Az eu-LISA felelős a 4. cikk (1) bekezdésének d) pontjában említett kommunikációs infrastruktúrával kapcsolatos következő feladatokért:

- a) felügyelet;
- b) biztonság;
- c) a tagállamok és a kommunikációs infrastruktúra szolgáltatója közötti kapcsolatok koordinációja.

(12) A Bizottság felelős a 4. cikk (1) bekezdése d) pontjában említett kommunikációs infrastruktúrához kapcsolódó minden egyéb feladatért, különösen a következőkért:

- a) a költségvetés végrehajtásával kapcsolatos feladatok;
- b) beszerzés és megújítás;
- c) szerződéses ügyek.

(13) Az eu-LISA az ECRIS-TCN-ben tárolt adatok minőségének ellenőrzésére szolgáló mechanizmust és eljárásokat dolgoz ki és tart fenn, továbbá rendszeresen jelentést tesz a tagállamoknak. Az eu-LISA rendszeresen jelentéseket küld a Bizottságnak és az érintett tagállamoknak, amelyben beszámol a felmerült problémákról.

(14) Az ECRIS-TCN üzemeltetési igazgatása magában foglalja az ECRIS-TCN e rendeletnek megfelelő működtetéséhez szükséges valamennyi feladatot, különösen azokat a karbantartási munkákat és műszaki fejlesztéseket, amelyek az ECRIS-TCN kielégítő szintű, a műszaki előírásoknak megfelelő működéséhez szükségesek.

(15) Az eu-LISA ellátja az ECRIS-TCN és az ECRIS referenciaalkalmazás műszaki használatára vonatkozó képzéssel kapcsolatos feladatokat.

(16) A 259/68/EGK, Euratom, ESZAK tanácsi rendelettel<sup>(17)</sup> megállapított, az Európai Unió tisztviselőinek személyzeti szabályzata 17. cikkének sérelme nélkül, az eu-LISA megfelelő szakmai titoktartási vagy azzal egyenértékű titoktartási szabályokat alkalmaz személyzetének minden olyan tagjára, aki munkája során a központi rendszerben rögzített adatokkal dolgozik. Ezt a kötelezettséget a személyzet említett tagjai hivatali vagy munkaviszonyának megszűnését, illetve tevékenységük befejezését követően is alkalmazni kell.

## 12. cikk

### A tagállamok feladatai

(1) Valamennyi tagállam feladata:

- a) nemzeti bűnügyi nyilvántartásai és ujjnyomat-adatbázisai, valamint a nemzeti központi hozzáférési pont közötti biztonságos kapcsolat biztosítása;
- b) az a) pontban említett kapcsolat fejlesztése, működtetése és karbantartása;
- c) nemzeti rendszereik és az ECRIS referenciaalkalmazás közötti kapcsolat biztosítása;

<sup>(17)</sup> HLL 56., 1968.3.4., 1. o.

d) a központi hatóságok megfelelően felhatalmazott személyzete számára az ECRIS-TCN-hez e rendelettel összhangban biztosított hozzáférés irányítása és szabályozása, valamint a személyzet említett tagjai listájának és a 19. cikk (3) bekezdésének g) pontjában említett profiloknak az elkészítése és rendszeres aktualizálása.

(2) Valamennyi tagállam megfelelő – különösen az adatbiztonsággal és az adatvédelmi szabályokkal, valamint az alkalmazandó alapvető jogokkal kapcsolatos – képzésben részesíti központi hatóságának az ECRIS-TCN-hez hozzáférési jogosultsággal rendelkező személyzetét, mielőtt engedélyezné számukra a központi rendszerben tárolt adatok kezelését.

### 13. cikk

#### **Az adatok felhasználásával kapcsolatos kötelezettség**

(1) Az alkalmazandó uniós adatvédelmi szabályokkal összhangban valamennyi tagállam biztosítja az ECRIS-TCN-ben rögzített adatok jogszerű kezelését és különösen az alábbiakat:

- a) kizárólag a megfelelően felhatalmazott személyzet rendelkezik hozzáféréssel az adatokhoz feladatai ellátása érdekében;
- b) az adatokat jogszerűen és a harmadik országbeli állampolgár emberi méltóságát és alapvető jogait maradéktalanul tiszteletben tartó módon gyűjtik;
- c) az adatokat jogszerűen töltik fel az ECRIS-TCN-be;
- d) az ECRIS-TCN-be való feltöltésükkor az adatok pontosak és naprakészek.

(2) Az eu-LISA biztosítja, hogy az ECRIS-TCN működtetésére e rendelettel, a 6. cikk (2) bekezdésében említett felhatalmazáson alapuló jogi aktusokkal, a 10. cikkben említett végrehajtási jogi aktusokkal, valamint az (EU) 2018/1725 rendelettel összhangban kerüljön sor. Az eu-LISA különösen megteszi a központi rendszer, valamint a 4. cikk (1) bekezdésének d) pontjában említett kommunikációs infrastruktúra biztonságának biztosítása érdekében szükséges intézkedéseket, az egyes tagállamok feladatainak sérelme nélkül.

(3) Az eu-LISA az ECRIS-TCN működésének megkezdésére tekintettel a (2) bekezdés alapján általa megtett intézkedésekről a lehető leghamarabb tájékoztatja az Európai Parlamentet, a Tanácsot, a Bizottságot és az európai adatvédelmi biztost.

(4) A Bizottság a (3) bekezdésben említett információkat egy rendszeresen aktualizált, nyilvános honlapon elérhetővé teszi a tagállamok és a nyilvánosság számára.

### 14. cikk

#### **Az Eurojust, az Europol és az Európai Ügyészség hozzáférése**

(1) Az Eurojust a 17. cikk végrehajtása, valamint az (EU) 2018/1727 rendelet 2. cikke szerinti feladatai teljesítése céljából közvetlen hozzáféréssel rendelkezik az ECRIS-TCN-hez a harmadik országbeli állampolgárokkal szemben hozott korábbi ítéletekre vonatkozó információval rendelkező tagállamok azonosítása érdekében.

(2) Az Europol az (EU) 2016/794 rendelet 4. cikke (1) bekezdésének a)–e) és h) pontja szerinti feladatai teljesítése céljából közvetlen hozzáféréssel rendelkezik az ECRIS-TCN-hez a harmadik országbeli állampolgárokkal szemben hozott korábbi ítéletekre vonatkozó információval rendelkező tagállamok azonosítása érdekében.

(3) Az Európai Ügyészség az (EU) 2017/1939 rendelet 4. cikke szerinti feladatai teljesítése céljából közvetlen hozzáféréssel rendelkezik az ECRIS-TCN-hez a harmadik országbeli állampolgárokkal szemben hozott korábbi ítéletekre vonatkozó információval rendelkező tagállamok azonosítása érdekében.

(4) Az azt jelző találatot követően, hogy egyes tagállamok egy harmadik országbeli állampolgárra vonatkozóan bünyügyi nyilvántartási információkkal rendelkeznek, az Eurojust, az Europol és az Európai Ügyészség felhasználhatja ezen tagállamok nemzeti hatóságaival a létesítő jogi eszközének megfelelően kialakított vonatkozó kapcsolatait, hogy kikérje a bünyügyi nyilvántartási információkat.

### 15. cikk

#### **Az Eurojust, az Europol és az Európai Ügyészség felhatalmazott személyzetének hozzáférése**

Az Eurojust, az Europol és az Európai Ügyészség feladata megfelelően felhatalmazott személyzete számára az ECRIS-TCN-hez e rendelettel összhangban biztosított hozzáférés irányítása és szabályozása, valamint a személyzet említett tagjai listájának és profiljuknak az elkészítése és rendszeres aktualizálása.



## 16. cikk

**Az Eurojust, az Europol és az Európai Ügyészség feladatai**

Az Eurojust, az Europol és az Európai Ügyészség:

- a) kialakítja az ECRIS-TCN-hez való kapcsolódásra szolgáló műszaki eszközöket, és felelős a kapcsolat fenntartásáért;
- b) megfelelő – különösen az adatbiztonsággal és az adatvédelmi szabályokkal, valamint az alkalmazandó alapvető jogokkal kapcsolatos – képzésben részesíti az ECRIS-TCN-hez hozzáférési jogosultsággal rendelkező személyzetét, mielőtt engedélyezné számára a központi rendszerben tárolt adatok kezelését;
- c) biztosítja, hogy az e rendelet alapján általa kezelt személyes adatok az alkalmazandó adatvédelmi szabályoknak megfelelő védelemben részesüljenek.

## 17. cikk

**Kapcsolattartó pont harmadik országok és nemzetközi szervezetek számára**

- (1) Harmadik országok és nemzetközi szervezetek büntetőeljárások céljából az Eurojusthoz azon uniós tagállamokra vonatkozó információ iránti megkereséseket intézhetnek, amelyek harmadik országbeli állampolgárokkal kapcsolatos bűnügyi nyilvántartási információkkal rendelkeznek, ha vannak ilyen tagállamok. E célra az e rendelet mellékletében foglalt egységes formanyomtatványt kell használniuk.
- (2) Amikor az Eurojusthoz az (1) bekezdésben említett megkeresés érkezik, az az ECRIS-TCN használatával azonosítja, hogy – ha vannak ilyen tagállamok – mely tagállamok rendelkeznek bűnügyi nyilvántartási információkkal az érintett harmadik országbeli állampolgárra vonatkozóan.
- (3) Találat esetén az Eurojust az érintett harmadik országbeli állampolgárra vonatkozó bűnügyi nyilvántartási információval rendelkező tagállamhoz kérdést intéz, hogy hozzájárul-e ahhoz, hogy az Eurojust tájékoztassa a harmadik országot vagy nemzetközi szervezetet az érintett tagállam nevééről. E tagállam hozzájárulása esetén az Eurojust tájékoztatja a harmadik országot vagy a nemzetközi szervezetet e tagállam nevééről, valamint arról, hogy az adott tagállamhoz hogyan intézhet bűnügyi nyilvántartási kivonatok iránti megkeresést az alkalmazandó eljárásokkal összhangban.
- (4) Amennyiben a keresés nem eredményez találatot, vagy az Eurojust a (3) bekezdéssel összhangban nem tudja megválaszolni az e cikk szerinti megkereséseket, az Eurojust tájékoztatja az érintett harmadik országot vagy nemzetközi szervezetet, hogy lezárta az eljárást, arra való utalás nélkül, hogy valamelyik tagállam rendelkezik-e az érintett személyre vonatkozó bűnügyi nyilvántartási információkkal.

## 18. cikk

**Információs szolgáltatás harmadik ország, nemzetközi szervezet vagy magánfél részére**

Az Eurojust, az Europol, az Európai Ügyészség, és a központi hatóság nem továbbítja és nem bocsátja rendelkezésre az ECRIS-TCN-ből származó, valamely harmadik országbeli állampolgárra vonatkozó információkat harmadik ország, nemzetközi szervezet vagy magánfél részére. Ez a cikk a 17. cikk (3) bekezdésének sérelme nélkül alkalmazandó.

## 19. cikk

**Adatbiztonság**

- (1) Az eu-LISA – az egyes tagállamok feladatainak sérelme nélkül – megteszi a szükséges intézkedéseket az ECRIS-TCN biztonságának biztosítása érdekében, figyelembe véve a (3) bekezdésben megállapított biztonsági intézkedéseket.
- (2) Az ECRIS-TCN üzemeltetését illetően az eu-LISA megteszi a szükséges intézkedéseket a (3) bekezdésben foglalt célok – ideértve egy biztonsági terv, valamint egy üzletmenet-folytonossági és katasztrófa utáni helyreállítási terv elfogadását is – teljesülése, továbbá a telepített rendszerek üzemzavar esetén való helyreállíthatóságának biztosítása érdekében.
- (3) A tagállamok biztosítják az adatok biztonságát a nemzeti központi hozzáférési ponthoz való adattovábbítás és az onnan való adatátvitel előtt és alatt. Minden tagállam különösen:
  - a) fizikai adatvédelmet valósít meg, többek között az infrastruktúra védelmére irányuló vészhelyzeti tervek kidolgozása által;
  - b) megtagadja a jogosulatlan személyek hozzáféréseit azokhoz a nemzeti létesítményekhez, amelyekben a tagállam az ECRIS-TCN-nel kapcsolatos műveleteket végez;
  - c) megakadályozza az adathordozók jogosulatlan olvasását, másolását, módosítását és eltávolítását;

- d) megakadályozza az adatok jogosulatlan bevitelét, valamint a tárolt személyes adatok jogosulatlan ellenőrzését, módosítását vagy törlését;
  - e) megakadályozza az ECRIS-TCN-ben található adatok jogosulatlan kezelését és az ECRIS-TCN-ben kezelt adatok jogosulatlan módosítását vagy törlését;
  - f) biztosítja, hogy az ECRIS-TCN-hez való hozzáférésre jogosult személyek kizárólag a hozzáférési engedélyükben meghatározott adatokhoz férjenek hozzá, kizárólag egyéni felhasználói azonosítók és titkos hozzáférési módszerek útján;
  - g) biztosítja, hogy az ECRIS-TCN-hez hozzáférési jogosultsággal rendelkező összes hatóság olyan profilokat hozzon létre, amelyek leírják az adatok feltöltésére, helyesbítésére, törlésére, lekérdezésére és az adatokba való betekintésre jogosult személyek feladat- és hatáskörét, és ezeket a profilokat a nemzeti felügyeleti hatóságok számára – kérelmükre – indokolatlan késedelem nélkül rendelkezésre bocsássa;
  - h) biztosítja, hogy ellenőrizhető és megállapítható legyen, hogy mely uniós szervekhez, hivatalokhoz és ügynökségekhez lehet személyes adatokat továbbítani az adatátviteli berendezések használatával;
  - i) biztosítja, hogy ellenőrizhető és megállapítható legyen, hogy ki, mikor, mely adatokat és milyen célból kezelt az ECRIS-TCN-ben;
  - j) megakadályozza a személyes adatok ECRIS-TCN-be vagy ECRIS-TCN-ből történő továbbítása vagy adathordozón történő szállítása során a személyes adatok jogosulatlan olvasását, másolását, módosítását vagy törlését, különösen megfelelő titkosítási technikák révén;
  - k) ellenőrzi az e bekezdésben említett biztonsági intézkedések hatékonyságát, és megteszi az önellenőrzéssel és felügyelettel kapcsolatban szükséges szervezési intézkedéseket az e rendeletnek való megfelelés biztosítása érdekében.
- (4) Az eu-LISA és a tagállamok együttműködnek egy olyan egységes adatbiztonsági megközelítés biztosítása érdekében, amely az ECRIS-TCN egészére kiterjedő biztonságkockázat-kezelési folyamaton alapul.

#### 20. cikk

#### Felelősség

(1) Minden személy vagy tagállam, aki vagy amely jogszerűtlen adatkezelési művelet vagy az e rendelettel összeegyeztethetetlen bármilyen egyéb cselekmény eredményeként vagyoni vagy nem vagyoni kárt szenvedett, kártérítésre jogosult:

- a) az elszenvedett kárért felelős tagállamtól; vagy
- b) az eu-LISA-tól, ha az eu-LISA nem tett eleget az e rendeletben vagy az (EU) 2018/1725 rendeletben meghatározott kötelezettségeinek.

Az elszenvedett kárért felelős tagállam vagy az eu-LISA részben vagy egészben mentesül e felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért nem terheli felelősség.

(2) Ha egy tagállam, az Eurojust, az Europol vagy az Európai Ügyészség e rendelet szerinti kötelezettségeinek elmulasztásával kárt okoz az ECRIS-TCN-ben, az okozott kárért való felelősséget ez a tagállam, az Eurojust, az Europol vagy az Európai Ügyészség – attól függően, hogy a kárt melyikük okozta – viseli, kivéve, amennyiben az eu-LISA vagy az ECRIS-TCN-ben részt vevő valamely másik tagállam elmulasztotta megtenni a kár megelőzéséhez vagy hatásának minimalizálásához szükséges észszerű intézkedéseket.

(3) A tagállammal szembeni, az (1) és a (2) bekezdésben említett kárral kapcsolatos kártérítési igényre az alperes tagállam joga alkalmazandó. Az eu-LISA-val, az Eurojust-tal, az Europolal és az Európai Ügyészséggel szembeni, az (1) és a (2) bekezdésben említett kárral kapcsolatos kártérítési igényre az őket létrehozó jogi aktusok alkalmazandók.

#### 21. cikk

#### Önellenőrzés

A tagállamok biztosítják, hogy valamennyi központi hatóság megtegye az e rendeletnek való megfeleléshez szükséges intézkedéseket, és szükség esetén együttműködjön a felügyeleti hatóságokkal.

#### 22. cikk

#### Szankciók

Az ECRIS-TCN-be feltöltött adatokkal való visszaélésekre a nemzeti vagy az uniós joggal összhangban hatékony, arányos és visszatartó erejű szankcióknak vagy fegyelmi intézkedéseknek kell vonatkoznuk.

## V. FEJEZET

**Adatvédelmi jogok és felügyelet**

## 23. cikk

**Adatkezelő és adatfeldolgozó**

- (1) Minden központi hatóság az alkalmazandó uniós adatvédelmi szabályokkal összhangban adatkezelőnek minősül az adott tagállam által e rendelet alapján végzett személyesadat-kezelés tekintetében.
- (2) Az eu-LISA az (EU) 2018/1725 rendelettel összhangban adatfeldolgozónak minősül a tagállamok által a központi rendszerbe feltöltött személyes adatok tekintetében.

## 24. cikk

**A személyes adatok kezelésének célja**

- (1) A központi rendszerbe feltöltött adatok kizárólag a harmadik országbeli állampolgárokra vonatkozó bűnügyi nyilvántartási információval rendelkező tagállamok azonosítása céljából kezelhetők.
- (2) Az Eurojust, az Europol és az Európai Ügyészség megfelelően felhatalmazott személyzetének kivételével, akik ezen rendelet céljából hozzáféréssel rendelkeznek az ECRIS-TCN-hez, az ECRIS-TCN-hez való hozzáférés kizárólag a központi hatóságok megfelelően felhatalmazott személyzete számára biztosítható. A hozzáférésnek az (1) bekezdésben említett céllal összhangban álló feladatok elvégzéséhez szükséges mértékre kell korlátozódnia, és a kítűzött célok szempontjából szükségesnek és arányosnak kell lennie.

## 25. cikk

**A hozzáféréshez, a helyesbítéshez, a törléshez és az adatkezelés korlátozásához való jog**

- (1) Harmadik országbeli állampolgárok az alkalmazandó uniós adatvédelmi szabályokban meghatározott, a személyes adatokhoz való hozzáférés jogával, és a személyes adatok helyesbítéséhez és törléséhez, valamint a személyesadat-kezelés korlátozásához való joggal kapcsolatos kérelmeit bármely tagállam központi hatóságához lehet címezni.
- (2) Ha a kérelmet az ítélelhozatal szerinti tagállamtól eltérő tagállamhoz nyújtották be, az a tagállam amelyhez a kérelmet benyújtották indokolatlan késedelem nélkül, de minden esetben a kérelem kézhezvételét követő 10 munkanapon belül továbbítja azt az ítélelhozatal szerinti tagállamnak. A kérelem kézhezvételét követően az ítélelhozatal szerinti tagállam:
- azonnal elindítja az érintett adatok pontosságának vagy az azok ECRIS-TCN-ben való jogszerű kezelésének ellenőrzésére irányuló eljárást; valamint
  - indokolatlan késedelem nélkül válaszol a kérelmet továbbító tagállamnak.
- (3) Amennyiben az ECRIS-TCN-ben rögzített adatok pontatlanok vagy kezelésük jogellenesen történt, az ítélelhozatal szerinti tagállam a 9. cikkel összhangban helyesbíti vagy törli az adatokat. Az ítélelhozatal szerinti tagállam, illetve adott esetben az a tagállam amelyhez a kérelmet benyújtották indokolatlan késedelem nélkül írásban megerősíti az érintett személynek, hogy intézkedett a rá vonatkozó adatok helyesbítése vagy törlése érdekében. Az ítélelhozatal szerinti tagállam továbbá a megtett intézkedésről indokolatlan késedelem nélkül tájékoztat minden más olyan tagállamot is, amely az ECRIS-TCN-ben végzett lekérdezés eredményeként ítéletre vonatkozó információt kapott.
- (4) Ha az ítélelhozatal szerinti tagállam nem ért egyet azzal, hogy az ECRIS-TCN-ben rögzített adatok pontatlanok vagy azok kezelése jogellenesen történt, e tagállam közigazgatási vagy bírósági határozatot hoz, amely írásbeli magyarázatot nyújt az érintett személynek arról, hogy miért nem kívánja a rá vonatkozó adatokat helyesbíteni vagy törölni. Az ilyen esetekről adott esetben tájékoztatni lehet a nemzeti felügyeleti hatóságot.
- (5) A (4) bekezdés alapján határozatot elfogadó tagállam tájékoztatja továbbá az érintett személyt arról, hogy milyen lépéseket tehet, ha a (4) bekezdésnek megfelelően adott magyarázat számára nem elfogadható. Ez a tájékoztatás kiterjed annak ismertetésére, hogy hogyan lehet keresetet benyújtani vagy panaszt tenni az adott tagállam illetékes hatóságai vagy bíróságai előtt, valamint arra, hogy az adott tagállam nemzeti jogával összhangban – többek között a nemzeti felügyeleti hatóságok részéről – milyen segítség vehető igénybe.

(6) Az (1) bekezdés alapján benyújtott kérelmeknek tartalmazniuk kell az érintett személy személyazonosságának megállapításához szükséges információkat. Ezek az információk kizárólag arra használhatók fel, hogy lehetővé tegyék az (1) bekezdésben említett jogok gyakorlását, és ezt követően azokat haladéktalanul törölni kell.

(7) A (2) bekezdés alkalmazásában, annak a központi hatóságnak, amelyiknek a kérelmet címezték írásbeli dokumentum formájában nyilvántartásba kell vennie a kérelem benyújtásának tényét és azt, hogy a kérelmet hogyan kezelték és melyik hatóságnak továbbították. A központi hatóságnak a nemzeti felügyeleti hatóság kérésére ezt a bejegyzést haladéktalanul az említett nemzeti felügyeleti hatóság rendelkezésére kell bocsátania. A központi hatóságnak és a nemzeti felügyeleti hatóságnak az ilyen bejegyzéseket a létrehozásukat követő három év elteltével törölniük kell.

#### 26. cikk

### Az adatvédelemi jogok tiszteletben tartásának biztosítását célzó együttműködés

(1) A központi hatóságoknak együtt kell működniük egymással a 25. cikkben megállapított jogok tiszteletben tartásának biztosítása érdekében.

(2) Minden tagállamban a nemzeti felügyeleti hatóságnak kérésre tájékoztatást kell nyújtania az érintett személynek arról, hogy az alkalmazandó uniós adatvédelmi szabályokkal összhangban hogyan gyakorolhatja a rá vonatkozó adatok helyesbítéséhez vagy törléséhez való jogát.

(3) E cikk alkalmazásában az adatokat továbbító tagállam nemzeti felügyeleti hatóságának és azon tagállam nemzeti felügyeleti hatóságának, amelyhez a kérelmet benyújtották együtt kell működniük egymással.

#### 27. cikk

### Jogorvoslat

A nemzeti vagy az uniós joggal összhangban minden személy jogosult panaszt tenni és jogorvoslattal élni abban az ítélethozatal szerinti tagállamban, amely megtagadta a 25. cikkben említett, a rá vonatkozó adatokhoz való hozzáférés jogát, vagy az ilyen adatok helyesbítéséhez vagy törléséhez való jogot.

#### 28. cikk

### A nemzeti felügyeleti hatóságok által gyakorolt felügyelet

(1) Minden tagállam biztosítja, hogy az alkalmazandó uniós adatvédelmi szabályok alapján kijelölt nemzeti felügyeleti hatóságok ellenőrizzék az 5. és a 6. cikkben említett személyes adatok érintett tagállam általi kezelésének jogszerűségét, beleértve azoknak az ECRIS-TCN-be és az ECRIS-TCN-ből történő továbbítását is.

(2) A nemzeti felügyeleti hatóság biztosítja, hogy az ECRIS-TCN működése megkezdésének időpontjától kezdve legalább háromévente elvégezzék a nemzeti bünyügyi nyilvántartásokban és ujjnyomat-adatbázisokban végzett adatkezelési műveleteknek az e rendszerek és az ECRIS-TCN közötti adatcserével kapcsolatos, a vonatkozó nemzetközi auditálási standardok szerinti auditálását.

(3) A tagállamok biztosítják, hogy nemzeti felügyeleti hatóságaik rendelkezzenek az e rendelet alapján rájuk ruházott feladatok ellátásához szükséges erőforrásokkal.

(4) Minden tagállam nemzeti felügyeleti hatóságai rendelkezésére bocsátja az általuk kért információkat, különösen a 12., a 13. és a 19. cikkkel összhangban folytatott tevékenységekre vonatkozó információkat. Minden tagállam biztosítja nemzeti felügyeleti hatóságai számára a nyilvántartásaihoz való hozzáférést a 25. cikk (7) bekezdése, és a naplóihoz való hozzáférést a 31. cikk (6) bekezdése alapján, valamint mindenkor lehetővé teszi számukra az ECRIS-TCN-nel kapcsolatos létesítményekbe történő bejutást.

#### 29. cikk

### Az európai adatvédelmi biztos által gyakorolt felügyelet

(1) Az európai adatvédelmi biztos figyelemmel kíséri, hogy az eu-LISA e rendelettel összhangban végzi-e az ECRIS-TCN-nel kapcsolatos személyes adat-kezelési tevékenységeit.

(2) Az európai adatvédelmi biztos biztosítja, hogy az eu-LISA által végzett személyesadat-kezelési tevékenységek auditálását a vonatkozó nemzetközi auditálási standardoknak megfelelően legalább háromévente elvégezzék. Az auditról szóló jelentést meg kell küldeni az Európai Parlamentnek, a Tanácsnak, a Bizottságnak, az eu-LISA-nak és a felügyeleti hatóságoknak. A jelentés elfogadása előtt az eu-LISA számára lehetőséget kell biztosítani arra, hogy észrevételeket tegyen.

(3) Az eu-LISA az európai adatvédelmi biztos rendelkezésére bocsátja az általa kért információkat, hozzáférést biztosít számára minden dokumentumhoz és a 31. cikkben említett naplóihoz, valamint mindenkor lehetővé teszi számára az eu-LISA összes létesítményébe történő bejutást.

### 30. cikk

#### **Együttműködés a nemzeti felügyeleti hatóságok és az európai adatvédelmi biztos között**

Az ECRIS-TCN koordinált felügyeletét az (EU) 2018/1725 rendelet 62. cikkével összhangban kell biztosítani.

### 31. cikk

#### **Naplózási kötelezettség**

(1) Az eu-LISA és az illetékes hatóságok – saját feladatkörükön belül – biztosítják, hogy az ECRIS-TCN-ben végzett összes adatkezelési műveletet a (2) bekezdéssel összhangban naplózzák a kérelmek elfogadhatóságának ellenőrzése, az adatok sérthetlenségének és biztonságának, valamint az adatkezelés jogszerűségének ellenőrzése, továbbá önellenőrzés céljából.

(2) A naplónak a következőket kell tartalmaznia:

- a) az ECRIS-TCN adataihoz való hozzáférés iránti kérelem célja;
- b) az 5. cikkben említettek szerint továbbított adatok;
- c) a nemzeti ügyiratszám;
- d) a művelet dátuma és pontos időpontja;
- e) a lekérdezéshez használt adatok;
- f) a keresést végrehajtó tisztviselő azonosítója.

(3) A betekintésre és a közlésre vonatkozó naplók lehetővé kell, hogy tegyék e műveletek indokoltságának megállapítását.

(4) A naplók kizárólag az adatkezelés jogszerűségének ellenőrzésére, valamint az adatok sértetlenségének és biztonságának biztosítására használhatók fel. A 36. cikkben említett ellenőrzés és értékelés céljából kizárólag személyes adatot nem tartalmazó naplók használhatók fel. Az említett naplókat megfelelő intézkedésekkel védeni kell a jogosulatlan hozzáféréstől, és három év elteltével – ha már nincs rájuk szükség a megkezdett ellenőrzési eljárásokhoz – törölni kell azokat.

(5) Kérésre az eu-LISA indokolatlan késedelem nélkül a központi hatóságok rendelkezésére bocsátja adatkezelési műveleteinek naplóit.

(6) A kérelmek elfogadhatóságának ellenőrzéséért, valamint az adatkezelés jogszerűségének és az adatok sértetlenségének és biztonságának ellenőrzéséért felelős illetékes nemzeti felügyeleti hatóságok számára kérésükre feladataik ellátása céljából hozzáférést kell biztosítani a naplókhoz. Kérésre a központi hatóságoknak adatkezelési műveleteik naplóit indokolatlan késedelem nélkül az illetékes nemzeti felügyeleti hatóságok rendelkezésére kell bocsátaniuk.

## VI. FEJEZET

### **Záró rendelkezések**

### 32. cikk

#### **Az adatok jelentésekhez és statisztikákhoz történő felhasználása**

(1) Az eu-LISA, az illetékes hatóságok és a Bizottság megfelelően felhatalmazott személyzete számára kizárólag jelentések és statisztikák összeállítása céljából, az egyéni személyazonosítás lehetősége nélkül hozzáférést kell biztosítani az ECRIS-TCN-ben kezelt adatokhoz.

(2) Az (1) bekezdés alkalmazásában az eu-LISA létrehoz, bevezet és műszaki telephelyein elhelyez egy olyan, az (1) bekezdésben említett adatokat tartalmazó központi adattárat, amely az egyéni személyazonosítás lehetősége nélkül lehetővé teszi igényre szabható jelentések és statisztikák elkészítését. A központi adattárhoz biztonságos és ellenőrzött módon, egyedi felhasználói profilokkal, kizárólag jelentések és statisztikák elkészítése céljából lehet hozzáférni.

(3) Az eu-LISA által az ECRIS-TCN, valamint az ECRIS referenciaalkalmazás működésének a 36. cikkben említett ellenőrzése érdekében bevezetett eljárások keretében lehetővé kell tenni statisztikák rendszeres időközönként, nyomkövetési céllal történő készítését is.

Az eu-LISA havonta statisztikákat nyújt be a Bizottságnak a bűnügyi nyilvántartásokból származó információknak az ECRIS-TCN-en és az ECRIS referenciaalkalmazáson keresztül történő rögzítéséről, tárolásáról és cseréjéről. Az eu-LISA biztosítja, hogy az említett statisztikák alapján ne legyen lehetséges az egyének azonosítása. Az eu-LISA a Bizottság kérésére az e rendelet végrehajtásához kapcsolódó konkrét szempontok alapján készített statisztikákat bocsát a Bizottság rendelkezésére.

(4) A tagállamok benyújtják az eu-LISA-nak az e cikkben említett kötelezettségeik teljesítéséhez szükséges statisztikákat. Statisztikákat szolgáltatnak a Bizottságnak az elítélt harmadik országbeli állampolgárok számáról, valamint a területükön harmadik országbeli állampolgárokkal szemben hozott ítéletek számáról.

### 33. cikk

#### Költségek

(1) A központi rendszer, a 4. cikk (1) bekezdésének d) pontjában említett kommunikációs infrastruktúra, az interfész szoftver és az ECRIS referenciaalkalmazás létrehozásával és működtetésével kapcsolatban felmerülő költségeket az Unió általános költségvetéséből kell fedezni.

(2) Az Eurojustnak, az Europolnak és az Európai Ügyészségnek az ECRIS-TCN-hez való kapcsolódásával kapcsolatos költségeket e szervek költségvetéséből kell fedezni.

(3) A többi költséget a tagállamok viselik, különös tekintettel a meglévő nemzeti bűnügyi nyilvántartásoknak, ujjnyomat-adatbázisoknak és a központi hatóságoknak az ECRIS-TCN-hez való kapcsolódásával kapcsolatban felmerülő költségekre, valamint az ECRIS referenciaalkalmazás elhelyezésének költségeire.

### 34. cikk

#### Értesítések

(1) Minden tagállam értesíti az eu-LISA-t arról, hogy mely központi hatósága rendelkezik vagy mely központi hatóságai rendelkeznek hozzáféréssel az adatok feltöltése, helyesbítése, törlése, lekérdezése vagy az adatokba való betekintés céljából, valamint az ezzel kapcsolatos bármely változásról.

(2) Az eu-LISA biztosítja, hogy a tagállamok által az értesítésben megadott központi hatóságok jegyzékét közzétegyék az *Európai Unió Hivatalos Lapjában* és az eu-LISA honlapján. Ha az eu-LISA tagállami központi hatóságot érintő változással kapcsolatos értesítést kap, indokolatlan késedelem nélkül aktualizálja a jegyzéket.

### 35. cikk

#### Adatfeltöltés és a működés megkezdése

(1) Miután a Bizottság meggyőződött az alábbi feltételek teljesüléséről, meghatározza azt az időpontot, amelytől a tagállamok megkezdik az 5. cikkben említett adatok feltöltését az ECRIS-TCN-be:

- a) elfogadták a 10. cikkben említett vonatkozó végrehajtási jogi aktusokat;
- b) a tagállamok jóváhagyták az 5. cikkben említett adatok gyűjtésére és az ECRIS-TCN-be történő továbbítására szolgáló műszaki és jogi kereteket, és értesítették azokról a Bizottságot;
- c) az eu-LISA a tagállamokkal együttműködve, anonimizált tesztadatokat felhasználva elvégezte az ECRIS-TCN átfogó tesztelését.

(2) Ha a Bizottság az (1) bekezdéssel összhangban meghatározta az adatfeltöltés kezdő időpontját, tájékoztatja erről az időpontról a tagállamokat. Az ezen időpontot követő két hónapon belül a tagállamok a 41. cikk (2) bekezdését figyelembe véve feltöltik az 5. cikkben említett adatokat az ECRIS-TCN-be.

- (3) A (2) bekezdésben említett időtartam lejártát követően az eu-LISA a tagállamokkal együttműködve elvégzi az ECRIS-TCN végső tesztelését.
- (4) Ha sikeresen befejeződött a (3) bekezdésben említett tesztelés, és az eu-LISA úgy ítéli meg, hogy az ECRIS-TCN működésre kész, értesíti erről a Bizottságot. A Bizottság tájékoztatja az Európai Parlamentet és a Tanácsot a tesztelés eredményeiről, és határoz arról az időpontról, amelytől az ECRIS-TCN-nek kell kezdenie a működését.
- (5) Az ECRIS-TCN működésének kezdő időpontjáról szóló, a (4) bekezdésben említett bizottsági határozatot ki kell hirdetni az *Európai Unió Hivatalos Lapjában*.
- (6) A tagállamok a (4) bekezdéssel összhangban a Bizottság által meghatározott időponttól megkezdik az ECRIS-TCN használatát.
- (7) Az e cikkben említett határozatok meghozatalakor a Bizottság eltérő időpontokat határozhat meg az 5. cikkben említett alfanumerikus adatok és ujjnyomatadatok ECRIS-TCN-be való feltöltésére, valamint ezen különböző adatkategóriák tekintetében a működés megkezdésére vonatkozóan.

### 36. cikk

#### Ellenőrzés és értékelés

- (1) Az eu-LISA biztosítja a tervezéssel és a költségekkel kapcsolatos célok fényében az ECRIS-TCN kifejlesztésének ellenőrzésére, valamint a technikai eredményekkel, a költséghatékonysággal, a biztonsággal és a szolgáltatás minőségével kapcsolatos célok fényében az ECRIS-TCN és az ECRIS referenciaalkalmazás működésének ellenőrzésére irányuló eljárások meglétét.
- (2) Az ECRIS-TCN működésének ellenőrzése és műszaki karbantartása céljából az eu-LISA hozzáféréssel rendelkezik az ECRIS-TCN-ben és az ECRIS referenciaalkalmazásban végzett adatkezelési műveletekkel kapcsolatos szükséges információkhoz.
- (3) 2019. december 12-ig, majd azt követően a tervezési és kifejlesztési szakasz során hathavonta, az eu-LISA jelentést nyújt be az Európai Parlamentnek és a Tanácsnak az ECRIS-TCN és az ECRIS referenciaalkalmazás kifejlesztésének helyzetéről.
- (4) A (3) bekezdésben említett jelentésnek tartalmaznia kell a felmerült költségek és a projekt előrehaladásának áttekintését, pénzügyi hatásvizsgálatot, valamint tájékoztatást minden olyan műszaki problémáról és kockázatról, amely befolyásolhatja az ECRIS-TCN-nek a 33. cikkel összhangban az Unió általános költségvetéséből fedezendő valamennyi költségét.
- (5) A kifejlesztési folyamat bármely jelentős késedelmére esetén az eu-LISA az Európai Parlamentet és a Tanácsot a lehető leghamarabb tájékoztatja a késedelem okairól, valamint annak időbeli és pénzügyi következményeiről.
- (6) Az ECRIS-TCN és az ECRIS referenciaalkalmazás kifejlesztésének lezárultát követően az eu-LISA jelentést nyújt be az Európai Parlamentnek és a Tanácsnak, amely ismerteti – különösen a tervezéssel és a költségekkel kapcsolatos – célok megvalósításának mikéntjét és az esetleges eltérések indokait.
- (7) Az ECRIS-TCN esetlegesen komoly költségekkel járó műszaki korszerűsítése esetén az eu-LISA tájékoztatja az Európai Parlamentet és a Tanácsot.
- (8) Két évvel az ECRIS-TCN működésének megkezdése után, majd azt követően évente, az eu-LISA – különösen az ECRIS-TCN működésére és használatára, valamint a bünyügyi nyilvántartásokból származó információknak az ECRIS referenciaalkalmazás útján történő cseréjére vonatkozó statisztikák alapján – jelentést nyújt be a Bizottságnak az ECRIS-TCN és az ECRIS referenciaalkalmazás műszaki működéséről, beleértve azok biztonságosságát is.
- (9) Négy évvel az ECRIS-TCN működésének megkezdése után, majd azt követően négyévente a Bizottság elvégzi az ECRIS-TCN és az ECRIS referenciaalkalmazás átfogó értékelését. Az ennek alapján készült átfogó értékelő jelentésnek ki kell terjednie e rendelet alkalmazásának értékelésére és az elért eredményeknek a kitűzött célok fényében történő vizsgálatára, valamint az alapvető jogokra gyakorolt hatásra. A jelentésben ki kell térni annak értékelésére is, hogy az ECRIS-TCN működtetésének alapjául szolgáló megfontolások változatlanul helytállóak-e, hogy az ECRIS-TCN céljaira megfelelő-e a biometrikus adatok felhasználása, továbbá az ECRIS-TCN biztonságosságának és a majdani műveletek biztonsági vonzatának értékelésére. Az értékelés szükség esetén ajánlásokat is tartalmaz. A Bizottság továbbítja a jelentést az Európai Parlamentnek, a Tanácsnak, az európai adatvédelmi biztosnak és az Európai Unió Alapjogi Ügynökségének.

(10) Ezenkívül a (9) bekezdésben említett első átfogó értékelésnek tartalmaznia kell az alábbiak értékelését:

- a) a vonatkozó statisztikai adatok és a tagállamoktól származó további információk alapján milyen mértékben járult hozzá e rendelet céljainak eléréséhez az, hogy az ECRIS-TCN tartalmazza azoknak az uniós polgároknak a személyazonosító adatait, akik valamely harmadik ország állampolgárságával is rendelkeznek;
- b) egyes tagállamok továbbra is használhassák-e a 4. cikkben említett nemzeti ECRIS alkalmazási szoftvert;
- c) az ECRIS-TCN-be történő ujjnyomatadat-feltöltés, különösen ami az 5. cikk (1) bekezdése b) pontjának ii. alpontjában említett minimumkövetelmények alkalmazását illeti;
- d) az ECRIS és az ECRIS-TCN hatása a személyes adatok védelmére.

Az értékelést szükség esetén jogalkotási javaslatok kísérhetik. Az ezt követő átfogó értékelések e szempontok egyikének vagy mindegyikének értékelését is tartalmazhatják.

(11) A tagállamok, az Eurojust, az Europol és az Európai Ügyészség az eu-LISA és a Bizottság rendelkezésére bocsátják a (3), a (8) és a (9) bekezdésben említett jelentések elkészítéséhez szükséges információkat, a Bizottság vagy az eu-LISA, vagy a mindkettő által előzetesen meghatározott mennyiségi mutatókkal összhangban. Ezek az információk nem veszélyeztethetik a munkamódszereket, és nem tartalmazhatnak az információforrásokat, a személyzet tagjait, illetve a nyomozásokat felfedő információt.

(12) A felügyeleti hatóságok adott esetben az eu-LISA és a Bizottság rendelkezésére bocsátják a (9) bekezdésben említett jelentések elkészítéséhez szükséges információkat, a Bizottság vagy az eu-LISA, vagy a mindkettő által előzetesen meghatározott mennyiségi mutatókkal összhangban. Ezek az információk nem veszélyeztethetik a munkamódszereket, és nem tartalmazhatnak az információforrásokat, a személyzet tagjait, illetve a nyomozásokat felfedő információt.

(13) Az eu-LISA a Bizottság rendelkezésére bocsátja a (9) bekezdésben említett átfogó értékelések elkészítéséhez szükséges információkat.

### 37. cikk

#### A felhatalmazás gyakorlása

(1) A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozóan a Bizottság részére adott felhatalmazás feltételeit ez a cikk határozza meg.

(2) A Bizottságnak a 6. cikk (2) bekezdésében említett, felhatalmazáson alapuló jogi aktusok elfogadására vonatkozó felhatalmazása határozatlan időre szól 2019. június 11-től kezdődő hatállyal.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 6. cikk (2) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon, vagy a benne megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(4) A felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban foglalt elveknek megfelelően konzultál az egyes tagállamok által kijelölt szakértőkkel.

(5) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

(6) A 6. cikk (2) bekezdése értelmében elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő két hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam két hónappal meghosszabbodik.

### 38. cikk

#### A bizottsági eljárás

(1) A Bizottságot egy bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.



(2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikkét kell alkalmazni.

Ha a bizottság nem nyilvánít véleményt, a Bizottság nem fogadhatja el a végrehajtási jogi aktus tervezetét, és a 182/2011/EU rendelet 5. cikke (4) bekezdésének harmadik albekezdése alkalmazandó.

### 39. cikk

#### Tanácsadó csoport

Az eu-LISA tanácsadó csoportot hoz létre az ECRIS-TCN-nel és az ECRIS referenciaalkalmazással kapcsolatos – különösen az eu-LISA éves munkaprogramjának és éves tevékenységi jelentésének elkészítésével összefüggő – szakértelem biztosítása érdekében. A tervezési és kifejlesztési szakaszban a 11. cikk (9) bekezdését kell alkalmazni.

### 40. cikk

#### Az (EU) 2018/1726 rendelet módosítása

Az (EU) 2018/1726 rendelet a következőképpen módosul:

1. Az 1. cikk (4) bekezdése helyébe a következő szöveg lép:

„(4) Az ügynökség felelős a határregisztrációs rendszer (EES), a DubliNet, az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS), az ECRIS-TCN és az ECRIS referenciaalkalmazás előkészítéséért, kifejlesztéséért és üzemeltetési igazgatásáért.”

2. A rendelet a következő cikkel egészül ki:

„8a. cikk

#### Az ECRIS-TCN-nel és az ECRIS referenciaalkalmazással kapcsolatos feladatok

Az ECRIS-TCN-nel és az ECRIS referenciaalkalmazással kapcsolatban az ügynökség ellátja:

- az (EU) 2019/816 európai parlamenti és tanácsi rendelettel (\*) ráruházott feladatokat;
- az ECRIS-TCN és az ECRIS referenciaalkalmazás technikai használatára vonatkozó képzéssel kapcsolatos feladatokat.

(\*) Az Európai Parlament és a Tanács (EU) 2019/816 rendelete (2019. április 17.) az Európai Bűnügyi Nyilvántartási Információs Rendszer kiegészítése érdekében a harmadik országbeli állampolgárokkal és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval rendelkező tagállamok azonosítására szolgáló központosított rendszer (ECRIS-TCN) létrehozásáról, valamint az (EU) 2018/1726 rendelet módosításáról (HL L 135., 2019.5.22., 1. o.).”

3. A 14. cikk (1) bekezdése helyébe a következő szöveg lép:

„(1) Az ügynökség nyomon követi a SIS II, a VIS, az Eurodac, az EES, az ETIAS, a DubliNet, az ECRIS-TCN és az 1. cikk (5) bekezdésében említett eltérő nagyméretű IT-rendszerek üzemeltetési igazgatása szempontjából fontos kutatási fejleményeket.”

4. A 19. cikk (1) bekezdése a következőképpen módosul:

a) az ee) pont helyébe a következő szöveg lép:

„ee) az (EU) 2017/2226 rendelet 72. cikkének (2) bekezdése alapján elfogadja az EES fejlesztéséről szóló jelentéseket, az (EU) 2018/1240 rendelet 92. cikkének (2) bekezdése alapján elfogadja az ETIAS fejlesztéséről szóló jelentéseket, valamint az (EU) 2019/816 rendelet 36. cikkének (3) bekezdése alapján elfogadja az ECRIS-TCN és az ECRIS referenciaalkalmazás kifejlesztéséről szóló jelentéseket.”;

b) az ff) pont helyébe a következő szöveg lép:

„ff) elfogadja az 1987/2006/EK rendelet 50. cikkének (4) bekezdése és a 2007/533/IB határozat 66. cikkének (4) bekezdése alapján a SIS II, a 767/2008/EK rendelet 50. cikkének (3) bekezdése és a 2008/633/IB határozat 17. cikkének (3) bekezdése alapján a VIS, az (EU) 2017/2226 rendelet 72. cikkének (4) bekezdése alapján az EES, az (EU) 2018/1240 rendelet 92. cikkének (4) bekezdése alapján az ETIAS, valamint az (EU) 2019/816 rendelet 36. cikkének (8) bekezdése alapján az ECRIS-TCN és az ECRIS referenciaalkalmazás technikai működéséről készített jelentéseket.”

c) a hh) pont helyébe a következő szöveg lép:

„hh) hivatalos észrevételeket fogad el az európai adatvédelmi biztosnak az 1987/2006/EK rendelet 45. cikkének (2) bekezdése, a 767/2008/EK rendelet 42. cikkének (2) bekezdése, a 603/2013/EU rendelet 31. cikkének (2) bekezdése, az (EU) 2017/2226 rendelet 56. cikkének (2) bekezdése, az (EU) 2018/1240 rendelet 67. cikke, és az (EU) 2019/816 rendelet 29. cikkének (2) bekezdése alapján végzett auditokról szóló jelentései kapcsán, valamint biztosítja ezen auditok megfelelő nyomon követését;”

d) a szöveg a következő ponttal egészül ki:

„(lla) statisztikákat nyújt be a Bizottságnak az ECRIS-TCN-ről és az ECRIS referenciaalkalmazásról az (EU) 2019/816 rendelet 32. cikke (4) bekezdésének második albekezdése alapján;”

e) az mm) pont helyébe a következő szöveg lép:

„mm) gondoskodik arról, hogy évente közzétegyék azoknak az illetékes hatóságoknak az 1987/2006/EK rendelet 31. cikkének (8) bekezdése és a 2007/533/IB határozat 46. cikkének (8) bekezdése szerinti jegyzékét, amelyek jogosultak a SIS II-ben található adatok közvetlen lekérdezésére, a SIS II nemzeti rendszereihez tartozó hivataloknak (N.SIS II hivatalok) és a SIRENE-irodáknak az 1987/2006/EK rendelet 7. cikkének (3) bekezdése és a 2007/533/IB határozat 7. cikkének (3) bekezdése szerinti jegyzékével, valamint az illetékes hatóságoknak az (EU) 2017/2226 rendelet 65. cikkének (2) bekezdése szerinti jegyzékével, az illetékes hatóságoknak az (EU) 2018/1240 rendelet 87. cikkének (2) bekezdése szerinti jegyzékével, továbbá a központi hatóságoknak az (EU) 2019/816 rendelet 34. cikkének (2) bekezdése szerinti jegyzékével együtt;”

5. A 22. cikk (4) bekezdése a harmadik albekezdés után a következő albekezdéssel egészül ki:

„Az Eurojust, az Europol és az Európai Ügyészség megfigyelőként részt vehet az igazgatótanács ülésein, amikor az (EU) 2019/816 rendelet alkalmazásával kapcsolatos, az ECRIS-TCN-t érintő kérdés van napirenden.”

6. A 24. cikk (3) bekezdésének p) pontja helyébe a következő szöveg lép:

„p) a tisztviselők személyzeti szabályzata 17. cikkének sérelme nélkül a titoktartási követelmények megállapítása az 1987/2006/EK rendelet 17. cikkének, a 2007/533/IB határozat 17. cikkének, a 767/2008/EK rendelet 26. cikke (9) bekezdésének, a 603/2013/EU rendelet 4. cikke (4) bekezdésének, az (EU) 2017/2226 rendelet 37. cikke (4) bekezdésének, az (EU) 2018/1240 rendelet 74. cikke (2) bekezdésének, és az (EU) 2019/816 rendelet 11. cikke (16) bekezdésének való megfelelés érdekében.”

(7) A 27. cikk (1) bekezdése a következő ponttal egészül ki:

„da) az ECRIS-TCN-nel foglalkozó tanácsadó csoport;”

#### 41. cikk

### Végrehajtás és átmeneti rendelkezések

(1) A tagállamok meghozzák azokat az intézkedéseket, amelyek szükségesek ahhoz, hogy ennek a rendeletnek – az ECRIS-TCN megfelelő működésének biztosítása érdekében – a lehető leghamarabb megfeleljenek.

(2) Az adatfeltöltésnek a 35. cikk (1) bekezdésével összhangban meghatározott kezdő időpontja előtt hozott ítéletek esetében a központi hatóságoknak az alábbiak szerint kell létrehozniuk a központi rendszerben az egyéni adatrecordokat:

a) az alfanumerikus adatokat a 35. cikk (2) bekezdésében említett időtartam végéig kell feltölteni a központi rendszerbe;

b) az ujjnyomatadatokat a működés 35. cikk (4) bekezdésével összhangban történő megkezdését követő két éven belül kell feltölteni a központi rendszerbe.

#### 42. cikk

### Hatálybalépés

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet a Szerződéseknek megfelelően teljes egészében kötelező és közvetlenül alkalmazandó a tagállamokban.

Kelt Strasbourgban, 2019. április 17-én.

*az Európai Parlament részéről*

*az elnök*

A. TAJANI

*a Tanács részéről*

*az elnök*

G. CIAMBA

---

## MELLÉKLET

**AZ (EU) 2019/816 RENDELET 17. CIKKÉNEK (1) BEKEZDÉSÉBEN EMLÍTETT EGYSÉGES FORMANYOMTATVÁNY INFORMÁCIÓ IRÁNTI MEGKERESÉSHEZ, ARRÁ IRÁNYULÓAN, HOGY – HA VANNAK ILYEN TAGÁLLAMOK – MELY TAGÁLLAMOK RENDELKEZNEK BŰNÜGYI NYILVÁNTARTÁSI INFORMÁCIÓKKAL AZ ÉRINTETT HARMADIK ORSZÁGBELI ÁLLAMPOLGÁRRA VONATKOZÓAN**

A formanyomtatványt, amely a [www.eurojust.europa.eu](http://www.eurojust.europa.eu) honlapon az Unió intézményeinek mind a 24 hivatalos nyelvén rendelkezésre áll, ezen nyelvek egyikén kell az [ECRIS-TCN@eurojust.europa.eu](mailto:ECRIS-TCN@eurojust.europa.eu) e-mail címre küldeni.

A megkereső állam vagy nemzetközi szervezet:

Az állam vagy a nemzetközi szervezet neve:

A megkeresést benyújtó hatóság:

Képviseli (a személy neve):

Beosztás:

Cím:

Telefonszám:

E-mail cím:

Büntetőeljárás, amelyhez az információt kéri:

Belföldi ügyiratszám:

Illetékes hatóság:

A nyomozás tárgyát képező bűncselekmények típusa (kérjük, adja meg a büntető törvénykönyv vonatkozó cikkét/cikkeit):

Egyéb releváns információ (pl. a megkeresés sürgőssége):

A harmadik ország állampolgárságával rendelkező azon személy személyazonosító adatai, akivel kapcsolatban az ítélethozatal szerinti tagállamra vonatkozóan információt kérnek:

NB.: kérjük, lehetőség szerint adjon meg minél több rendelkezésre álló információt.

Vezetéknév (családi név):

Utónév/utónevek (keresztnevek):

Születési idő:

Születési hely (város és ország):

Állampolgárság vagy állampolgárságok:

Nem:

Korábbi név/nevek (adott esetben):

Szülők neve:

Személyazonosító szám:

A személyazonosító okmány(ok) típusa és száma:

Az okmány(oka)t kiállító hatóság:

Álnevek vagy felvett nevek:

Kérjük, küldje meg az ujjnyomatadatokat is, ha rendelkezésre állnak.

*Több személy esetén kérjük, külön-külön tüntesse fel őket.*

A legördülő panel segítségével további érintett személyek is bevitethők

Kelt

...-án/-én

(Elektronikus) aláírás és bélyegző:

**AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/817 RENDELETE****(2019. május 20.)**

**az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízumügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról**

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen 16. cikkének (2) bekezdésére, 74. cikkére, valamint 77. cikke (2) bekezdésének a), b), d) és e) pontjára,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére <sup>(1)</sup>,

a Régiók Bizottságával folytatott konzultációt követően,

rendes jogalkotási eljárás keretében <sup>(2)</sup>,

mivel:

- (1) „A határigazgatás és a biztonság erősítését szolgáló, szilárd és intelligens információs rendszerek” című, 2016. április 6-i közleményében a Bizottság hangsúlyozta, hogy javítani kell az uniós adatkezelés keretét a határ- és biztonsági ellenőrzés területén. A közlemény az uniós határigazgatási, biztonsági, és migrációkezelési információs rendszerek közötti interoperabilitás megteremtésére irányuló folyamatot kezdeményezett az e rendszerekkel kapcsolatos, a nemzeti hatóságok munkáját akadályozó strukturális hiányosságok kezelése, valamint annak biztosítása céljából, hogy a határőrök, a vámhatóságok, a rendőrtisztek és az igazságügyi hatóságok rendelkezzenek a szükséges információkkal.
- (2) Az „Ütemterv a bel- és igazságügyi területen alkalmazott információcseré és információkezelés javítására, beleértve az interoperabilitást biztosító megoldásokat is” című, 2016. június 6-i dokumentumban a Tanács számos jogi, műszaki és operatív kihívást azonosított az uniós információs rendszerek interoperabilitása terén, és megoldások keresését sürgette.
- (3) A 2017. évi bizottsági munkaprogrammal kapcsolatos stratégiai prioritásokról szóló, 2016. július 6-i állásfoglalásában <sup>(3)</sup> az Európai Parlament javaslatokat terjesztett elő a meglévő uniós információs rendszerek javítására és fejlesztésére, az információs hiányosságok kezelésére, az interoperabilitás előmozdítására, valamint az információk kötelező uniós szintű megosztására, amelyet megfelelő adatvédelmi biztosítékok kísérnek.
- (4) Az Európai Tanács 2016. december 15-i következtetéseiben az uniós információs rendszerek és adatbázisok interoperabilitása terén további eredmények elérése érdekében a munka folytatását sürgette.
- (5) Az információs rendszerekkel és az interoperabilitással foglalkozó magas szintű szakértői csoport 2017. május 11-i zárójelentésében arra a következtetésre jutott, hogy az interoperabilitáshoz vezető gyakorlati megoldások irányába való elmozdulás szükséges és technikailag megvalósítható, és hogy az interoperabilitás elvileg működési előnyökkel járhat és az adatvédelmi követelményeknek eleget téve megvalósítható.

<sup>(1)</sup> HL C 283., 2018.8.10., 48. o.

<sup>(2)</sup> Az Európai Parlament 2019. április 16-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2019. május 14-i határozata.

<sup>(3)</sup> HL C 101., 2018.3.16., 116. o.

- (6) A „Hetedik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról” című, 2017. május 16-i közleményében a Bizottság – 2016. április 6-i közleményével, valamint az információs rendszerekkel és az interoperabilitással foglalkozó magas szintű szakértői csoport megállapításaival és ajánlásaival összhangban – új megközelítésbe helyezte az adatkezelést a határigazgatás, a biztonság és a migráció terén, amelynek értelmében a biztonság, a határigazgatás és a migrációkezelés terén használt valamennyi uniós információs rendszer interoperabilis módon, az alapvető jogok maradéktalan tiszteletben tartásával működik.
- (7) Az információcsere javítását és az uniós információs rendszerek interoperabilitásának biztosítását célzó további lépésekről szóló, 2017. június 9-i következtetéseiben a Tanács felkérte a Bizottságot, hogy valósítsa meg a magas szintű szakértői csoport által az interoperabilitás biztosítása érdekében javasolt megoldásokat.
- (8) Az Európai Tanács 2017. június 23-i következtetéseiben hangsúlyozta az adatbázisok közötti interoperabilitás javításának szükségességét, és felkérte a Bizottságot, hogy a lehető legrövidebb időn belül dolgozzon ki jogszabálytervezeteket az információs rendszerekkel és az interoperabilitással foglalkozó magas szintű szakértői csoport javaslatai alapján.
- (9) A külső határokon végzett határellenőrzések hatékonyságának és eredményességének javítása, az illegális bevándorlás megelőzéséhez és az ellene vívott küzdelemhez való hozzájárulás, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló uniós térség magas szintű biztonságának elősegítése – beleértve a közbiztonság és a közrend fenntartását, valamint a tagállamok területén a biztonság védelmét –, a közös vízümpolitika végrehajtásának javítása, a nemzetközi védelem iránti kérelmek vizsgálatának elősegítése, a terrorista bűncselekmények és egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez és nyomozásához való hozzájárulás, a személyazonosságukat igazolni nem tudó ismeretlen személyek vagy a természeti katasztrófák, balesetek vagy terrortámadások esetében az azonosítatlan emberi maradványok azonosításának elősegítése céljából, az uniós migrációs és menekültügyi rendszerbe, az uniós biztonsági intézkedésekbe és az Unió külső határainak igazgatására vonatkozó képességébe vetett közbizalom fenntartása érdekében meg kell valósítani az uniós információs rendszerek, azaz a határregisztrációs rendszer („Entry/Exit System”, a továbbiakban: EES), a Vízüminformációs Rendszer („Visa Information System”, a továbbiakban: VIS), az Európai Utasinformációs és Engedélyezési Rendszer („European Travel Information and Authorisation System”, a továbbiakban: ETIAS), az Eurodac, a Schengeni Információs Rendszer („Schengen Information System”, a továbbiakban: SIS), valamint a harmadik országok állampolgáira vonatkozó Európai Bűnügyi Nyilvántartási Információs Rendszer („European Criminal Records Information System for Third-Country Nationals”, a továbbiakban: ECRIS-TCN) interoperabilitását, hogy ezek az uniós információs rendszerek és az azokban található adatok kiegészítsék egymást, tiszteletben tartva ugyanakkor az egyének alapvető jogait és különösen a személyes adatok védelméhez való jogot. Ehhez létre kell hozni – interoperabilitási elemekként – az európai keresőportált („European search portal”, a továbbiakban: ESP), a közös biometrikus megfeleltetési szolgáltatást („shared biometric matching service”, a továbbiakban: közös BMS), a közös személyazonosítótárakat („common identity repository”, a továbbiakban: CIR) és a többszörös személyazonosságot felismerő rendszert („multiple-identity detector”, a továbbiakban: MID).
- (10) Az uniós információs rendszerek közötti interoperabilitásnak lehetővé kell tennie, hogy az említett rendszerek kiegészítsék egymást, a személyek – köztük a személyazonosságukat igazolni nem tudó ismeretlen személyek vagy az azonosítatlan emberi maradványok – helyes azonosításának megkönnyítése, a személyazonossággal való visszaélés elleni küzdelemhez való hozzájárulás, az egyes uniós információs rendszerekre vonatkozó adatminőségi követelmények javítása és harmonizálása, az uniós információs rendszerek tagállamok általi műszaki és operatív alkalmazásának megkönnyítése, a vonatkozó uniós információs rendszereket szabályozó adatbiztonsági és adatvédelmi biztosítékok megerősítése, az EES-hez, a VIS-hez, az ETIAS-hoz és az Eurodachoz terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése és nyomozása céljából történő hozzáférés észszerűsítése, valamint az EES, a VIS, az ETIAS, az Eurodac, a SIS és az ECRIS-TCN célkitűzéseinek támogatása érdekében.
- (11) Az interoperabilitási elemeknek az EES-t, a VIS-t, az ETIAS-t, az Eurodacot, a SIS-t és az ECRIS-TCN-t kell lefedniük. Emellett az Europol-adatokat is le kell fedniük, de csak olyan mértékben, hogy az Europol-adatok az említett uniós információs rendszerekkel egyidejűleg lekérdezhetők legyenek.
- (12) Az interoperabilitási elemeknek olyan személyek személyes adatait kell kezelniük, akiknek személyes adatait az alapul szolgáló uniós információs rendszerekben kezelik, vagy az Europol kezeli.
- (13) Az ESP-t annak elősegítése érdekében kell létrehozni, hogy a tagállami hatóságok és az uniós ügynökségek gyors, zökkenőmentes, hatékony, szisztematikus és ellenőrzött módon hozzáférjenek az uniós információs rendszerekhez, az Europol-adatokhoz és a Nemzetközi Bűnügyi Rendőrség Szervezete (Interpol) adatbázisaihoz,

amennyiben ez feladataik hozzáférési jogosultságaikkal összhangban történő ellátásához szükséges. Az ESP-t továbbá annak érdekében is létre kell hozni, hogy támogassa az EES, a VIS, az ETIAS, az Eurodac, a SIS, az ECRIS-TCN és az Europol-adatok célkitűzéseit. Az ESP rendeltetése, hogy valamennyi megfelelő uniós információs rendszer, valamint az Europol-adatok és az Interpol-adatbázisok egyidejű lekérdezésének lehetővé tétele révén egyedüli lekérdezési pontként vagy „üzenetközvetítőként” szolgáljon a különböző központi rendszerek kereséséhez és a szükséges információk zökkenőmentes lehívásához, az alapul szolgáló rendszerek hozzáférési és adatvédelmi követelményeinek teljes körű tiszteletben tartása mellett.

- (14) Az ESP kialakításának biztosítania kell, hogy az Interpol-adatbázisok lekérdezésekor az ESP-felhasználó által a lekérdezés kezdeményezéséhez használt adatok ne kerüljenek megosztásra az Interpol adatainak tulajdonosaival. Az ESP kialakításának azt is biztosítania kell, hogy az Interpol-adatbázisok lekérdezésére kizárólag az alkalmazandó uniós és nemzeti joggal összhangban kerülhessen sor.
- (15) Az Interpol ellopott és elvesztett úti okmányokat tartalmazó adatbázisa (SLTD adatbázis) lehetővé teszi a tagállamokban a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséért, felderítéséért és nyomozásáért felelős, felhatalmazással rendelkező szervezetek, többek között a bevándorlási és a határellenőrző hatóságok számára, hogy az úti okmányok érvényességét megállapítsák. Annak értékelése során, hogy valamely, beutazási engedélyt kérelmező személy esetében fennáll-e például az irreguláris migráció valószínűsége, vagy e személy biztonsági veszélyt jelenthet-e, az ETIAS lekérdezést végez az SLTD adatbázisában és az Interpol-körözésben megjelölt úti okmányok adatbázisában (TDAWN adatbázis). Az ESP-nak lehetővé kell tennie az SLTD és a TDAWN adatbázisok lekérdezését az egyének személyazonosító adatainak vagy útiokmány-adatainak felhasználásával. Amennyiben az Unióból az Interpol részére az ESP-n keresztül továbbítanak személyes adatokat, az (EU) 2016/679 európai parlamenti és tanácsi rendelet <sup>(4)</sup> V. fejezetében szereplő, a nemzetközi adattovábbításokra vonatkozó rendelkezéseket, vagy az (EU) 2016/680 európai parlamenti és tanácsi irányelv <sup>(5)</sup> V. fejezetét átültető nemzeti rendelkezéseket kell alkalmazni. Ez nem érintheti a 2005/69/IB tanácsi közös álláspontban <sup>(6)</sup> és a 2007/533/IB tanácsi határozatban <sup>(7)</sup> meghatározott különös szabályokat.
- (16) Az ESP-t úgy kell kialakítani és konfigurálni, hogy az effajta lekérdezéseket csak a személyekkel vagy úti okmányokkal kapcsolatos azon adatok felhasználásával tegye lehetővé, amelyek szerepelnek valamelyik uniós információs rendszerben, az Europol-adatokban vagy az Interpol-adatbázisokban.
- (17) A megfelelő uniós információs rendszerek szisztematikus használatának biztosítása érdekében az ESP-t kell használni a CIR, az EES, a VIS, az ETIAS, az Eurodac és az ECRIS-TCN lekérdezésére. Továbbra is fenn kell tartani azonban a különböző uniós információs rendszerekhez való nemzeti kapcsolódást tartalékmegoldásként technikai problémák esetére. Az ESP-t az uniós ügynökségeknek is használniuk kell a központi SIS-nek a hozzáférési jogosultságaikkal összhangban és feladataik ellátása érdekében történő lekérdezése céljából. Az ESP további eszközt jelent a központi SIS, az Europol-adatok és az Interpol-adatbázisok lekérdezéséhez, kiegészítve a meglévő célzott interfészeket.
- (18) A biometrikus adatok – például az ujjnyomatok és arcképmások – egyediek, ezért a személyek azonosítása céljából sokkal megbízhatóbbak, mint az alfanumerikus adatok. A közös BMS a megfelelő uniós információs rendszerek és az egyéb interoperabilitási elemek munkájának támogatását és megkönnyítését szolgáló technikai eszköz kell, hogy legyen. A közös BMS fő célja, hogy megkönnyítse a több adatbázisban nyilvántartott személyek azonosítását azáltal, hogy a számos összetevő helyett egyetlen technológiai összetevőt használ az adott személy különböző rendszerekben tárolt biometrikus adatainak összevetéséhez. A közös BMS növeli a biztonságot, valamint pénzügyi, fenntartási és működési előnyökkel jár. Valamennyi automatikus ujjnyomat-azonosító rendszer, beleértve az Eurodachoz, a VIS-hez és a SIS-hez jelenleg használt rendszereket is, valódi biometrikus minták jellemzőinek leképezése útján nyert adatokból összeállított biometrikus sablonokat használ. A közös BMS egyetlen helyszínen gyűjti össze és tárolja az összes ilyen biometrikus sablont – logikailag különválasztva azon információs rendszerek szerint, amelyekből az adatok származnak –, ezáltal megkönnyíti a biometrikus sablonokat használó rendszerek közötti összehasonlításokat, és lehetővé teszi az EU központi rendszereinek méretgazdaságos fejlesztését és fenntartását.

<sup>(4)</sup> Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

<sup>(5)</sup> Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a védeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (HL L 119., 2016.5.4., 89. o.).

<sup>(6)</sup> A Tanács 2005/69/IB közös álláspontja (2005. január 24.) egyes adatoknak az Interpollal történő cseréjéről (HL L 27., 2005.1.29., 61. o.).

<sup>(7)</sup> A Tanács 2007/533/IB határozata (2007. június 12.) a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról (HL L 205., 2007.8.7., 63. o.).

- (19) A közös BMS-ben tárolt biometrikus sablonok a valódi biometrikus minták jellemzőinek leképezése útján nyert adatokból kell, hogy álljanak és azokat úgy kell létrehozni, hogy a kinyerési eljárást fordított irányba ne lehessen végrehajtani. A biometrikus sablonokat biometrikus adatokból kell létrehozni, de oly módon, hogy ugyanazokat a biometrikus adatokat ne lehessen kinyerni a biometrikus sablonokból. Mivel tenyérynymatokra vonatkozó adatokat és DNS-profilokat kizárólag a SIS-ben tárolnak, és azok nem használhatók más információs rendszerekben lévő adatokkal való összehasonlításra, a szükségesség és az arányosság elvével összhangban a közös BMS nem tárolhat DNS-profilokat vagy tenyérynymatokra vonatkozó adatokból létrehozott biometrikus sablonokat.
- (20) A biometrikus adatok különleges személyes adatnak minősülnek. E rendeletben meg kell határozni az ilyen adatok – kizárólag az érintett személyek azonosítása céljából megengedett – kezelésének jogalapját és az arra vonatkozó biztosítékokat.
- (21) Az EES, a VIS, az ETIAS, az Eurodac és az ECRIS-TCN megkívánja azon személyek pontos azonosítását, akiknek személyes adatait e rendszerekben tárolják. A CIR-nek ezért elő kell segítenie az említett rendszerekben nyilvántartott személyek pontos azonosítását.
- (22) Az említett uniós információs rendszerekben tárolt személyes adatok vonatkozhatnak ugyanazokra a személyekre, de eltérő vagy hiányos személyazonosság alapján. A tagállamok hatékony módszerekkel rendelkeznek az állampolgáraik vagy a területükön állandó lakóhellyel rendelkező személyek azonosítására. Az uniós információs rendszerek közötti interoperabilitás hozzájárul az említett rendszerekben szereplő személyek pontosabb azonosításához. A CIR-nek tárolnia kell azon személyes adatokat, amelyek szükségesek azon személyek pontosabb azonosításának lehetővé tételéhez, akiknek adatait e rendszerek tárolják, többek között személyazonosító adataikat, útiokmány-adataikat és biometrikus adataikat, függetlenül attól, hogy az adatokat mely rendszerbe gyűjtötték be. A CIR-ben csak azokat a személyes adatokat lehet tárolni, amelyek a pontos személyazonosság-ellenőrzések végzéséhez elengedhetetlenül szükségesek. A CIR-ben rögzített személyes adatokat csak az alapul szolgáló rendszerek céljaihoz feltétlenül szükséges ideig lehet megőrizni, és azokat automatikusan törölni kell, ha az adatokat logikai elkülönítésüknek megfelelően törlik az alapul szolgáló rendszerekből.
- (23) Az új kezelési művelet, amely ezen adatoknak a CIR-ben történő tárolásából áll az egyes különálló rendszerekben történő tárolás helyett, azért szükséges, hogy növelni lehessen az azonosítás pontosságát az ilyen adatok automatizált összehasonlítása és megfeleltetése révén. Az a tény, hogy a CIR tárolja a személyazonosító adatokat, az útiokmány-adatokat és a biometrikus adatokat, nem akadályozhatja az adatoknak az EES, a VIS, az ETIAS, az Eurodac vagy az ECRIS-TCN céljából történő kezelését, tekintve, hogy a CIR az említett alapul szolgáló rendszerek új közös eleme.
- (24) A CIR-ben ezért egyéni aktát kell létrehozni az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban vagy az ECRIS-TCN-ben nyilvántartott minden egyes személyre vonatkozóan annak érdekében, hogy megvalósítható legyen a schengeni térségben történő helyes személyazonosításra irányuló célkitűzés, valamint a MID támogatása érdekében, amelynek kettős célja a jóhiszemű utazók személyazonossága ellenőrzésének megkönnyítése és a személyazonossággal való visszaélés elleni küzdelem. Az egyéni akta az adott személyhez kapcsolható összes lehetséges személyazonosító információt egyetlen helyen kell, hogy tárolja és hozzáférhetővé kell, hogy tegye a megfelelő felhatalmazással rendelkező végfelhasználók számára.
- (25) A CIR-nek ezáltal meg kell könnyítenie és egyszerűsíteni kell a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséért, felderítéséért és nyomozásáért felelős hatóságok hozzáférését az olyan uniós információs rendszerekhez, amelyeket nem kizárólag súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából hoztak létre.
- (26) A CIR az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban és az ECRIS-TCN-ben nyilvántartott személyek személyazonosító adatait, útiokmány-adatait és biometrikus adatait tartalmazó közös adattárként kell, hogy szolgáljon. A CIR-nek e rendszerek műszaki felépítésének részét kell képeznie, és az azok közötti közös elemként az említett rendszerek által kezelt személyazonosító adatok, útiokmány-adatok és biometrikus adatok tárolására és lekérdezésére kell szolgálnia.
- (27) A CIR-ben szereplő bejegyzéseket logikailag el kell különíteni egymástól azáltal, hogy mindegyik esetében automatikusan feltüntetésre kerül, hogy név szerint melyik rendszerhez tartozik. A CIR hozzáférés-ellenőrzésének ezeket a címkéket kell használnia a bejegyzéshez való hozzáférés engedélyezése vagy megtagadása céljából.
- (28) Amennyiben egy tagállami rendőri hatóság úti okmány vagy az adott személy személyazonosságát hitelt érdemlően igazoló más dokumentum hiányában nem tud azonosítani egy személyt, vagy amennyiben kétség merül fel az adott személy által rendelkezésre bocsátott személyazonosító adatokat, illetve az úti okmány



hitelességét vagy birtokosának személyazonosságát illetően, vagy ha a személy nem képes az együttműködésre vagy megtagadja azt, a rendőri hatóságnak jogosultsággal kell rendelkeznie arra, hogy a szóban forgó személy azonosítása céljából lekérdezést végezhesen a CIR-ben. E célból a rendőri hatóságoknak nyomatvételi munkaálomások (live-scan) alkalmazásával ujjnyomatokat kell venniük, feltéve, hogy az eljárást az adott személy jelenlétében indították meg. A CIR ilyen lekérdezése 12 év alatti kiskorúak személyazonosságának megállapítása céljából nem megengedett, kivéve, ha ezt a gyermek mindenek felett álló érdeke megkívánja.

- (29) Amennyiben a személy biometrikus adatai nem használhatók, vagy ha az ilyen adatokkal történő lekérdezés sikertelen, a lekérdezést a személy személyazonosító adataival és útiokmány-aadataival együttesen kell elvégezni. Amennyiben a lekérdezés nyomán kiderül, hogy a CIR tartalmaz az adott személyre vonatkozó adatokat, a tagállami hatóságok számára hozzáférést kell biztosítani a CIR-hez az érintett személy személyazonosító adataiba és útiokmány-aadataiba való betekintés céljából anélkül, hogy a CIR megjelölné, hogy ezek az adatok melyik uniós információs rendszerben találhatóak.
- (30) A tagállamoknak nemzeti jogalkotási intézkedéseket kell elfogadniuk, amelyekben kijelölik azokat a nemzeti hatóságokat, amelyek hatáskörrel rendelkeznek arra, hogy a CIR használatával személyazonosság-ellenőrzést végezzenek, valamint – az arányosság elvével összhangban – meghatározzák az ilyen ellenőrzések végzésére vonatkozó eljárásokat, azok feltételeit és kritériumait. Nemzeti jogszabálynak kell rendelkeznie különösen az említett hatóságok személyi állományának tagja előtt megjelent személyek személyazonosságának ellenőrzése során a biometrikus adatok gyűjtésére vonatkozó hatáskörrel.
- (31) E rendelet ezen túlmenően új lehetőséget kell, hogy bevezessen a tagállamok terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséért, felderítéséért és nyomozásáért felelős kijelölt hatóságai és az Europol számára az EES-ben, a VIS-ben, az ETIAS-ban vagy az Eurodacban található, a személyazonosító adatokon vagy útiokmány-adatokon felüli adatokhoz való egyszerűbb hozzáférésre is. Ezen adatok szükségesek lehetnek a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez vagy nyomozásához, ha alapos okkal feltételezhető, hogy az azokba való betekintés jelentősen hozzájárul a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez vagy nyomozásához, különösen, ha fennáll annak a gyanúja, hogy a terrorista bűncselekmény vagy egyéb súlyos bűncselekmény elkövetésével gyanúsított személy, az ilyen bűncselekmények elkövetője vagy áldozata olyan személy, akinek adatait az EES-ben, a VIS-ben, az ETIAS-ban vagy az Eurodacban tárolják.
- (32) Az EES-ben, a VIS-ben, az ETIAS-ban vagy az Eurodac-ban található adatokhoz a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása érdekében szükséges teljes körű hozzáférést – a CIR-ben található személyazonosító vagy útiokmány-adatoktól eltérő adatokhoz való hozzáféréseken felül – továbbra is az alkalmazandó jogi eszközök szabályozzák. A terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséért, felderítéséért és nyomozásáért felelős kijelölt hatóságok és az Europol nem tudják előre, hogy az uniós információs rendszerek közül melyik tartalmazza az általuk vizsgálandó személyek adatait. Ez gyakran késedelmet és hatékonysági problémákat eredményez. A kijelölt hatóság által felhatalmazott végfelhasználó számára ezért lehetővé kell tenni annak megismerését, hogy az említettek közül melyik uniós információs rendszer rögzíti a lekérdezés eredményének megfelelő adatokat. Ennek megfelelően a rendszerben talált egyezés automatizált ellenőrzését követően az érintett rendszer megjelölésre kerülne (úgynevezett „egyezés-megjelölés” funkció).
- (33) Ebben az összefüggésben a CIR-től kapott válasz nem értelmezhető vagy nem használható alapként vagy indokként következtetések levonásához vagy intézkedések megtételéhez valamely személy tekintetében, hanem csak az alapul szolgáló uniós információs rendszerekhez való hozzáférési kérelem benyújtására használható, az e hozzáférést szabályozó, megfelelő jogi eszközben megállapított feltételeknek és eljárásoknak megfelelően. Minden ilyen hozzáférés e rendelet VII. fejezetének hatálya alá, és esettől függően az (EU) 2016/679 rendelet, az (EU) 2016/680 irányelv vagy az (EU) 2018/1725 európai parlamenti és tanácsi rendelet <sup>(8)</sup> hatálya alá tartozik.
- (34) Általános szabályként, amennyiben az egyezés-megjelölés azt jelzi, hogy az adatok szerepelnek az EES-ben, a VIS-ben, az ETIAS-ban vagy az Eurodacban, a kijelölt hatóságoknak vagy az Europolnak teljes körű hozzáférést kell kérnie legalább az egyik érintett uniós információs rendszerhez. Amennyiben a teljes körű hozzáférést kivételesen nem kérik, például azért, mert a kijelölt hatóságok vagy az Europol más módon már megszerezték az adatokat, vagy az adatok megszerzését a nemzeti jog már nem teszi lehetővé, a hozzáférés iránti kérelem elmulasztásának indokolását rögzíteni kell.

<sup>(8)</sup> Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o.).

- (35) A CIR-ben végzett lekérdezések naplóiban jelezni kell a lekérdezések célját. Amennyiben az ilyen lekérdezés végzése a kétlépcsős adatbetekintési megközelítés alkalmazásával történt, a naplóknak tartalmazniuk kell a nyomozás vagy az ügy nemzeti aktájára való hivatkozást, ami azt jelzi, hogy a lekérdezést terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából kezdeményezték.
- (36) A CIR-nek a kijelölt hatóságok és az Europol általi, egyezés-megjelölés típusú válasz megszerzése céljából történő lekérdezése – amely válasz arra utal, hogy az adat szerepel az EES-ben, a VIS-ben, az ETIAS-ban vagy az Eurodacban – a személyes adatok automatizált kezelését teszi szükségessé. Az egyezés-megjelölés nem fedheti fel az érintett személy személyes adatait, csak arra utalhat, hogy bizonyos adatait tárolja valamelyik rendszer. A felhatalmazással rendelkező végfelhasználó pusztán az egyezés-megjelölés előfordulása alapján nem hozhat elmarasztaló határozatot az érintett személyre vonatkozóan. A végfelhasználó hozzáférése az egyezés-megjelöléshez ezért nagyon korlátozott mértékű beavatkozást valósít meg az érintett személy személyes adatainak védelméhez való jogába, míg a kijelölt hatóságok és az Europol számára lehetővé teszi, hogy hatékonyabban kérelmezhessek a személyes adatokhoz való hozzáférést.
- (37) A MID létrehozása a CIR működésének támogatása, valamint az EES, a VIS, az ETIAS, az Eurodac, a SIS és az ECRIS-TCN célkitűzéseinek támogatása érdekében szükséges. Annak érdekében, hogy hatékonyan teljesítsék célkitűzéseiket, az összes említett uniós információs rendszer szükségessé teszi azon személyek pontos azonosítását, akiknek személyes adatait azokban tárolják.
- (38) Az uniós információs rendszerek céljainak jobb megvalósítása érdekében az e rendszereket használó hatóságoknak képeseknek kell lenniük arra, hogy kellően megbízhatóan tudják ellenőrizni azon személyek személyazonosságát, akiknek adatait különböző rendszerekben tárolják. Egy adott önálló rendszerben tárolt személyazonosító adatok vagy útiokmány-adatok helytelenek, hiányosak vagy csalárdak lehetnek, és jelenleg nincs mód arra, hogy észleljék a helytelen, hiányos vagy csalárd személyazonosító adatokat vagy útiokmány-adatokat a más rendszerben tárolt adatokkal történő összehasonlítás révén. E helyzet orvoslása érdekében egy olyan uniós szintű technikai eszközt kell létrehozni, amely lehetővé teszi a személyek e célokból történő pontos azonosítását.
- (39) A MID-nek a különböző uniós információs rendszerekben található adatok között kapcsolatokat kell létrehoznia és tárolnia a többszörös személyazonosságok észlelése érdekében, a jóhiszemű utazók személyazonosság-ellenőrzésének megkönnyítése és a személyazonossággal való visszaélés elleni küzdelem kettős célját követve. A MID csak olyan személyekre vonatkozó adatok közötti kapcsolatokat tartalmazhat, amelyek egynél több uniós információs rendszerben szerepelnek. Az összekapcsolt adatok körét szigorúan azokra az adatokra kell korlátozni, amelyek annak ellenőrzéséhez szükségesek, hogy egy adott személy indokoltan vagy indokolatlanul szerepel-e különböző személyazonosságokkal a különböző rendszerekben, vagy annak tisztázásához szükségesek, hogy két, hasonló személyazonosító adatokkal rendelkező személy esetében nem lehet szó ugyanarról a személyről. Az egyéni aktáknak a különböző rendszerek közötti összekapcsolása céljából az ESP-n és a közös BMS-en keresztül történő adatkezelést a lehető legkisebb mértékűre kell szorítani, ezért annak a többszörös személyazonosságot használók észlelésére kell korlátozódnia, amit abban a pillanatban kell elvégezni, amikor a CIR-ben tárolt adatokkal rendelkező valamelyik rendszerhez, vagy a SIS-hez új adatot adnak hozzá. A MID-nek biztosítékokat kell magában foglalnia az olyan személyekkel szembeni esetleges hátrányos megkülönböztetéssel és kedvezőtlen döntéshozattal szemben, akik jogszerűen rendelkeznek több személyazonossággal.
- (40) Ez a rendelet új adatkezelési műveleteket ír elő az érintett személyek pontos azonosítása céljából. Ez az Európai Unió Alapjogi Chartájának 7. és 8. cikke által védett alapvető jogaikba való beavatkozásnak minősül. Mivel az uniós információs rendszerek hatékony alkalmazása az érintett személyek helyes azonosításától függ, az ilyen beavatkozást ugyanazok a célkitűzések indokolják, mint amelyek érdekében az egyes rendszereket létrehozták: az Unió határainak hatékony igazgatása, az Unió belső biztonsága és az uniós menekültügyi és vízumpolitika hatékony végrehajtása.
- (41) Az ESP-nek és a közös BMS-nek össze kell hasonlítania a CIR és a SIS személyekre vonatkozó adatait, amikor valamelyik nemzeti hatóság vagy uniós ügynökség új bejegyzést hoz létre vagy tölt fel. Az ilyen összehasonlítást automatizált módon kell végezni. A CIR és a SIS a közös BMS-t arra kell, hogy használja, hogy a biometrikus adatok alapján észlelje az esetleges kapcsolatokat. A CIR és a SIS az ESP-t arra kell, hogy használja, hogy az alfanumerikus adatok alapján észlelje az esetleges kapcsolatokat. A CIR-nek és a SIS-nek képesnek kell lennie az egyes személyekre vonatkozóan különböző rendszerekben tárolt azonos vagy hasonló adatok azonosítására. Amennyiben ilyen eset áll fenn, létre kell hozni egy kapcsolatot, amely jelzi, hogy ugyanarról a személyről van szó. A CIR-t és a SIS-t úgy kell konfigurálni, hogy észleljék a kisebb átírási vagy helyesírási hibákat annak érdekében, hogy ezek ne okozzanak indokolatlan akadályokat az érintett személy számára.

- (42) A nemzeti hatóságnak vagy uniós ügynökségnek, amely rögzítette az adatokat a megfelelő uniós információs rendszerben, meg kell erősítenie vagy módosítania kell ezeket a kapcsolatokat. Ennek a nemzeti hatóságnak vagy uniós ügynökségnek hozzáféréssel kell rendelkeznie a CIR-ben vagy a SIS-ben és a MID-ben tárolt adatokhoz a különböző személyazonosságok manuális ellenőrzése céljából.
- (43) A különböző személyazonosságok manuális ellenőrzését annak a hatóságnak kell biztosítania, amely létrehozta vagy aktualizálta azokat az adatokat, amelyek más uniós információs rendszerben tárolt adatokkal kapcsolatot létrehozva egyezést eredményeztek. A különböző személyazonosságok manuális ellenőrzéséért felelős hatóságnak azt kell értékelnie, hogy indokoltan vagy indokolatlanul áll-e fenn az ugyanarra a személyre vonatkozó többszörös személyazonosság. Ezt az értékelést lehetőség szerint az érintett személy jelenlétében kell elvégezni, és szükség esetén további pontosítást vagy információt kell kérni tőle. Az ilyen értékelést haladéktalanul el kell végezni, az információk pontosságára vonatkozó uniós jogi és nemzeti jogi követelményekkel összhangban. Különösen a határokon, az érintett személyek mozgását az ellenőrzés idejére korlátozni fogják, az ellenőrzés ezért nem tarthat határozatlan ideig. A MID-ben szereplő sárga kapcsolat önmagában nem szolgálhat alapul a beléptetés megtagadásához, és a beléptetés engedélyezésére vagy megtagadására vonatkozó határozatot kizárólag az (EU) 2016/399 európai parlamenti és tanácsi rendelet<sup>(9)</sup> alkalmazandó rendelkezései alapján kell meghozni.
- (44) A SIS-el kapcsolatban az átadási vagy kiadási letartóztatás céljából körözött személyekre, eltűnt vagy különleges bánásmódot igénylő személyekre, a bírósági eljárásban való közreműködés céljából keresett személyekre vagy rejtett ellenőrzés, kikérdezés vagy célzott ellenőrzés miatt keresett személyekre vonatkozó figyelmeztető jelzésekhez kötődő kapcsolatok tekintetében a különböző személyazonosságok manuális ellenőrzéséért felelős hatóságnak a figyelmeztető jelzést létrehozó tagállam SIRENE-irodájának kell lennie. A SIS figyelmeztető jelzések e kategóriái érzékenyek, ezért azokat nem feltétlenül kell megosztani a más uniós információs rendszerekben ezen adatokkal összekapcsolt adatokat létrehozó vagy frissítő hatóságokkal. A SIS-adatokkal való kapcsolat létrehozása nem sértheti az (EU) 2018/1860<sup>(10)</sup>, az (EU) 2018/1861<sup>(11)</sup> és az (EU) 2018/1862<sup>(12)</sup> európai parlamenti és tanácsi rendeletnek megfelelően meghozandó intézkedéseket.
- (45) E kapcsolatok létrehozása az érintett személyek irányába átláthatóságot követel meg. Az alkalmazandó uniós adatvédelmi szabályoknak megfelelő szükséges biztosítékok végrehajtásának megkönnyítése érdekében azon személyeket, akik a különböző személyazonosságok manuális ellenőrzését követően vörös vagy fehér kapcsolattal rendelkeznek, írásban kell tájékoztatni a biztonság és közrend védelme, a bűncselekmények megelőzése és a nemzeti nyomozások veszélyeztetésének megakadályozása érdekében szükséges korlátozások sérelme nélkül. Az ilyen személyek kapnak egy egységes azonosító számot, amely lehetővé teszi számukra azon hatóság azonosítását, amelyhez jogaik gyakorlása érdekében fordulniuk kell.
- (46) Sárga kapcsolat létrehozása esetén a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság számára hozzáférést kell biztosítani a MID-hez. Vörös kapcsolat fennállása esetén azon tagállami hatóságok és uniós ügynökségek számára is hozzáférést kell biztosítani a MID-hez, amelyek hozzáféréssel rendelkeznek a CIR-ben szereplő legalább egy uniós információs rendszerhez vagy a SIS-hez. A vörös kapcsolat azt kell, hogy jelezze, hogy az adott személy indokolatlan módon használ különböző személyazonosságokat, vagy hogy valaki más személyazonosságát használja.
- (47) A tagállami hatóságok és az uniós ügynökségek akkor is hozzáférhetnek a MID-hez, ha két uniós információs rendszer adatai között fehér vagy zöld kapcsolat áll fenn, amennyiben az ilyen hatóság vagy ügynökség mindkét információs rendszerhez hozzáfér. Az ilyen hozzáférést kizárólag azzal a céllal kell biztosítani, hogy a hatóság vagy ügynökség észlelje azokat a lehetséges eseteket, amikor az adatokat helytelenül kapcsolták össze, vagy hogy az adatokat a MID-ben, a CIR-ben és a SIS-ben e rendeletet megsértve kezelték, és megtegye a helyzet javításához szükséges intézkedéseket, és frissítse vagy törölje a kapcsolatot.

<sup>(9)</sup> Az Európai Parlament és a Tanács (EU) 2016/399 rendelete (2016. március 9.) a személyek határátlépésére irányadó szabályok uniós kódexéről (Schengeni határellenőrzési kódex) (HL L 77., 2016.3.23., 1. o.).

<sup>(10)</sup> Az Európai Parlament és a Tanács (EU) 2018/1860 rendelete (2018. november 28.) a Schengeni Információs Rendszernek a jogellenesen tartózkodó harmadik országbeli állampolgárok visszaküldése céljából történő használatáról (HL L 312., 2018.12.7., 1. o.).

<sup>(11)</sup> Az Európai Parlament és a Tanács (EU) 2018/1861 rendelete (2018. november 28.) a határforgalom-ellenőrzés terén a Schengeni Információs Rendszer (SIS) létrehozásáról, működéséről és használatáról, a Schengeni Megállapodás végrehajtásáról szóló egyezmény módosításáról, valamint az 1987/2006/EK rendelet módosításáról és hatályon kívül helyezéséről (HL L 312., 2018.12.7., 14. o.).

<sup>(12)</sup> Az Európai Parlament és a Tanács (EU) 2018/1862 rendelete (2018. november 28.) a rendőrségi együttműködés és a büntetőügyekben folytatott igazságügyi együttműködés terén a Schengeni Információs Rendszer (SIS) létrehozásáról, működéséről és használatáról, a 2007/533/IB tanácsi határozat módosításáról és hatályon kívül helyezéséről, valamint az 1986/2006/EK európai parlamenti és tanácsi rendelet és a 2010/261/EU bizottsági határozat hatályon kívül helyezéséről (HL L 312., 2018.12.7., 56. o.).

- (48) A szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai uniós ügynökségnek (eu-LISA) az adatminőség ellenőrzésére irányuló, automatizált mechanizmusokat és az adatminőségre vonatkozó közös mutatókat kell létrehoznia. Az eu-LISA felelősségi körébe kell, hogy tartozzon egy központi adatminőség-ellenőrzési kapacitás kiépítése, valamint rendszeres adatelemzési jelentések készítése az uniós információs rendszerek tagállamok általi végrehajtásának javítása érdekében. A közös adatminőségi mutatóknak tartalmazniuk kell az uniós információs rendszerekben vagy az interoperabilitási elemekben szereplő adatok tárolására vonatkozó minőségi minimumkövetelményeket. Az ilyen adatminőségi követelmények célja az uniós információs rendszerekbe és az interoperabilitási elemekbe történő láthatóan helytelen vagy következtelen adatbevitel automatikus azonosítása annak érdekében, hogy az adatbevitelt végző tagállam képes legyen ellenőrizni az adatokat, és szükség esetén korrekciós intézkedéseket alkalmazni.
- (49) A Bizottságnak értékelnie kell az eu-LISA minőségi jelentéseit, és szükség esetén ajánlásokat kell intéznie a tagállamokhoz. A tagállamok feladata kell, hogy legyen egy olyan cselekvési terv elkészítése, amely ismerteti az adatok minőségével kapcsolatos hiányosságok orvoslását célzó intézkedéseket, valamint a tagállamoknak rendszeresen be kell számolniuk az elért eredményekről.
- (50) Az egységes üzenetformátum (UMF) a bel- és igazságügy területén működő információs rendszerek, hatóságok vagy szervezetek közötti strukturált, határokon átnyúló információcserére vonatkozó normaként kell, hogy szolgáljon. Az UMF-nek közös kifejezéseket és logikai struktúrákat kell meghatároznia a kölcsönös információcserében szereplő adatok vonatkozásában az interoperabilitás megkönnyítése céljából, a cserélt tartalmak következetes és szemantikailag egyenértékű módon történő létrehozásának és olvasásának lehetővé tétele által.
- (51) Megfontolás tárgyát képezheti az UMF szabvány alkalmazása a VIS-ben, a SIS-ben, valamint a bel- és igazságügy területén működő, bármely meglévő vagy új, a tagállamok által kidolgozott információcsere-modell és információs rendszer esetében.
- (52) Létre kell hozni a jelentések és statisztikák központi adattárát (CRRS), amely rendszerek közötti statisztikai adatokat és elemzési jelentéseket készít szakpolitikai, működési és adatminőségi célokból, a vonatkozó jogi eszközöknek megfelelően. Az eu-LISA-nak kell létrehoznia, bevezetnie és technikai helyszínein üzemeltetnie a CRRS-t. A CRRS az uniós információs rendszerekből, a CIR-ből, a MID-ből és a közös BMS-ből származó anonimizált statisztikai adatokat tartalmaz. A CRRS-ben szereplő adatok nem tehetik lehetővé az egyének azonosítását. Az eu-LISA-nak automatikusan anonimizálnia kell az adatokat, és csak ilyen anonimizált adatokat rögzíthet a CRRS-ben. Az adatok anonimizálásának folyamatát automatizálni kell, és az eu-LISA személyi állománya nem kaphat közvetlen hozzáférést az uniós információs rendszerekben vagy az interoperabilitási elemekben tárolt személyes adatokhoz.
- (53) A személyes adatoknak a nemzeti hatóságok által az e rendelet szerinti interoperabilitási célból történő kezelésére az (EU) 2016/679 rendelet alkalmazandó, kivéve, ha az adatkezelést a tagállamok kijelölt hatóságai vagy központi hozzáférési pontjai terrorcselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából végzik.
- (54) Ha a személyes adatok tagállami szintű, e rendelet szerinti interoperabilitási célból történő kezelését az illetékes hatóságok terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából végzik, az (EU) 2016/680 irányelv alkalmazandó.
- (55) Az (EU) 2016/679 rendelet, az (EU) 2018/1725 rendelet vagy adott esetben az (EU) 2016/680 irányelv alkalmazandó a személyes adatok harmadik országok vagy nemzetközi szervezetek számára e rendelet szerinti továbbítására is. Az (EU) 2016/679 rendelet V. fejezete vagy adott esetben az (EU) 2016/680 irányelv V. fejezete szerinti adattovábbítási indokok sérelme nélkül, valamely harmadik ország bíróságának azon ítéletét, valamint valamely harmadik ország közigazgatási hatóságának azon határozatát, amely személyes adatok továbbítását vagy közzétételét írja elő egy adatkezelő vagy adatfeldolgozó számára, kizárólag akkor kell elismerni vagy bármilyen módon végrehajtani, ha a kérelmező harmadik ország és az Unió vagy valamely tagállam között nemzetközi megállapodás van hatályban.

- (56) A személyes adatoknak az (EU) 2017/2226<sup>(13)</sup>, a 767/2008/EK<sup>(14)</sup>, és az (EU) 2018/1240<sup>(15)</sup> európai parlamenti és tanácsi rendelet, valamint az (EU) 2018/1861 rendelet által szabályozott rendszerekben történő kezelésére az említett rendeletek adatvédelemre vonatkozó különös rendelkezései alkalmazandók.
- (57) A személyes adatoknak az eu-LISA és az Unió más intézményei és szervei által feladataik ellátása során történő, e rendelet szerinti kezelésére az (EU) 2018/1725 rendelet alkalmazandó, az (EU) 2016/794 európai parlamenti és tanácsi rendelet<sup>(16)</sup> sérelme nélkül, amely a személyes adatok Európa általi kezelésére alkalmazandó.
- (58) A személyes adatok tagállamok általi kezelésének jogszerűségét az (EU) 2016/679 rendeletben vagy az (EU) 2016/680 irányelvben említett felügyeleti hatóságoknak kell felügyelniük. Az európai adatvédelmi biztosnak felügyelnie kell az uniós intézményeknek és szervezeteknek a személyes adatok kezeléséhez kapcsolódó tevékenységét. Az európai adatvédelmi biztosnak és a felügyeleti hatóságoknak együtt kell működniük egymással a személyes adatok interoperabilitási elemek által történő kezelésének nyomon követése során. Ahhoz, hogy az európai adatvédelmi biztos elláthassa az e rendelet alapján ráruházott feladatokat, megfelelő forrásokra, többek között emberi és pénzügyi forrásokra van szükség.
- (59) Az európai adatvédelmi biztossal a 45/2001/EK európai parlamenti és tanácsi rendelet<sup>(17)</sup> 28. cikkének (2) bekezdésével összhangban konzultációt folytattak, és a biztos 2018. április 16-án véleményt nyilvánított<sup>(18)</sup>.
- (60) A 29. cikk szerinti adatvédelmi munkacsoport 2018. április 11-én véleményt nyilvánított.
- (61) Mind a tagállamoknak, mind az eu-LISA-nak biztonsági tervet kell fenntartaniuk a biztonsági kötelezettségek teljesítésének megkönnyítése érdekében, és együtt kell működniük egymással a biztonsági problémák kezelése terén. Az eu-LISA-nak emellett biztosítani kell a legújabb technológiafejlesztések folyamatos használatát az interoperabilitási elemek fejlesztésével, kialakításával és kezelésével összefüggésben az adatok sértetlenségének biztosítása érdekében. Az eu-LISA e tekintetben fennálló kötelezettségei közé tartozik a jogosulatlan személyek, például külső szolgáltatók személyi állománya interoperabilitási elemeken keresztül kezelt személyes adatokhoz való hozzáféréseinek megakadályozásához szükséges intézkedések elfogadása. A szolgáltatásnyújtásra irányuló szerződések odaítélésekor a tagállamoknak és az eu-LISA-nak fontolóra kell vennie minden olyan intézkedést, amely a személyes adatok és az egyének magánéletének védelmére vagy az alapvető biztonsági érdekek védelmére vonatkozó jogszabályoknak vagy rendelkezéseknek való megfelelés biztosításához szükséges, az (EU, Euratom) 2018/1046 európai parlamenti és tanácsi rendelet<sup>(19)</sup>, valamint a vonatkozó nemzetközi egyezmények alapján. Az eu-LISA az interoperabilitási elemek fejlesztése során a beépített és alapértelmezett adatvédelem elveit követi.
- (62) Az e rendeletben előírt interoperabilitási elemek alkalmazása hatással lesz a határátkelőhelyeken végzett ellenőrzések módjára. Ezeket a hatásokat az (EU) 2016/399 rendelet hatályos szabályainak és az interoperabilitásra vonatkozóan e rendeletben előírt szabályoknak az együttes alkalmazása fogja eredményezni.
- (63) A szabályok említett együttes alkalmazásának következtében az ESP-nek kell lennie az elsődleges hozzáférési pontnak az (EU) 2016/399 rendeletben foglaltak szerint a határátkelőhelyeken a személyekre vonatkozó adatbázisokba történő kötelező szisztematikus betekintés céljából. Emellett a határőröknek a MID-ben szereplő kapcsolat vörös besorolását eredményező személyazonosító adatokat vagy útiokmány-adatokat is figyelembe kell

<sup>(13)</sup> Az Európai Parlament és a Tanács (EU) 2017/2226 rendelete (2017. november 30.) a tagállamok külső határait átlépő harmadik országbeli állampolgárok belépésére és kilépésére, valamint beléptetésének megtagadására vonatkozó adatok rögzítésére szolgáló határregisztrációs rendszer (EES) létrehozásáról és az EES-hez való bűnüldözési célú hozzáférés feltételeinek meghatározásáról, valamint a Schengeni Megállapodás végrehajtásáról szóló egyezmény, a 767/2008/EK rendelet és az 1077/2011/EU rendelet módosításáról (HL L 327., 2017.12.9., 20. o.).

<sup>(14)</sup> Az Európai Parlament és a Tanács 767/2008/EK rendelete (2008. július 9.) a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről (VIS-rendelet) (HL L 218., 2008.8.13., 60. o.).

<sup>(15)</sup> Az Európai Parlament és a Tanács (EU) 2018/1240 rendelete (2018. szeptember 12.) az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS) létrehozásáról, valamint az 1077/2011/EU rendelet, az 515/2014/EU rendelet, az (EU) 2016/399 rendelet, az (EU) 2016/1624 rendelet és az (EU) 2017/2226 rendelet módosításáról (HL L 236., 2018.9.19., 1. o.).

<sup>(16)</sup> Az Európai Parlament és a Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Unió Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről HL L 135., 2016.5.24., 53. o.).

<sup>(17)</sup> Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő kezelése tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról (HL L 8., 2001.1.12., 1. o.).

<sup>(18)</sup> HL C 233., 2018.7.4., 12. o.

<sup>(19)</sup> Az Európai Parlament és a Tanács (EU, Euratom) 2018/1046 rendelete (2018. július 18.) az Unió általános költségvetésére alkalmazandó pénzügyi szabályokról, az 1296/2013/EU, az 1301/2013/EU, az 1303/2013/EU, az 1304/2013/EU, az 1309/2013/EU, az 1316/2013/EU, a 223/2014/EU és a 283/2014/EU rendelet és az 541/2014/EU határozat módosításáról, valamint a 966/2012/EU, Euratom rendelet hatályon kívül helyezéséről (HL L 193., 2018.7.30., 1. o.).

venniük annak értékelése céljából, hogy az adott személy megfelel-e az (EU) 2016/399 rendeletben meghatározott beutazási feltételeknek. Önmagában a vörös kapcsolat megléte azonban nem minősülhet a beléptetés megtagadását eredményező oknak, ezért az (EU) 2016/399 rendeletben szereplő, a beléptetés megtagadására vonatkozó jelenlegi indokokat nem kell módosítani.

- (64) Helyénvaló lenne naprakésszé tenni a Határőrök gyakorlati kézikönyvét e pontosítások egyértelművé tétele érdekében.
- (65) Ha az MID-nek az ESP-n keresztül történő lekérdezése sárga kapcsolatot eredményez, vagy vörös kapcsolat meglétét jelzi, az ellenőrzést végző határőrnek betekintést kell végeznie a CIR-be vagy a SIS-be, vagy mindkettőbe, annak érdekében, hogy értékelje az ellenőrzött személyre vonatkozó információkat, manuálisan ellenőrizze az illető személyazonosító adatait, és szükség esetén módosítsa a kapcsolat színét.
- (66) A statisztikák és a jelentéstétel céljainak támogatása érdekében az e rendeletben említett illetékes hatóságok, uniós intézmények és ügynökségek felhatalmazással rendelkező személyi állománya számára hozzáférést kell biztosítani az egyes interoperabilitási elemekhez kapcsolódó bizonyos adatokba való betekintés céljából oly módon, hogy a személyek azonosítása ne váljon lehetővé.
- (67) Annak érdekében, hogy a tagállami hatóságok és az uniós ügynökségek alkalmazkodni tudjanak az ESP használatára vonatkozó új követelményekhez, átmeneti időszakot kell biztosítani. Hasonlóképpen, a MID koherens és optimális működésének lehetővé tétele érdekében annak megkezdésére vonatkozóan átmeneti intézkedéseket kell megállapítani.
- (68) Mivel e rendelet célját – nevezetesen az uniós információs rendszerek közötti interoperabilitás keretének létrehozását – a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban a fellépés léptéke és hatása miatt e cél jobban megvalósítható, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés (EUSZ) 5. cikkében foglalt szubszidiaritási elvnek megfelelően. Az említett cikkben foglalt arányosság elvének megfelelően ez a rendelet nem lépi túl az e cél eléréséhez szükséges mértéket.
- (69) Az 515/2014/EU európai parlamenti és tanácsi rendelet<sup>(20)</sup> szerinti intelligens határellenőrzésre elkülönített költségvetés fennmaradó összegét át kell csoportosítani erre a rendeletre az 515/2014/EU rendelet 5. cikke (5) bekezdése b) pontjának megfelelően, az interoperabilitási elemek fejlesztési költségeinek fedezésére.
- (70) E rendelet egyes részletes technikai vonatkozásainak kiegészítése érdekében a Bizottságot fel kell hatalmazni arra, hogy az Európai Unió működéséről szóló szerződés (EUMSZ) 290. cikkének megfelelően jogi aktusokat fogadjon el az alábbiakra vonatkozóan:
- az ESP átmeneti használati időszakának meghosszabbítása;
  - az ETIAS központi egysége által végzett többszörös személyazonosság-észlelés átmeneti időszakának meghosszabbítása;
  - az eljárások tekintetében azon esetek meghatározására, amikor a személyazonosító adatok azonosaknak vagy hasonlóaknak tekinthetők;
  - a CRRS működésére vonatkozó szabályok, többek között a személyes adatok kezelésének speciális biztosítékai és az adattárra alkalmazandó biztonsági szabályok; valamint
  - a webportál működtetésére vonatkozó részletes szabályok.

Különösen fontos, hogy a Bizottság az előkészítő munkája során megfelelő konzultációkat folytasson, többek között szakértői szinten is, és hogy e konzultációkra a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásnak<sup>(21)</sup> megfelelően kerüljön sor. A felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg kap kézhez minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein.

- (71) E rendelet végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni azon időpontok meghatározására vonatkozóan, amikortól az ESP, a közös BMS, a CIR, a MID és a CRRS megkezdí működését.

<sup>(20)</sup> Az Európai Parlament és a Tanács 515/2014/EU rendelete (2014. április 16.) a Belső Biztonsági Alap részét képező, a külső határok és a vízumügy pénzügyi támogatására szolgáló eszköz létrehozásáról és az 574/2007/EK határozat hatályon kívül helyezéséről (HL L 150., 2014.5.20., 143. o.).

<sup>(21)</sup> HLL 123., 2016. 5.12., 1. o.

- (72) A Bizottságra végrehajtási hatásköröket kell ruházni emellett az alábbiakra vonatkozó részletes szabályok elfogadására: az ESP felhasználói profiljainak technikai részleteire; azon technikai megoldás követelményeire, amely megkönnyíti az uniós információs rendszerek, az Europol-adatok és az Interpol-adatbázisok ESP-n keresztül történő lekérdezését, és az ESP válaszainak formátumára; a MID-ben a különböző uniós információs rendszerekből származó adatok közötti kapcsolatok létrehozásának technikai szabályaira; vörös kapcsolat létrehozása esetén az érintett tájékoztatására szolgáló formanyomtatvány tartalmára és formájára; a közös BMS teljesítményével kapcsolatos követelményekre és teljesítményének nyomon követésére; az adatminőség ellenőrzésére irányuló automatizált mechanizmusokra, eljárásokra és mutatókra; az UMF-re vonatkozó szabvány kidolgozására; a biztonsági incidensek esetén irányadó együttműködési eljárásra; valamint a tagállamok számára a felhasználói hozzáférési kérelmek kezelését szolgáló technikai megoldás követelményeire vonatkozóan. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek<sup>(22)</sup> megfelelően kell gyakorolni.
- (73) Mivel az interoperabilitási elemek jelentős mennyiségű különleges személyes adat kezelésével járnak, fontos, hogy azok a személyek, akiknek az adatait a szóban forgó interoperabilitási elemeken keresztül kezelik, hatékonyan tudják gyakorolni az őket érintettként megillető jogokat az (EU) 2016/679 rendeletben, az (EU) 2016/680 irányelvben és az (EU) 2018/1725 rendeletben előírt módon. Az érintettek rendelkezésére kell bocsátani egy webportált, amely megkönnyíti számukra a személyes adataikhoz való hozzáféréshez, az adatok helyesbítéséhez, törléséhez és kezelésének korlátozásához való joguk gyakorlását. Ezt a webportált az eu-LISA-nak kell létrehoznia és kezelnie.
- (74) Az adatvédelem egyik legfőbb elve az adattakarékosság: az (EU) 2016/679 rendelet 5. cikke (1) bekezdésének c) pontja értelmében a személyes adatok kezelésének az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lennie, és a szükségesre kell korlátozódnia. Emiatt az interoperabilitási elemek nem irányozhatják elő új személyes adatok tárolását, kivéve azokat a kapcsolatokat, amelyek a MID-ben kerülnek tárolásra, és amelyek e rendelet céljai szempontjából a szükséges minimumot jelentik.
- (75) E rendeletnek egyértelmű rendelkezéseket kell tartalmaznia a személyes adatok jogellenes kezelésével, valamint az e rendelettel összeegyeztethetetlen bármely egyéb cselekménnyel kapcsolatos felelősségre és az abból fakadó kártérítési jogosultságra vonatkozóan, az (EU) 2016/679 rendelet, az (EU) 2016/680 irányelv és az (EU) 2018/1725 rendelet alapján fennálló adatkezelői és adatfeldolgozói felelősség és az abból fakadó kártérítési jogosultság sérelme nélkül. Az eu-LISA-nak felelősséggel kell tartoznia mindazon kárért, amelyet adatkezelői minőségében okoz az e rendelet által kifejezetten rá ruházott kötelezettségek nem teljesítése által vagy azáltal, hogy az adatkezelő tagállam jogszerű utasításai által szabott kereteken kívül vagy azokkal ellentétes módon járt el.
- (76) Ez a rendelet nem érinti a 2004/38/EK európai parlamenti és tanácsi irányelv<sup>(23)</sup> alkalmazását.
- (77) Az EUSZ-hez és az EUMSZ-hez csatolt, Dánia helyzetéről szóló 22. jegyzőkönyv 1. és 2. cikke értelmében Dánia nem vesz részt ennek a rendeletnek az elfogadásában, az rá nézve nem kötelező és nem alkalmazandó. Mivel e rendelet a schengeni vívmányokon alapul, Dánia az említett jegyzőkönyv 4. cikkének megfelelően az e rendeletről szóló tanácsi döntést követő hat hónapos időszakon belül határoz arról, hogy azt nemzeti jogában végrehajtsa-e.
- (78) Ez a rendelet a schengeni vívmányok azon rendelkezéseinek továbbfejlesztését képezi, amelyek alkalmazásában az Egyesült Királyság a 2000/365/EK tanácsi határozattal<sup>(24)</sup> összhangban nem vesz részt. Ennélfogva az Egyesült Királyság nem vesz részt ennek a rendeletnek az elfogadásában, az rá nézve nem kötelező és nem alkalmazandó.
- (79) Ez a rendelet a schengeni vívmányok azon rendelkezéseinek továbbfejlesztését képezi, amelyek alkalmazásában Írország a 2002/192/EK tanácsi határozattal<sup>(25)</sup> összhangban nem vesz részt. Ennélfogva Írország nem vesz részt ennek a rendeletnek az elfogadásában, az rá nézve nem kötelező és nem alkalmazandó.

<sup>(22)</sup> Az Európai Parlament és a Tanács 182/2011/EU rendelete (2011. február 16.) a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról (HL L 55., 2011.2.28., 13. o.).

<sup>(23)</sup> Az Európai Parlament és a Tanács 2004/38/EK irányelve (2004. április 29.) az Unió polgárainak és családtagjaiknak a tagállamok területén történő szabad mozgáshoz és tartózkodáshoz való jogáról, valamint az 1612/68/EGK rendelet módosításáról, továbbá a 64/221/EGK, a 68/360/EGK, a 72/194/EGK, a 73/148/EGK, a 75/34/EGK, a 75/35/EGK, a 90/364/EGK, a 90/365/EGK, és a 93/96/EGK irányelv hatályon kívül helyezéséről. (HL L 158., 2004.4.30., 77. o.).

<sup>(24)</sup> A Tanács 2000/365/EK határozata (2000. május 29.) Nagy-Britannia és Észak-Írország Egyesült Királyságának a schengeni vívmányok egyes rendelkezéseinek alkalmazásában való részvételére vonatkozó kéréséről (HL L 131., 2000.6.1., 43. o.).

<sup>(25)</sup> A Tanács 2002/192/EK határozata (2002. február 28.) Írországnak a schengeni vívmányok egyes rendelkezései alkalmazásában való részvételére vonatkozó kéréséről (HL L 64., 2002.3.7., 20. o.).

- (80) Izland és Norvégia tekintetében e rendelet az Európai Unió Tanácsa, valamint az Izlandi Köztársaság és a Norvég Királyság közötti, az utóbbiaknak a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról szóló megállapodás <sup>(26)</sup> értelmében a schengeni vívmányok azon rendelkezéseinek továbbfejlesztését képezi, amelyek az 1999/437/EK tanácsi határozat <sup>(27)</sup> 1. cikkének A., B., C. és G. pontjában említett területhez tartoznak.
- (81) Svájc tekintetében e rendelet az Európai Unió, az Európai Közösség és a Svájci Államszövetség közötti, a Svájci Államszövetségnek a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról szóló megállapodás <sup>(28)</sup> értelmében a schengeni vívmányok azon rendelkezéseinek továbbfejlesztését képezi, amelyek a 1999/437/EK határozatnak a 2008/146/EK tanácsi határozat <sup>(29)</sup> 3. cikkével együtt értelmezett 1. cikke A., B., C. és G. pontjában említett területhez tartoznak.
- (82) Liechtenstein tekintetében ez a rendelet az Európai Unió, az Európai Közösség, a Svájci Államszövetség és a Liechtensteini Hercegség közötti, a Liechtensteini Hercegségnek az Európai Unió, az Európai Közösség és a Svájci Államszövetség közötti, a Svájci Államszövetségnek a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról szóló megállapodáshoz való csatlakozásáról szóló jegyzőkönyv <sup>(30)</sup> értelmében a schengeni vívmányok azon rendelkezéseinek továbbfejlesztését képezi, amelyek az 1999/437/EK határozatnak a 2011/349/EU határozat <sup>(31)</sup> 3. cikkével együtt értelmezett 1. cikke A., B., C. és G. pontjában említett területhez tartoznak.
- (83) Ez a rendelet tiszteletben tartja az alapvető jogokat és különösen az Európai Unió Alapjogi Chartájában elismert elveket, és végrehajtása során e jogoknak és elveknek megfelelően kell eljárni.
- (84) Annak érdekében, hogy e rendelet illeszkedjen a hatályos jogi keretbe, a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 rendeletet, valamint a 2004/512/EK <sup>(32)</sup> és a 2008/633/IB <sup>(33)</sup> tanácsi határozatot megfelelően módosítani kell,

ELFOGADTA EZT A RENDELETET:

#### I. FEJEZET

### Általános rendelkezések

#### 1. cikk

#### Tárgy

(1) Ez a rendelet az (EU) 2019/818 európai parlamenti és tanácsi rendelettel <sup>(34)</sup> együtt létrehozza a határregisztrációs rendszer (EES), a Vízuminformációs Rendszer (VIS), az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS), az Eurodac, a Schengeni Információs Rendszer (SIS) és a harmadik országok állampolgáira vonatkozó Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS-TCN) interoperabilitását biztosító keretet.

<sup>(26)</sup> HL L 176., 1999.7.10., 36. o.

<sup>(27)</sup> A Tanács 1999/437/EK határozata (1999. május 17.) az Európai Unió Tanácsa, valamint az Izlandi Köztársaság és a Norvég Királyság között, e két államnak a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról kötött megállapodás alkalmazását szolgáló egyes szabályokról (HL L 176., 1999.7.10., 31. o.).

<sup>(28)</sup> HL L 53., 2008.2.27., 52. o.

<sup>(29)</sup> A Tanács 2008/146/EK határozata (2008. január 28.) az Európai Unió, az Európai Közösség és a Svájci Államszövetség közötti, a Svájci Államszövetségnek a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról szóló megállapodásnak az Európai Közösség nevében történő megkötéséről (HL L 53., 2008.2.27., 1. o.).

<sup>(30)</sup> HL L 160., 2011.6.18., 21. o.

<sup>(31)</sup> A Tanács határozata (2011. március 7.) az Európai Unió, az Európai Közösség, a Svájci Államszövetség és a Liechtensteini Hercegség közötti, a Liechtensteini Hercegségnek az Európai Unió, az Európai Közösség és a Svájci Államszövetség közötti, a Svájci Államszövetségnek a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló, különösen a belső határokon történő ellenőrzés megszüntetéséhez és a személyek mozgásához kapcsolódó társulásáról szóló megállapodáshoz való csatlakozásáról szóló jegyzőkönyvnek az Európai Unió nevében történő megkötéséről (HL L 160., 2011.6.18., 19. o.).

<sup>(32)</sup> A Tanács 2004/512/EK határozata (2004. június 8.) a Vízuminformációs Rendszer létrehozásáról (VIS) (HL L 213., 2004.6.15., 5. o.).

<sup>(33)</sup> A Tanács 2008/633/IB határozata (2008. június 23.) a vízuminformációs rendszerhez (VIS) a tagállamok kijelölt hatóságai, valamint az Europol számára a terrorcselekmények és egyéb súlyos bűncselekmények megelőzése, felderítése és kivizsgálása érdekében, betekintés céljából történő hozzáférésről (HL L 218., 2008.8.13., 129. o.).

<sup>(34)</sup> Az Európai Parlament és a Tanács (EU) 2019/818 rendelete (2019. május 20.) az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a rendőrségi és igazságügyi együttműködés, a menekültügy és a migráció területén, valamint az (EU) 2018/1726, az (EU) 2018/1862 és az (EU) 2019/816 rendelet módosításáról (lásd e Hivatalos Lap 85. oldalát).



(2) A keret az alábbi interoperabilitási elemeket foglalja magában:

- a) az európai keresőportál (ESP);
- b) a közös biometrikus megfeleltetési szolgáltatás (közös BMS);
- c) a közös személyazonosítóadat-tár (CIR);
- d) a többszörös személyazonosságot észlelő rendszer (MID).

(3) Ez a rendelet ezen felül rendelkezéseket állapít meg az adatminőségre vonatkozó követelményekre, az egységes üzenetformátumra (UMF) és a jelentések és statisztikák központi adattárára (CRRS) vonatkozóan, valamint az interoperabilitási elemek kialakítása, fejlesztése és működése tekintetében a tagállamok és a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagy méretű IT-rendszereinek üzemeltetési igazgatását végző európai ügynökség (eu-LISA) feladataira vonatkozóan.

(4) Ez a rendelet módosítja továbbá a tagállamok kijelölt hatóságainak és a Bűnüldözési Együttműködés Európai Uniói Ügynökségének (Europol) az EES-hez, a VIS-hez, az ETIAS-hoz és az Eurodachoz a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából való hozzáféréssel kapcsolatos eljárásokat és feltételeket.

(5) Ez a rendelet meghatározza továbbá a személyek személyazonosságának ellenőrzésére és a személyek azonosítására szolgáló keretrendszert.

## 2. cikk

### Célkitűzések

(1) Az interoperabilitás biztosítása révén e rendelet célkitűzései a következők:

- a) a külső határokon a határforgalom-ellenőrzések hatékonyságának és eredményességének javítása;
- b) az illegális bevándorlás megelőzéséhez és az ellene folytatott küzdelemhez való hozzájárulás;
- c) hozzájárulás az Unióban a szabadság, a biztonság és a jog érvényesülésén alapuló uniós térség magas fokú biztonságához, beleértve a tagállamok területén a közbiztonság és a közrend fenntartását és a biztonság védelmét is;
- d) a közös vízümpolitika végrehajtásának javítása;
- e) segítségnyújtás a nemzetközi védelem iránti kérelmek vizsgálatához;
- f) hozzájárulás a terrorista bűncselekmények és egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez és nyomozásához;
- g) a személyazonosságukat igazolni nem tudó ismeretlen személyek vagy természeti katasztrófa, baleset vagy terroristámadás esetén az azonosítatlan emberi maradványok azonosításának elősegítése.

(2) Az (1) bekezdésben említett célokat az alábbiak révén kell megvalósítani:

- a) a személyek helyes azonosításának biztosítása;
- b) a személyazonossággal való visszaélés elleni küzdelemhez való hozzájárulás;
- c) az adatminőség javítása és az uniós információs rendszerekben tárolt adatokra vonatkozó minőségi követelmények harmonizálása az egyes rendszereket szabályozó jogi eszközök adatkezelési követelményeinek, valamint az adatvédelmi előírások és elvek egyidejű tiszteletben tartása mellett;
- d) az uniós információs rendszerek tagállami technikai és operatív végrehajtásának megkönnyítése és támogatása;
- e) az egyes uniós információs rendszerekre vonatkozó adatbiztonsági és adatvédelmi feltételek megerősítése, egyszerűsítése és egységesebbé tétele, a bizonyos adatkategóriák esetében biztosított különös védelem és biztosítékok sérelme nélkül;
- f) a kijelölt hatóságok EES-hez, VIS-hez, ETIAS-hoz és Eurodachoz való hozzáféréseinek egyszerűsítése, a hozzáférés szükséges és arányos feltételeinek biztosítása mellett;
- g) az EES, a VIS, az ETIAS, az Eurodac, a SIS és az ECRIS-TCN céljainak támogatása.

*3. cikk***Hatály**

(1) Ez a rendelet az EES, a VIS, az ETIAS, valamint a SIS vonatkozásában alkalmazandó.

(2) E rendelet azokra a személyekre alkalmazandó, akiknek személyes adatai az e cikk (1) bekezdésében említett uniós információs rendszerekben kezelhetők, és akiknek az adatait a 767/2008/EK rendelet 1. és 2. cikkében, az (EU) 2017/2226 rendelet 1. cikkében, az (EU) 2018/1240 rendelet 1. és 4. cikkében, az (EU) 2018/1860 rendelet 1. cikkében és az (EU) 2018/1861 rendelet 1. cikkében meghatározott célokból gyűjtik.

*4. cikk***Fogalommeghatározások**

E rendelet alkalmazásában:

1. „külső határok”: az (EU) 2016/399 rendelet 2. cikkének 2. pontjában meghatározott külső határok;
2. „határforgalom-ellenőrzés”: az (EU) 2016/399 rendelet 2. cikkének 11. pontjában meghatározott határforgalom-ellenőrzés;
3. „határforgalom-ellenőrzést végző hatóság”: az a határőr, akit a nemzeti jognak megfelelően határforgalom-ellenőrzés elvégzésére kijelöltek;
4. „felügyeleti hatóságok”: az (EU) 2016/679 rendelet 51. cikkének (1) bekezdésében említett felügyeleti hatóság és az (EU) 2016/680 irányelv 41. cikkének (1) bekezdésében említett felügyeleti hatóság;
5. „ellenőrzés”: az adatcsoportok összehasonlításának folyamata, amelynek célja a közölt személyazonosság érvényességének megállapítása (egy az egyhez megfeleltetés);
6. „személyazonosítás”: egy személy személyazonosságának több adatcsoport és adatbázis összehasonlításával történő megállapítása (egy a többhöz megfeleltetés);
7. „alfanumerikus adatok”: betűkből, számokból, speciális karakterekből, szóközökből és központozási jelekből álló adatok;
8. „személyazonosító adatok”: a 27. cikk (3) bekezdésének a)–e) pontjában említett adatok;
9. „ujjnyomatadatok”: ujjnyomatok és látens ujjnyomok képmásai, amelyek egyedi jellegűeknek és a bennük foglalt referenciapontoknak köszönhetően lehetővé teszik az adott személy személyazonosságával kapcsolatos pontos és kétséget kizáró összehasonlításokat;
10. „arcképmás”: a személy arcáról készült digitális felvételek;
11. „biometrikus adatok”: az ujjnyomatadatok vagy az arcképmás, vagy mindkettő;
12. „biometrikus sablon”: a biometrikus adatok jellemzőinek leképezése útján nyert matematikai ábrázolás, ami a személyazonosítások és az ellenőrzések elvégzéséhez szükséges jellegzetességekre korlátozódik;
13. „úti okmány”: útlevél vagy azzal egyenértékű egyéb okmány, amely feljogosítja birtokosát a külső határ átlépésére és vízummal látható el;
14. „útiokmány-adatok”: az úti okmány típusa, száma és a kibocsátó ország, az úti okmány érvényességének lejárat dátuma és az úti okmányt kiállító ország hárombetűs kódja;
15. „uniós információs rendszerek”: az EES, a VIS, az ETIAS, az Eurodac, a SIS és az ECRIS-TCN;
16. „Europol-adatok”: az Europol által az (EU) 2016/794 rendelet 18. cikke (2) bekezdésének a), b) és c) pontjában említett célből kezelt személyes adatok;
17. „Interpol-adatbázisok”: az Interpol ellopott és elvesztett úti okmányokat tartalmazó adatbázisa (SLTD adatbázis) és az Interpol-körzésben megjelölt úti okmányok adatbázisa (TDAWN adatbázis);
18. „egyezés”: olyan megfelelés megléte, ami a valamely információs rendszerben vagy adatbázisban rögzített vagy rögzítés alatt álló személyes adatok automatizált összehasonlításának eredménye;
19. „rendőri hatóság”: az (EU) 2016/680 irányelv 3. cikkének 7. pontja szerinti illetékes hatóság;
20. „kijelölt hatóságok”: az (EU) 2017/2226 rendelet 3. cikke (1) bekezdésének 26. pontjában, a 2008/633/IB határozat 2. cikke (1) bekezdésének e) pontjában és az (EU) 2018/1240 rendelet 3. cikke (1) bekezdésének 21. pontjában meghatározott kijelölt hatóságok;

21. „terrorista bűncselekmény”: az a nemzeti jog szerinti bűncselekmény, amely megfelel az (EU) 2017/541 európai parlamenti és tanácsi irányelvben <sup>(35)</sup> említett bűncselekmények valamelyikének, vagy azzal egyenértékű;
22. „súlyos bűncselekmény” az a bűncselekmény, amely megfelel a 2002/584/IB tanácsi kerethatározat <sup>(36)</sup> 2. cikkének (2) bekezdésében említett valamely bűncselekménynek, vagy azzal egyenértékű, amennyiben esetében a nemzeti jog alapján kiszabható büntetési tétel felső határa legalább három év szabadságvesztés vagy szabadságelvonással járó intézkedés;
23. „határregisztrációs rendszer” vagy „EES”: az (EU) 2017/2226 rendelet által létrehozott határregisztrációs rendszer;
24. „vízuminformációs rendszer” vagy „VIS”: a 767/2008/EK rendelettel létrehozott vízuminformációs rendszer;
25. „Európai Utasinformációs és Engedélyezési Rendszer” vagy „ETIAS” az (EU) 2018/1240 rendelettel létrehozott Európai Utasinformációs és Engedélyezési Rendszer;
26. „Eurodac”: a 603/2013/EU európai parlamenti és tanácsi rendelettel <sup>(37)</sup> létrehozott Eurodac;
27. „Schengeni Információs Rendszer” vagy „SIS”: az (EU) 2018/1860, az (EU) 2018/1861 és az (EU) 2018/1862 rendelettel létrehozott Schengeni Információs Rendszer;
28. „ECRIS-TCN”: az (EU) 2019/816 európai parlamenti és tanácsi rendelettel <sup>(38)</sup> létrehozott, a harmadik országbeli állampolgárokkal és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval rendelkező tagállamok azonosítására szolgáló központosított rendszer.

## 5. cikk

### Megkülönböztetésmentesség és alapvető jogok

A személyes adatok e rendelet alkalmazásában történő kezelése nem eredményezheti a személyek semmilyen fajta, például nem, fajon, bőrszínen, etnikai vagy társadalmi származáson, genetikai jellemzőkön, nyelven, valláson vagy meggyőződésen, politikai vagy más véleményen, nemzeti kisebbséghez való tartozáson, vagyoni helyzeten, születésen, fogyatékoságon, életkoron vagy szexuális irányultságon alapuló megkülönböztetését. A személyes adatok kezelése során teljes mértékben tiszteletben kell tartani az emberi méltóságot és sérthetlenséget, valamint az alapvető jogokat, többek között a magánélet tiszteletben tartására és a személyes adatok védelmére vonatkozó jogot. Különös figyelmet kell fordítani a gyermekekre, az idősekre, a fogyatékosággal élő személyekre és a nemzetközi védelemre szoruló személyekre. A gyermek mindenképp felett álló érdekeire kiemelt figyelmet kell fordítani.

## II. FEJEZET

### Európai keresőportál

## 6. cikk

### Európai keresőportál

(1) Az európai keresőportál (ESP) létrehozásának célja a tagállami hatóságok és az uniós ügynökségek gyors, akadálytalan, hatékony, szisztematikus és ellenőrzött hozzáféréseinek megkönnyítése az uniós információs rendszerekhez, az Europol-adatokhoz és az Interpol-adatbázisokhoz feladataik ellátása céljából, összhangban hozzáférési jogosultságokkal és az EES, a VIS, az ETIAS, az Eurodac, a SIS, és az ECRIS-TCN céljaival és célkitűzéseivel.

<sup>(35)</sup> Az Európai Parlament és a Tanács (EU) 2017/541 irányelve (2017. március 15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról (HL L 88., 2017.3.31., 6. o.).

<sup>(36)</sup> A Tanács 2002/584/IB kerethatározata (2002. június 13.) az európai elfogatóparancsról és a tagállamok közötti átadási eljárásokról (HL L 190., 2002.7.18., 1. o.).

<sup>(37)</sup> Az Európai Parlament és a Tanács 603/2013/EU rendelete (2013. június 26.) a harmadik országbeli állampolgár vagy hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról szóló 604/2013/EU rendelet hatékony alkalmazása érdekében az újjelenyomatok összehasonlítását szolgáló Eurodac létrehozásáról, továbbá a tagállamok bűnüldöző hatóságai és az Europol által az Eurodac-adatokkal való, bűnüldözési célú összehasonlítások kérelmezéséről, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző ügynökség létrehozásáról szóló 1077/2011/EU rendelet módosításáról (HL L 180., 2013.6.29., 1. o.).

<sup>(38)</sup> Az Európai Parlament és a Tanács (EU) 2019/816 rendelete (2019. április 17.) az Európai Bűnügyi Nyilvántartási Információs Rendszer kiegészítése érdekében a harmadik országbeli állampolgárokkal és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval rendelkező tagállamok azonosítására szolgáló központosított rendszer (ECRIS-TCN) létrehozásáról, valamint az (EU) 2018/1726 rendelet módosításáról (lásd e Hivatalos Lap 1. oldalát).

- (2) Az ESP összetevői:
- egy keresőportált is tartalmazó központi infrastruktúra, amely lehetővé teszi az EES, a VIS, az ETIAS, az Eurodac, a SIS, az ECRIS-TCN, valamint az Europol-adatok és az Interpol-adatbázisok egyidejű lekérdezését;
  - egy biztonságos kommunikációs csatorna az ESP, a tagállamok és az uniós ügynökségek között, amelyek jogosultak az ESP használatára;
  - egy biztonságos kommunikációs infrastruktúra az ESP és az EES, a VIS, az ETIAS, az Eurodac, a központi SIS, az ECRIS-TCN, az Europol-adatok és az Interpol-adatbázisok között, valamint az ESP és a CIR és a MID központi infrastruktúrái között.
- (3) Az eu-LISA kifejleszti az ESP-t, és gondoskodik annak műszaki irányításáról.

### 7. cikk

#### **Az európai keresőportál használata**

(1) Az ESP használatára kizárólag azon tagállami hatóságok és uniós ügynökségek jogosultak, amelyek az uniós információs rendszereket szabályozó jogi eszközökkel összhangban hozzáféréssel rendelkeznek legalább egy uniós információs rendszerhez, e rendelettel összhangban hozzáféréssel rendelkeznek a CIR-hez és a MID-hez, az (EU) 2016/794 rendelettel összhangban hozzáféréssel rendelkeznek az Europol-adatokhoz, vagy az ilyen hozzáférést szabályozó uniós vagy nemzeti joggal összhangban hozzáféréssel rendelkeznek az Interpol-adatbázisokhoz.

Ezek a tagállami hatóságok és uniós ügynökségek csak az említett uniós információs rendszereket szabályozó jogi eszközökben, az (EU) 2016/794 rendeletben és az e rendeletben meghatározott célokból használhatják az ESP-t és az általa rendelkezésre bocsátott adatokat.

(2) Az (1) bekezdésben említett tagállami hatóságok és uniós ügynökségek az ESP-t személyekre vagy azok úti okmányaira vonatkozó adatoknak az EES, a VIS és az ETIAS központi rendszereiben történő keresésére használják, az említett uniós információs rendszereket szabályozó jogi eszközökben említett és a nemzeti jog szerinti hozzáférési jogosultságaikkal összhangban. Az ESP-t ezen kívül – e rendeletben meghatározott hozzáférési jogosultságaikkal összhangban és a 20., a 21. és a 22. cikk szerinti célokból – a CIR lekérdezésére is használják.

(3) Az (1) bekezdésben említett tagállami hatóságok az ESP-t személyekre vagy azok úti okmányaira vonatkozó adatoknak az (EU) 2018/1860 és az (EU) 2018/1861 rendeletben említett központi SIS-ben történő keresésére használhatják.

(4) Ha az uniós jog ekként rendelkezik, az (1) bekezdésben említett uniós ügynökségek az ESP-t személyekre vagy azok úti okmányaira vonatkozó adatoknak a központi SIS-ben történő keresésére használják.

(5) Az (1) bekezdésben említett tagállami hatóságok és uniós ügynökségek az ESP-t úti okmányokra vonatkozó adatoknak az Interpol-adatbázisokban történő keresésére használhatják, amennyiben az uniós jog és a nemzeti jog ekként rendelkezik, az abban foglalt hozzáférési jogosultságaikkal összhangban.

### 8. cikk

#### **Az európai keresőportál felhasználói számára készült profilok**

(1) Az ESP használatának lehetővé tétele érdekében az eu-LISA a tagállamokkal együttműködve a (2) bekezdésben említett technikai részletekkel és hozzáférési jogokkal összhangban profilt hoz létre minden egyes ESP-felhasználói kategória és a lekérdezések célja alapján. Minden egyes profil az uniós és a nemzeti joggal összhangban az alábbi információkat foglalja magában:

- a lekérdezéshez használandó adatmezők;
- azok az uniós információs rendszerek, Europol-adatok és Interpol-adatbázisok, amelyeket le kell, illetve amelyeket le lehet kérdezni, és amelyek a felhasználónak választ kell, hogy adjanak;
- az uniós információs rendszerek, az Europol-adatok és az Interpol-adatbázisok azon konkrét adatai, amelyek lekérdezhetők;
- az egyes válaszokban rendelkezésre bocsátható adatkategóriák.

(2) A Bizottság végrehajtási jogi aktusokat fogad el az (1) bekezdésben említett profilok technikai részleteinek meghatározása céljából, az ESP-felhasználóknak az uniós információs rendszereket szabályozó jogi eszközök és a nemzeti jog szerinti hozzáférési jogosultságaival összhangban. Ezeket a végrehajtási jogi aktusokat a 74. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(3) Az (1) bekezdésben említett profilokat az eu-LISA a tagállamokkal együttműködésben rendszeresen, legalább évente egyszer felülvizsgálja és szükség esetén frissíti.

#### 9. cikk

#### Lekérdezések

(1) Az ESP-felhasználó a lekérdezést alfanumerikus vagy biometrikus adatok ESP-be történő bevitelére kezdeményezi. Ha lekérdezést kezdeményeztek, az ESP a felhasználó által bevitt adatokkal és a felhasználói profilnak megfelelően egyidejűleg végez lekérdezést az EES-ben, az ETIAS-ban, a VIS-ben, a SIS-ben, az Eurodacban, az ECRIS-TCN-ben, a CIR-ben, az Europol-adatokban és az Interpol-adatbázisokban.

(2) Az ESP útján történő lekérdezés kezdeményezéséhez használt adatkategóriák megfelelnek a különböző uniós információs rendszerek, az Europol-adatok és az Interpol-adatbázisok lekérdezésére felhasználható, személyekre vagy úti okmányokra vonatkozó adatkategóriáknak, a rájuk irányadó jogi eszközöknek megfelelően.

(3) Az eu-LISA a tagállamokkal együttműködésben az ESP vonatkozásában a 38. cikkben említett UMF-n alapuló interfészvezérlési dokumentációt alkalmaz.

(4) A lekérdezés ESP-felhasználó általi kezdeményezése esetén az EES, az ETIAS, a VIS, a SIS, az Eurodac, az ECRIS-TCN, a CIR és a MID, valamint az Europol-adatok és az Interpol-adatbázisok a lekérdezésre válaszként rendelkezésre bocsátják az általuk tárolt adatokat.

A 20. cikk sérelme nélkül az ESP által adott válasznak jeleznie kell, hogy az adatok mely uniós információs rendszerben vagy adatbázisban található meg.

Az ESP nem szolgáltat információkat az uniós információs rendszerekben tárolt olyan adatokról, olyan Europol-adatokról és az olyan Interpol-adatbázisokról, amelyekhez a felhasználónak az alkalmazandó uniós és nemzeti jog szerint nincs hozzáférése.

(5) Az ESP-n keresztül kezdeményezett, Interpol-adatbázisokra irányuló lekérdezéseket úgy kell elvégezni, hogy az információk ne jussanak az Interpol-riasztás rögzítőjének tudomására.

(6) Az ESP választ ad a felhasználónak, amint az egyik uniós információs rendszerben, az Europol-adatok között vagy az Interpol-adatbázisokban rendelkezésre áll az adat. Ezek a válaszok csak azokat az adatokat tartalmazzák, amelyekhez a felhasználó az uniós és a nemzeti jog alapján hozzáféréssel rendelkezik.

(7) A Bizottság végrehajtási jogi aktust fogad el az uniós információs rendszerek, az Europol-adatok és az Interpol-adatbázisok ESP általi lekérdezésére vonatkozó technikai eljárásnak és az ESP által adott válaszok formátumának meghatározására. Ezeket a végrehajtási jogi aktusokat a 74. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

#### 10. cikk

#### Naplóvezetés

(1) Az (EU) 2017/2226 rendelet 46. cikkének, a 767/2008/EK rendelet 34. cikkének, az (EU) 2018/1240 rendelet 69. cikkének, valamint az (EU) 2018/1861 rendelet 12. és 18. cikkének sérelme nélkül, az eu-LISA az ESP-n végzett valamennyi adatkezelési műveletről naplót vezet. A napló az alábbiakat tartalmazza:

- a) a lekérdezést kezdeményező tagállam vagy uniós ügynökség és a használt ESP profil;
- b) a lekérdezés napja és időpontja;
- c) azon uniós információs rendszerek és Interpol-adatbázisok, amelyekben lekérdezést végeztek.

(2) Minden tagállam naplót vezet az ESP használatára megfelelő felhatalmazással rendelkező hatóságai által és e hatóságok megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről. Minden uniós ügynökség naplót vezet a megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről.

(3) Az (1) és a (2) bekezdésben említett naplókat kizárólag az adatvédelmi ellenőrzés érdekében – ideértve a lekérdezés elfogadhatóságának és az adatkezelés jogszerűségének ellenőrzését –, valamint az adatbiztonság és az adatok sértetlensége biztosításának céljára lehet felhasználni. E naplókat megfelelő intézkedésekkel kell védeni a jogosulatlan hozzáféréstől, és létrehozásuk után egy évvel törölni kell. Ha azonban egy már megkezdett ellenőrzési eljáráshoz szükség van rájuk, akkor törlésükre akkor kell sort keríteni, amikor már nem szükségesek az ellenőrzési eljáráshoz.

### 11. cikk

#### **Tartalékeljárások arra az esetre, ha az európai keresőportál használata műszakilag lehetetlen**

(1) Ha az ESP-t annak meghibásodása miatt azt műszakilag lehetetlen egy vagy több uniós információs rendszer vagy a CIR lekérdezésére használni, az eu-LISA automatikusan értesíti erről az ESP-felhasználókat.

(2) Ha az ESP-t valamely tagállam nemzeti infrastruktúrájának meghibásodása miatt műszakilag lehetetlen egy vagy több uniós információs rendszer vagy a CIR lekérdezésére használni, e tagállam automatikusan értesíti erről az eu-LISA-t és a Bizottságot.

(3) Az e cikk (1) vagy (2) bekezdésében említett esetekben a műszaki hiba orvoslásáig a 7. cikk (2) és (4) bekezdésében foglalt kötelezettség nem alkalmazandó, és a tagállamok az uniós információs rendszerekhez vagy a CIR-hez közvetlenül férnek hozzá, ha az uniós vagy a nemzeti jog ezt előírja.

(4) Ha az ESP-t valamely uniós ügynökség infrastruktúrájának meghibásodása miatt műszakilag lehetetlen egy vagy több uniós információs rendszer vagy a CIR lekérdezésére használni, az adott ügynökség automatikusan értesíti erről az eu-LISA-t és a Bizottságot.

### III. FEJEZET

#### **Közös biometrikus megfeleltetési szolgáltatás**

### 12. cikk

#### **Közös biometrikus megfeleltetési szolgáltatás**

(1) Létrejön a 13. cikkben említett, a CIR-ben és a SIS-ben tárolt biometrikus adatokból kinyert biometrikus sablonokat tároló és több uniós információs rendszer biometrikus adatokkal történő lekérdezését lehetővé tevő közös biometrikus megfeleltetési szolgáltatás (közös BMS) a CIR és a MID támogatása, valamint az EES, a VIS, az Eurodac, a SIS és az ECRIS-TCN célkitűzéseinek elősegítése céljából.

(2) A közös BMS a következőkből áll:

- a) olyan központi infrastruktúra, amely az EES, a VIS, a SIS, az Eurodac és az ECRIS-TCN központi rendszereinek helyébe lép, amennyiben tárolja a biometrikus sablonokat és lehetővé teszi a biometrikus adatokkal való kereséseket;
- b) egy biztonságos kommunikációs infrastruktúra a közös BMS, a központi SIS és a CIR között.

(3) Az eu-LISA kifejleszti a közös BMS-t, és gondoskodik annak műszaki irányításáról.

### 13. cikk

#### **Biometrikus sablonok tárolása a közös biometrikus megfeleltetési szolgáltatásban**

(1) A közös BMS tárolja a biometrikus sablonokat, amelyeket az alábbi biometrikus adatokból nyer:

- a) az (EU) 2017/2226 rendelet 16. cikke (1) bekezdésének d) pontjában, 17. cikke (1) bekezdésének b) pontjában, valamint 18. cikke (2) bekezdésének a), b) és c) pontjában említett adatok;
- b) a 767/2008/EK rendelet 9. cikkének 6. pontjában említett adatok;

- c) az (EU) 2018/1861 rendelet 20. cikke (2) bekezdésének w) és x) pontjában említett adatok, a tenyérnyomatokra vonatkozó adatok kivételével;
- d) az (EU) 2018/1860 rendelet 4. cikke (1) bekezdésének u) és v) pontjában említett adatok, a tenyérnyomatokra vonatkozó adatok kivételével.

A biometrikus sablonokat a közös BMS logikailag különválasztva tárolja azon információs rendszerek szerint, amelyekből az adatok származnak.

(2) A közös BMS az (1) bekezdésben említett valamennyi adatcsoport vonatkozásában minden biometrikus sablonban hivatkozást tartalmaz azokra az uniós információs rendszerekre, amelyekben a megfelelő biometrikus adatokat tárolják, és ezen uniós információs rendszerek konkrét bejegyzéseire.

(3) A biometrikus sablonokat csak azt követően lehet bevinni a közös BMS-be, hogy a közös BMS elvégezte a valamelyik uniós információs rendszerhez hozzáadott biometrikus adatok automatizált minőség-ellenőrzését annak biztosítása céljából, hogy az adatminőségi minimumkövetelmények teljesüljenek.

(4) Az (1) bekezdésben említett adatok tárolásának meg kell felelnie a 37. cikk (2) bekezdésében említett minőségi követelményeknek.

(5) A Bizottság végrehajtási jogi aktus révén meghatározza a közös BMS teljesítményének nyomon követésére vonatkozó teljesítmény-követelményeket és gyakorlati szabályokat annak biztosítása érdekében, hogy a biometrikus keresések hatékonysága megfeleljen az olyan időtartam szempontjából érzékeny eljárásoknak, mint például a határforgalom-ellenőrzések és a személyazonosítások. Ezeket a végrehajtási jogi aktusokat a 74. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

#### 14. cikk

### **Biometrikus adatok keresése a közös biometrikus megfeleltetési szolgáltatással**

A CIR-ben és a SIS-ben tárolt biometrikus adatok keresése céljából a CIR és a SIS a közös BMS-ben tárolt biometrikus sablonokat használja. Biometrikus adatokkal történő lekérdezés az e rendeletben, illetve a 767/2008/EK, az (EU) 2017/2226, az (EU) 2018/1860, az (EU) 2018/1861, az (EU) 2018/1862 és az (EU) 2019/816 rendeletben előírt célokból végezhető.

#### 15. cikk

### **Adatmegőrzés a közös biometrikus megfeleltetési szolgáltatás keretében**

A 13. cikk (1) és (2) bekezdésében említett adatokat kizárólag addig lehet tárolni a közös BMS rendszerben, amíg a megfelelő biometrikus adatokat a CIR vagy a SIS tárolja. Ezeket az adatokat automatikusan törölni kell a közös BMS-ből.

#### 16. cikk

### **Naplóvezetés**

(1) Az (EU) 2017/2226 rendelet 46. cikkének, a 767/2008/EK rendelet 34. cikkének, valamint az (EU) 2018/1861 rendelet 12. és 18. cikkének sérelme nélkül, az eu-LISA a közös BMS-en végzett valamennyi adatkezelési műveletről naplót vezet. A napló az alábbiakat tartalmazza:

- a) a lekérdezést kezdeményező tagállam vagy uniós ügynökség;
- b) a biometrikus sablonok létrehozásával és tárolásával kapcsolatos előzmények;
- c) azon uniós információs rendszerek, amelyekben a közös BMS-ben tárolt biometrikus sablonokkal lekérdezést végeztek;
- d) a lekérdezés napja és időpontja;
- e) a lekérdezés kezdeményezéséhez használt biometrikus adatok típusa;
- f) a lekérdezés eredményei, valamint az eredmény elérésének napja és időpontja.

(2) Minden tagállam naplót vezet a közös BMS használatára megfelelő felhatalmazással rendelkező hatóságai által és e hatóságok megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről. Minden uniós ügynökség naplót vezet a megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről.

(3) Az (1) és a (2) bekezdésben említett naplókat kizárólag az adatvédelmi ellenőrzés érdekében – ideértve a lekérdezés elfogadhatóságának és az adatkezelés jogszerűségének ellenőrzését –, valamint az adatbiztonság és az adatok sértetlensége biztosításának céljára lehet felhasználni. E naplókat megfelelő intézkedésekkel kell védeni a jogosulatlan hozzáféréstől, és létrehozásuk után egy évvel törölni kell. Ha azonban egy már megkezdett ellenőrzési eljáráshoz szükség van rájuk, akkor törlésükre akkor kell sort keríteni, amikor már nem szükségesek az ellenőrzési eljáráshoz.

#### IV. FEJEZET

### **Közös személyazonosítóadat-tár**

#### 17. cikk

### **Közös személyazonosítóadat-tár**

(1) Létrejön az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban vagy az ECRIS-TCN-ben nyilvántartott valamennyi személy vonatkozásában egyéni aktát létrehozó, a 18. cikk szerinti adatokat tartalmazó közös személyazonosítóadat-tár (CIR), az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban és az ECRIS-TCN-ben nyilvántartott személyek 20. cikkel összhangban történő helyes azonosításának megkönnyítése és segítése, a 21. cikkel összhangban a MID működésének támogatása, valamint a kijelölt hatóságok és az Europol EES-hez, VIS-hez, ETIAS-hoz és Eurodachoz való hozzáféréseinek megkönnyítése és észszerűsítése céljából, amikor ez terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez vagy nyomozásához szükséges a 22. cikkel összhangban.

(2) A CIR a következőkből áll:

- a) egy központi infrastruktúra, amely a 18. cikkben említett adatok tárolásához szükséges mértékben az EES, a VIS, az ETIAS, az Eurodac és az ECRIS-TCN központi rendszereinek helyébe lép;
- b) a CIR és az uniós és nemzeti jog alapján a CIR használatára jogosult tagállamok és uniós ügynökségek közötti biztonságos kommunikációs csatorna;
- c) egy biztonságos kommunikációs infrastruktúra a CIR és az EES, a VIS, az ETIAS, az Eurodac és az ECRIS-TCN között, valamint az ESP, a közös BMS és a MID központi infrastruktúráival.

(3) Az eu-LISA kifejleszti a CIR-t, és gondoskodik annak műszaki irányításáról.

(4) Ha a CIR meghibásodása miatt műszakilag lehetetlen lekérdezést végezni a CIR-ben személyazonosítás céljából a 20. cikk szerint, a többszörös személyazonosság észlelése céljából a 21. cikk szerint vagy terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából a 22. cikk szerint, az eu-LISA automatikusan értesíti erről a CIR-felhasználókat.

(5) Az eu-LISA a tagállamokkal együttműködésben a CIR vonatkozásában a 38. cikkben említett UMF-n alapuló interfészvezérlési dokumentációt alkalmaz.

#### 18. cikk

### **A közös személyazonosítóadat-tár adatai**

(1) A CIR a következő adatokat logikailag különválasztva tárolja azon információs rendszerek szerint, amelyekből az adatok származnak:

- a) az (EU) 2017/2226 rendelet 16. cikke (1) bekezdésének a)–d) pontjában, 17. cikke (1) bekezdésének a), b) és c) pontjában, valamint 18. cikkének (1) és (2) bekezdésében említett adatok;
- b) a 767/2008/EK rendelet 9. cikke 4. pontjának a)–c) alpontjában, valamint 5. és 6. pontjában említett adatok;
- c) az (EU) 2018/1240 rendelet 17. cikke (2) bekezdésének a)–e) pontjában említett adatok.

(2) A CIR az (1) bekezdésben említett minden adatcsoport esetében hivatkozást tartalmaz azon uniós információs rendszerekre, amelyekhez az adatok tartoznak.



(3) A CIR-hez hozzáférő hatóságok az uniós információs rendszereket szabályozó jogi eszközökben említett és a nemzeti jog, valamint az e rendelet szerinti hozzáférési jogosultságaikkal összhangban járnak el a hozzáférés során a 20., a 21. és a 22. cikkben említett célokból.

(4) A CIR az (1) bekezdésben említett minden adatszoport tekintetében hivatkozást tartalmaz az uniós információs rendszerek azon konkrét bejegyzésére, amelyhez az adatok tartoznak.

(5) Az (1) bekezdésben említett adatok tárolásának meg kell felelnie a 37. cikk (2) bekezdésében foglalt minőségi követelményeknek.

#### 19. cikk

##### **Adatok hozzáadása, módosítása és törlése a közös személyazonosítóadat-tárban**

(1) Adatoknak az EES-ben, a VIS-ben és az ETIAS-ban történő hozzáadása, módosítása vagy törlése esetén a 18. cikkben említett, a CIR egyéni aktájában tárolt adatokat ennek megfelelően automatikusan ki kell egészíteni, módosítani, vagy törölni kell.

(2) Amennyiben a MID-ben a 32. vagy a 33. cikk szerinti fehér vagy vörös kapcsolatot hoznak létre a CIR-t alkotó két vagy több uniós információs rendszer adatai között, a CIR új egyéni akta létrehozása helyett hozzáadja az új adatokat az összekapcsolt adatok egyéni aktájához.

#### 20. cikk

##### **Hozzáférés a közös személyazonosítóadat-tárhoz személyazonosítás céljából**

(1) A CIR lekérdezését a rendőri hatóság csak az alábbi körülmények között, a (2) és az (5) bekezdésnek megfelelően hajthatja végre:

- a) amennyiben a rendőri hatóság úti okmány vagy az adott személy személyazonosságát hitelt érdemlően igazoló más dokumentum hiányában nem tud azonosítani egy személyt;
- b) amennyiben kétség merül fel a személy által rendelkezésre bocsátott személyazonosító adatokat illetően;
- c) amennyiben kétség merül fel a személy által rendelkezésre bocsátott úti okmány vagy más hitelt érdemlő dokumentum eredetiségét illetően;
- d) amennyiben kétség merül fel az úti okmány vagy más hitelt érdemlő dokumentum birtokosának személyazonosságát illetően; vagy
- e) ha a személy nem tud vagy nem akar együttműködni.

Ilyen lekérdezések 12 év alatti kiskorúak esetében nem végezhetők, kivéve, ha ezt a gyermek mindenek felett álló érdeke megkívánja.

(2) Amennyiben felmerül az (1) bekezdésben felsorolt körülmények egyike és a rendőri hatóságot az (5) bekezdésben említett nemzeti jogalkotási intézkedések arra felhatalmazták, az kizárólag valamely személy azonosítása céljából jogosult a CIR lekérdezésére az illető személy személyazonosságának ellenőrzése során közvetlenül a helyszínen nyert biometrikus adatokkal, amennyiben az eljárást az adott személy jelenlétében kezdeményezték.

(3) Amennyiben a lekérdezés azt jelzi, hogy a CIR tárol az adott személyre vonatkozó adatokat, a rendőri hatóság betekintés céljából hozzáféréssel rendelkezik a 18. cikk (1) bekezdésében említett adatokhoz.

Amennyiben a személy biometrikus adatai nem használhatók, vagy ha az ilyen adatokkal történő lekérdezés sikertelen, a lekérdezést a személy személyazonosító adataival és az útiokmány-adatokkal együttesen, vagy az adott személy által szolgáltatott személyazonosító adatokkal kell elvégezni.

(4) Amennyiben a rendőri hatóságot a (6) bekezdésben említett nemzeti jogalkotási intézkedések felhatalmazták arra, az adott rendőri hatóság természeti katasztrófa, baleset vagy terrortámadás esetén és kizárólag a személyazonosságukat igazolni nem tudó ismeretlen személyek vagy az azonosítatlan emberi maradványok azonosítása céljából e személyek biometrikus adataival lekérdezheti a CIR-t.

(5) Azok a tagállamok, amelyek élni kívánnak a (2) bekezdésben biztosított lehetőséggel, nemzeti jogalkotási intézkedéseket fogadnak el. Ennek során a tagállamok figyelembe veszik, hogy el kell kerülni a harmadik országok állampolgáiraival szembeni mindennemű megkülönböztetést. E jogalkotási intézkedésekben meg kell határozni, hogy a 2. cikk (1) bekezdésének b) és c) pontjában szereplő célkitűzések körén belül melyek a személyazonosítás pontos céljai. A jogalkotási intézkedésekben ki kell jelölni az illetékes rendőri hatóságokat, és meg kell állapítani az ilyen ellenőrzésekre irányadó eljárásokat, feltételeket és kritériumokat.

(6) Azok a tagállamok, amelyek élni kívánnak a (4) bekezdésben foglalt lehetőséggel, nemzeti jogalkotási intézkedéseket fogadnak el, amelyben meghatározzák az eljárásokat, a feltételeket és a kritériumokat.

#### 21. cikk

##### **Hozzáférés a közös személyazonosítóadat-tárhoz a többszörös személyazonosság észlelése céljából**

(1) Amennyiben a CIR lekérdezése a 28. cikk (4) bekezdése szerinti sárga kapcsolatot eredményez, a különböző személyazonosságoknak a 29. cikk szerinti manuális ellenőrzéséért felelős hatóság – kizárólag ezen ellenőrzés céljából – hozzáféréssel rendelkezik a sárga kapcsolattal összekapcsolt, CIR-ben tárolt, a 18. cikk (1) és (2) bekezdésében említett adatokhoz.

(2) Amennyiben a CIR lekérdezése a 32. cikk szerinti vörös kapcsolatot eredményez, a 26. cikk (2) bekezdésében említett hatóságok – kizárólag a személyazonossággal való visszaélés elleni küzdelem céljából – hozzáféréssel rendelkeznek a vörös kapcsolattal összekapcsolt, CIR-ben tárolt, a 18. cikk (1) és (2) bekezdésében említett adatokhoz.

#### 22. cikk

##### **A közös személyazonosítóadat-tár lekérdezése terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából**

(1) Konkrét esetekben, amennyiben alapos okkal feltételezhető, hogy az uniós információs rendszerekbe való betekintés hozzájárul a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez vagy nyomozásához, különösen ha fennáll annak a gyanúja, hogy egy terrorista bűncselekmény vagy egyéb súlyos bűncselekmény elkövetésével gyanúsított személy, az ilyen bűncselekmények elkövetője vagy áldozata olyan személy, akinek adatait az EES-ben, a VIS-ben vagy az ETIAS-ban tárolják, a kijelölt hatóságok és az Europol betekintheznek a CIR-be azon információ megszerzése érdekében, hogy egy adott személyre vonatkozó adatok szerepelnek-e az EES-ben, a VIS-ben vagy az ETIAS-ban.

(2) Amennyiben a lekérdezésre válaszként a CIR azt jelzi, hogy az EES-ben, a VIS-ben vagy az ETIAS-ban szerepelnek az adott személyre vonatkozó adatok, a CIR a kijelölt hatóságoknak és az Europolnak a 18. cikk (2) bekezdésében említett hivatkozás formájában ad választ, amely megjelöli, hogy melyik uniós információs rendszer tartalmaz egyező adatokat. A CIR olyan módon ad választ, amely nem veszélyeztetheti az adatbiztonságot.

A választ, amely szerint az adott személyre vonatkozóan szerepelnek adatok az (1) bekezdésben említett valamely uniós információs rendszerben, csak arra a célra lehet felhasználni, hogy hozzáférés iránti kérelmet nyújtsanak be az ilyen hozzáférésre vonatkozó megfelelő jogi eszközökben meghatározott feltételekkel és eljárások révén.

Egyezés vagy többszörös egyezés esetén a kijelölt hatóság vagy az Europol teljes körű hozzáférésre vonatkozó kérelmet nyújt be legalább egy olyan információs rendszerhez, amelyből a lekérdezésre adott választ egyezést jelez.

Ha kivételesen nem nyújtanak be ilyen teljes körű hozzáférésre irányuló kérelmet, a kijelölt hatóságok a kérelem benyújtásának hiányára vonatkozó indokolást visszakereshető módon rögzítik a nemzeti aktában. Az Europol rögzíti az indokolást a megfelelő aktában.

(3) A terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából az EES-ben, a VIS-ben vagy az ETIAS-ban tárolt adatokhoz való teljes körű hozzáférés továbbra is az ilyen hozzáférést szabályozó megfelelő jogi eszközökben meghatározott feltételek és eljárások hatálya alá tartozik.

#### 23. cikk

##### **Adatmegőrzés a közös személyazonosítóadat-tárban**

(1) A 18. cikk (1), (2) és (4) bekezdésében említett adatokat az (EU) 2017/2226 rendelet, a 767/2008/EK rendelet és az (EU) 2018/1240 rendelet adatmegőrzésre vonatkozó rendelkezéseivel összhangban automatikusan törölni kell a CIR-ből.

(2) Az egyéni aktát a CIR-ben csak addig kell tárolni, amíg a megfelelő adatokat legalább azon uniós információs rendszerek egyike tárolja, amelyek adatait a CIR tartalmazza. A kapcsolat létrehozása nem befolyásolja az összekapcsolt adatok egyes elemeinek megőrzési időszakát.

#### 24. cikk

##### Naplóvezetés

(1) Az (EU) 2017/2226 rendelet 46. cikkének, a 767/2008/EK rendelet 34. cikkének és az (EU) 2018/1240 rendelet 69. cikkének sérelme nélkül, az eu-LISA e cikk (2), (3) és (4) bekezdésével összhangban a CIR-ben végzett valamennyi adatkezelési műveletről naplót vezet.

(2) Az eu-LISA a CIR-ben végzett, 20. cikk szerinti minden adatkezelési műveletről naplót vezet. A napló az alábbiakat tartalmazza:

- a) a lekérdezést kezdeményező tagállam vagy uniós ügynökség;
- b) a CIR-ben lekérdezést végző felhasználó hozzáféréseinek célja;
- c) a lekérdezés napja és időpontja;
- d) a lekérdezés kezdeményezéséhez használt adatok típusa;
- e) a lekérdezés eredményei.

(3) Az eu-LISA a CIR-ben végzett, 21. cikk szerinti minden adatkezelési műveletről naplót vezet. A napló az alábbiakat tartalmazza:

- a) a lekérdezést kezdeményező tagállam vagy uniós ügynökség;
- b) a CIR-ben lekérdezést végző felhasználó hozzáféréseinek célja;
- c) a lekérdezés napja és időpontja;
- d) amennyiben kapcsolat jön létre, a lekérdezés kezdeményezéséhez használt adatok és a lekérdezés eredményei azon uniós információs rendszer megjelölésével, amelyből az adatokat kapták.

(4) Az eu-LISA a CIR-ben végzett, 22. cikk szerinti minden adatkezelési műveletről naplót vezet. A napló az alábbiakat tartalmazza:

- a) a lekérdezés napja és időpontja;
- b) a lekérdezés kezdeményezéséhez használt adatok;
- c) a lekérdezés eredményei;
- d) a CIR-ben lekérdezést végző tagállam vagy uniós ügynökség.

Az ilyen hozzáférés nyomán keletkezett naplókat rendszeresen – hat hónapot meg nem haladó időközönként – ellenőrzi az illetékes felügyeleti hatóság az (EU) 2016/680 rendelet 41. cikkével összhangban, vagy az európai adatvédelmi biztos az (EU) 2016/794 rendelet 43. cikkével összhangban annak vizsgálata céljából, hogy az e rendelet 22. cikkének (1) és (2) bekezdésében meghatározott eljárásokat követték-e, és teljesültek-e az ott rögzített feltételek.

(5) Minden tagállam naplót vezet a CIR használatára a 20., a 21. és a 22. cikk alapján megfelelő felhatalmazással rendelkező hatóságai által és e hatóságok megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről. Minden uniós ügynökség naplót vezet a 21. és a 22. cikk alapján megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről.

Ezenkívül a CIR-hez való, 22. cikk szerinti valamennyi hozzáféréssel kapcsolatban minden tagállam naplóban rögzíti a következő adatokat:

- a) a nemzeti ügyiratszám;
- b) a hozzáférés célja;
- c) a nemzeti szabályokkal összhangban a lekérdezést végrehajtó tisztviselő és a lekérdezést elrendelő tisztviselő egyedi felhasználói azonosítója.

(6) Az (EU) 2016/794 rendelettel összhangban, az Europol a CIR-hez történő, e rendelet 22. cikke szerinti minden hozzáférés tekintetében naplót vezet a lekérdezést végrehajtó tisztviselő és a lekérdezést elrendelő tisztviselő egyedi felhasználói azonosítóját.

(7) A (2)–(6) bekezdésben említett naplókat kizárólag az adatvédelmi ellenőrzés érdekében – ideértve a lekérdezés elfogadhatóságának és az adatkezelés jogszerűségének ellenőrzését –, valamint az adatbiztonságnak és az adatok sértetlensége biztosításának céljára lehet felhasználni. E naplókat megfelelő intézkedésekkel kell védeni a jogosulatlan hozzáféréstől, és létrehozásuk után egy évvel törölni kell. Ha azonban egy már megkezdett ellenőrzési eljáráshoz szükség van rájuk, akkor törlésükre akkor kell sort keríteni, amikor már nem szükségesek az ellenőrzési eljáráshoz.

(8) Az eu-LISA az egyéni aktákban megőrzi a tárolt adatok előzményeivel kapcsolatos naplókat. Az eu-LISA az adatok törlése után automatikusan törli ezeket a naplókat.

## V. FEJEZET

### **A többszörös személyazonosságot észlelő rendszer**

#### 25. cikk

### **A többszörös személyazonosságot észlelő rendszer**

(1) Létrejön a többszörös személyazonosságot észlelő rendszer (MID), amely létrehozza és tárolja a 34. cikkben említett, személyazonosságot megerősítő dossziékat, tartalmazza az uniós információs rendszerekben – köztük a CIR-ben és a SIS-ben – található adatok közötti kapcsolatokat, és lehetővé teszi a személyazonosság-ellenőrzés megkönnyítése és egyidejűleg a személyazonossággal való visszaélés elleni küzdelem érdekében a többszörös személyazonosságok észlelését; a MID létrehozásának célja a CIR működésének, valamint az EES, a VIS, az ETIAS, az Eurodac, a SIS és az ECRIS-TCN céljainak támogatása.

(2) A MID a következőkből áll:

- a) a kapcsolatokat és az uniós információs rendszerekre való hivatkozásokat tároló központi infrastruktúra;
- b) egy biztonságos kommunikációs infrastruktúra, amely a MID-et összekapcsolja a SIS-szel, valamint az ESP és a CIR központi infrastruktúráival.

(3) Az eu-LISA kifejleszti a MID-et, és gondoskodik annak műszaki irányításáról.

#### 26. cikk

### **Hozzáférés a többszörös személyazonosságot észlelő rendszerhez**

(1) A különböző személyazonosságok 29. cikkben említett manuális ellenőrzése céljából a MID-ben tárolt, a 34. cikkben említett adatokhoz az alábbiaknak kell hozzáférést adni:

- a) az (EU) 2017/2226 rendelet 9. cikkének (2) bekezdésével összhangban kijelölt illetékes hatóságok, amikor az említett rendelet 14. cikkével összhangban az EES-ben létrehozzák vagy frissítik az egyéni aktát;
- b) a 767/2008/EK rendelet 6. cikkének (1) bekezdésében említett vízumhatóságok, amikor az említett rendelettel összhangban a VIS-ben létrehozzák vagy frissítik a kérelemfájlt;
- c) az ETIAS központi egysége és az ETIAS nemzeti egységei az (EU) 2018/1240 rendelet 22. és 26. cikkében említett feldolgozás elvégzésekor;
- d) az (EU) 2018/1861 és az (EU) 2018/1861 rendelettel összhangban SIS figyelmeztető jelzést létrehozó vagy frissítő tagállam SIRENE-irodája.

(2) A CIR-ben vagy a SIS-ben szereplő legalább egy uniós információs rendszerhez hozzáféréssel rendelkező tagállami hatóságok és uniós ügynökségek hozzáférést kapnak a 34. cikk a) és b) pontjában említett valamennyi, a 32. cikk szerinti vörös kapcsolatra vonatkozó adathoz.

(3) A tagállami hatóságok és az uniós ügynökségek hozzáférést kapnak a 33. cikk szerinti fehér kapcsolatokhoz, amennyiben hozzáféréssel rendelkeznek ahhoz a két uniós információs rendszerhez, amelyek tartalmazzák azokat az adatokat, amelyek között a fehér kapcsolat létrejött.

(4) A tagállami hatóságok és uniós ügynökségek hozzáférést kapnak a 31. cikk szerinti zöld kapcsolatokhoz, amennyiben hozzáféréssel rendelkeznek ahhoz a két uniós információs rendszerhez, amelyek tartalmazzák azokat az adatokat, amelyek között a zöld kapcsolat létrejött, és amennyiben az említett információs rendszerek lekérdezése egyezést eredményezett az összekapcsolt két adatscsoport között.

## 27. cikk

**A többszörös személyazonosság észlelése**

- (1) A többszörös személyazonosság észlelése céljából keresést kell kezdeményezni a CIR-ben és a SIS-ben, ha:
- a) az EES-ben az (EU) 2017/2226 rendelet 14. cikkével összhangban egyéni aktát hoznak létre vagy frissítenek;
  - b) a 767/2008/EK rendelet 8. cikkének megfelelően a VIS-ben kérelemfájl hoznak létre vagy frissítenek;
  - c) az ETIAS-ban az (EU) 2018/1240 rendelet 19. cikkének megfelelően kérelemfájl hoznak létre vagy frissítenek;
  - d) az (EU) 2018/1861 rendelet 3. cikkének és az (EU) 2018/1861 rendelet V. fejezetének megfelelően a SIS-ben egy adott személyre vonatkozó figyelmeztető jelzést hoznak létre vagy frissítenek.
- (2) Amennyiben az (1) bekezdésben említett valamely uniós információs rendszerben található adatok biometrikus adatokat tartalmaznak, a CIR és a központi SIS a közös BMS-t használja a többszörös személyazonosság észlelése céljából. A közös BMS összehasonlítja a bármely új biometrikus adatokból nyert biometrikus sablonokat a közös BMS-ben már szereplő biometrikus sablonokkal annak ellenőrzése érdekében, hogy ugyanazon személy adatai már szerepelnek-e a CIR-ben vagy a központi SIS-ben.
- (3) A (2) bekezdésben említett folyamaton túlmenően a CIR és a központi SIS az ESP-t használja a központi SIS-ben, illetve a CIR-ben tárolt adatok keresésére a következő adatok felhasználásával:
- a) vezetéknev (családi név), utónév vagy utónevek (keresztnevek), születési idő, állampolgárság vagy állampolgárságok és nem az (EU) 2017/2226 rendelet 16. cikke (1) bekezdésének a) pontjában, 17. cikke (1) bekezdésében és 18. cikke (1) bekezdésében említettek szerint;
  - b) vezetéknev (családi név), utónév vagy utónevek (keresztnevek), születési idő, nem, születési hely és ország, valamint állampolgárságok a 767/2008/EK rendelet 9. cikke 4. pontjának a) és aa) alpontjában említettek szerint;
  - c) vezetéknev (családi név), utónév vagy utónevek (keresztnev vagy keresztnevek), születéskori vezetéknev, álnév vagy álnevek, születési idő, születési hely, nem és jelenlegi állampolgárság az (EU) 2018/1240 rendelet 17. cikkének (2) bekezdésében említettek szerint;
  - d) vezetéknevek, utónevek, születési nevek, korábban használt nevek és álnevek, születési hely, születési idő, nem és állampolgárságok az (EU) 2018/1861 rendelet 20. cikkének (2) bekezdésében említettek szerint;
  - e) vezetéknevek, utónevek, születési nevek, korábban használt nevek és álnevek, születési hely, születési idő, nem és állampolgárságok az (EU) 2018/1860 rendelet 20. cikkének (4) bekezdésében említettek szerint.
- (4) A (2) és a (3) bekezdésben említett folyamaton túlmenően a CIR és a központi SIS az ESP-t használja a központi SIS-ben, illetve a CIR-ben tárolt adatok keresésére az útiokmány-adatok felhasználásával.
- (5) A többszörös személyazonosság észlelésére irányuló vizsgálat csak valamely uniós információs rendszerben rendelkezésre álló adatoknak más uniós információs rendszerekben rendelkezésre álló adatokkal való összehasonlítása céljából kezdeményezhető.

## 28. cikk

**A többszörös azonosság észlelésére irányuló vizsgálat eredményei**

- (1) Amennyiben a 27. cikk (2), (3) és (4) bekezdése szerinti lekérdezések nem eredményeznek egyezést, a 27. cikk (1) bekezdésében szereplő eljárások az azokat szabályozó jogi eszközöknek megfelelően folytatódnak.
- (2) Amennyiben a 27. cikk (2), (3) és (4) bekezdése szerinti lekérdezés egy vagy több egyezést eredményez, a CIR, és ha releváns, a SIS kapcsolatot hoz létre a lekérdezés kezdeményezéséhez használt adatok és a velük egyezést mutató adatok között.
- Amennyiben a lekérdezés többszörös egyezést eredményez, az egymással egyezést mutató összes adat között kapcsolat jön létre. Ha az adatokat előzőleg már összekapcsolták, a meglévő kapcsolatot ki kell terjeszteni a lekérdezés kezdeményezéséhez használt adatokra.
- (3) Amennyiben a 27. cikk (2), (3) és (4) bekezdése szerinti lekérdezés egy vagy több egyezést eredményez, és az összekapcsolt fájlokban szereplő személyazonosító adatok azonosak vagy hasonlóak, a 33. cikknek megfelelően fehér kapcsolat jön létre.

(4) Amennyiben a 27. cikk (2), (3) és (4) bekezdése szerinti lekérdezés egy vagy több egyezést eredményez, és az összekapcsolt fájlokban szereplő személyazonosító adatok nem tekinthetők hasonló adatoknak, a 30. cikknek megfelelően sárga kapcsolat jön létre, és a 29. cikkben említett eljárást kell alkalmazni.

(5) A Bizottság a 73. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogad el annak megállapítására irányuló eljárások meghatározására vonatkozóan, hogy a személyazonosító adatok mely esetekben tekintendők azonos vagy hasonló adatoknak.

(6) A kapcsolatokat a 34. cikkben említett, személyazonosságot megerősítő dossziében kell tárolni.

(7) A Bizottság az eu-LISA-val együttműködve végrehajtási jogi aktusok útján megállapítja a különböző uniós információs rendszerekből származó adatok közötti kapcsolatok létrehozására vonatkozó technikai szabályokat. Ezeket a végrehajtási jogi aktusokat a 74. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

#### 29. cikk

### A különböző személyazonosságok manuális ellenőrzése és a felelős hatóságok

(1) A (2) bekezdés sérelme nélkül, a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság a következő:

- a) az (EU) 2017/2226 rendelet 9. cikkének (2) bekezdésével összhangban kijelölt illetékes hatóság azon egyezések vonatkozásában, amelyek az EES-ben egyéni aktának az említett rendelet szerinti létrehozásakor vagy frissítésekor következtek be;
- b) a 767/2008/EK rendelet 6. cikkének (1) bekezdésében említett vízumhatóságok azon egyezések vonatkozásában, amelyek a VIS-ben kérelemfájlként az említett rendelet szerinti létrehozásakor vagy frissítésekor következtek be;
- c) az ETIAS központi egysége és az ETIAS nemzeti egységei azon egyezések vonatkozásában, amelyek a kérelemfájlként az (EU) 2018/1240 rendelet szerinti létrehozása vagy frissítése során következtek be;
- d) a tagállam SIRENE-irodája azon egyezések vonatkozásában, amelyek a SIS figyelmeztető jelzésnek az (EU) 2018/1860 és az (EU) 2018/1861 rendelet szerinti létrehozása vagy frissítése során következtek be.

A MID a személyazonosságot megerősítő dossziében megjelöli a különböző személyazonosságok manuális ellenőrzéséért felelős hatóságot.

(2) A személyazonosságot megerősítő dossziében szereplő, különböző személyazonosságok manuális ellenőrzéséért felelős hatóság a figyelmeztető jelzést kibocsátó tagállam SIRENE-irodája, amennyiben kapcsolatot hoznak létre az alábbi adatokkal:

- a) átadási vagy kiadási letartóztatás céljából körözött személyekre vonatkozó figyelmeztető jelzésben szereplő adatok, az (EU) 2018/1862 rendelet 26. cikkének megfelelően;
- b) eltűnt vagy különleges bánásmódot igénylő személyekre vonatkozó figyelmeztető jelzésben szereplő adatok, az (EU) 2018/1862 rendelet 32. cikkének megfelelően;
- c) bírósági eljárásban való közreműködés céljából keresett személyekre vonatkozó figyelmeztető jelzésben szereplő adatok, az (EU) 2018/1862 rendelet 34. cikkének megfelelően;
- d) rejtett ellenőrzés, kikérdezés vagy célzott ellenőrzés céljából keresett személyekre vonatkozó figyelmeztető jelzésben szereplő adatok, az (EU) 2018/1862 rendelet 36. cikkének megfelelően.

(3) E cikk (4) bekezdésének sérelme nélkül, a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság hozzáféréssel rendelkezik a releváns, személyazonosságot megerősítő dossziében szereplő összekapcsolt adatokhoz, valamint a CIR-ben és – adott esetben – a SIS-ben összekapcsolt személyazonosító adatokhoz. A hatóság késedelem nélkül megvizsgálja a különböző személyazonosságokat. A vizsgálat végeztével a 31., a 32. és a 33. cikkel összhangban frissíti a kapcsolatot, és haladéktalanul hozzáadja a személyazonosságot megerősítő dossziéhez.

(4) Amennyiben a személyazonosságot megerősítő dossziében szereplő, különböző manuális személyazonosságok ellenőrzéséért felelős hatóság az EES-ben az (EU) 2017/2226 rendelet 14. cikkével összhangban az egyéni aktát létrehozó vagy frissítő, az említett rendelet 9. cikkének (2) bekezdésével összhangban kijelölt illetékes hatóság, és amennyiben sárga kapcsolat jön létre, ez a hatóság további ellenőrzéseket végez. Ez a hatóság csak e célból hozzáféréssel rendelkezik a releváns, személyazonosságot megerősítő dossziében szereplő, vonatkozó adatokhoz. A hatóság megvizsgálja a különböző személyazonosságokat, e rendelet 31., 32. és 33. cikkével összhangban frissíti a kapcsolatot, és azt haladéktalanul hozzáadja a személyazonosságot megerősítő dossziéhez.

A különböző személyazonosságok ezen manuális ellenőrzését az érintett személy jelenlétében kell kezdeményezni, akinek fel kell ajánlani azt a lehetőséget, hogy kifejtse a körülményeket a felelős hatóságnak, amely figyelembe veszi ezeket a magyarázatokat.

Azokban az esetekben, amikor a különböző személyazonosságok manuális ellenőrzésére a határon kerül sor, arra lehetőség szerint a sárga kapcsolatnak a 28. cikk (4) bekezdése szerinti létrehozásától számított 12 órán belül kell sort keríteni.

(5) Ha egynél több kapcsolat jön létre, a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság mindegyiket külön-külön értékeli.

(6) Ha az egyezést jelző adatokat már összekapcsolták, a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság figyelembe veszi a meglévő kapcsolatokat, amikor új kapcsolatokat létrehozását értékeli.

### 30. cikk

#### Sárga kapcsolat

(1) Ha különböző személyazonosságok manuális ellenőrzésére még nem került sor, a két vagy több uniós információs rendszerben szereplő adatok közötti kapcsolatot a következő esetek bármelyikében sárga kapcsolatként kell besorolni:

- a) az összekapcsolt adatok azonos biometrikus adatokat, de hasonló vagy eltérő személyazonosító adatokat tartalmaznak;
- b) az összekapcsolt adatok eltérő személyazonosító adatokat, de azonos útiokmány-adatokat tartalmaznak, és legalább az uniós információs rendszerek egyike nem tartalmaz az érintett személyre vonatkozó biometrikus adatokat;
- c) az összekapcsolt adatok azonos személyazonosító adatokat, de eltérő biometrikus adatokat tartalmaznak;
- d) az összekapcsolt adatok hasonló vagy eltérő személyazonosító adatokat és azonos útiokmány-adatokat, de eltérő biometrikus adatokat tartalmaznak.

(2) Amennyiben egy kapcsolatot az (1) bekezdéssel összhangban sárga kapcsolatként soroltak be, a 29. cikkben megállapított eljárást kell alkalmazni.

### 31. cikk

#### Zöld kapcsolat

(1) A két vagy több uniós információs rendszerből származó adatok közötti kapcsolatot zöldnek kell minősíteni, ha:

- a) az összekapcsolt adatok eltérő biometrikus adatokat, de azonos személyazonosító adatokat tartalmaznak, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy az összekapcsolt adatok két különböző személyt jelölnek;
- b) az összekapcsolt adatok eltérő biometrikus adatokat, hasonló vagy eltérő személyazonosító adatokat és azonos útiokmány-adatokat tartalmaznak, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy az összekapcsolt adatok két különböző személyt jelölnek;
- c) az összekapcsolt adatok eltérő személyazonosító adatokat, de azonos útiokmány-adatokat tartalmaznak, és az uniós információs rendszerek közül legalább az egyik nem tartalmazza az érintett személyre vonatkozó biometrikus adatokat, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy az összekapcsolt adatok két különböző személyt jelölnek.

(2) A CIR vagy a SIS lekérdezésekor, ha az uniós információs rendszerek közül kettő vagy több rendszerben szereplő adatok között zöld kapcsolat áll fenn, a MID jelzi, hogy az összekapcsolt adatok között szereplő személyazonosító adatok nem ugyanarra a személyre vonatkoznak.

(3) Ha egy tagállami hatóságnak arra utaló bizonyítéka van, hogy a MID-ben hibásan rögzítették a zöld kapcsolatot, vagy az nem naprakész, illetve hogy az adatokat a MID-ben vagy az uniós információs rendszerekben e rendeletet megsértve kezelték, a hatóság ellenőrzi CIR-ben és a SIS-ben tárolt vonatkozó adatokat, és szükség esetén haladéktalanul helyesbíti vagy törli a kapcsolatot a MID-ből. Az említett tagállami hatóság haladéktalanul tájékoztatja a különböző személyazonosságok manuális ellenőrzéséért felelős tagállamot.

### 32. cikk

#### Vörös kapcsolat

(1) A két vagy több uniós információs rendszerben szereplő adatok közötti kapcsolatot a következő esetek bármelyikében vörös kapcsolatként kell besorolni:

- a) az összekapcsolt adatok azonos biometrikus adatokat, de hasonló vagy eltérő személyazonosító adatokat tartalmaznak, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy az összekapcsolt adatok – nem indokolt módon – ugyanazt a személyt jelölik;

- b) az összekapcsolt adatok azonos, hasonló vagy eltérő személyazonosító adatokat, azonos útiokmány-adatokat, de eltérő biometrikus adatokat tartalmaznak, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy ezek az adatok két különböző személyt jelölnek, akik közül legalább az egyik nem indokolt módon ugyanazt az úti okmányt használja;
- c) az összekapcsolt adatok azonos személyazonosító adatokat, de eltérő biometrikus adatokat tartalmaznak, és az úti okmány-adatok eltérőek vagy nem állnak rendelkezésre, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy ezek az adatok nem indokolt módon két különböző személyt jelölnek;
- d) az összekapcsolt adatok eltérő személyazonosító adatokat, de azonos útiokmány-adatokat tartalmaznak, az uniós információs rendszerek közül legalább az egyik nem tartalmaz az érintett személyre vonatkozó biometrikus adatokat, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy ezek az adatok nem indokolt módon ugyanazt a személyt jelölik.

(2) A CIR vagy a SIS lekérdezésekor, és ha az uniós információs rendszerek közül kettő vagy több rendszerben szereplő adatok között vörös kapcsolat áll fenn, a MID megjelöli a 34. cikkben említett adatokat. A vörös kapcsolat nyomon követése az uniós és a nemzeti joggal összhangban történik oly módon, hogy az érintett személyt terhelő jogkövetkezmények kizárólag az adott személyre vonatkozó adatokon alapulhatnak. Kizárólag a vörös kapcsolat meglétéből nem származhat semmilyen, az érintett személyt terhelő jogkövetkezmény.

(3) Ha az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban vagy az ECRIS-TCN-ben szereplő adatok között vörös kapcsolat jön létre, a CIR-ben tárolt egyéni aktát a 19. cikk (2) bekezdésében foglaltak szerint frissíteni kell.

(4) A SIS-be bevitt figyelmeztető jelzések kezelésére vonatkozó, az (EU) 2018/1860, az (EU) 2018/1861 és az (EU) 2018/1862 rendeletben foglalt rendelkezések sérelme nélkül, valamint a biztonság és a közrend védelme, a bűncselekmények megelőzése, és a nemzeti nyomozások veszélyeztetésének megakadályozása érdekében szükséges korlátozások sérelme nélkül, vörös kapcsolat létrehozása esetén a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság tájékoztatja az érintett személyt arról, hogy több jogellenes személyazonosító adat létezik, és a személlyel közli az e rendelet 34. cikkének c) pontjában említett egységes azonosító számot, az e rendelet 34. cikkének d) pontjában említett, különböző személyazonosságok manuális ellenőrzéséért felelős hatóságra való hivatkozást és az e rendelet 49. cikkével összhangban létrehozott webportál internetes címét.

(5) A (4) bekezdésben említett információkat szabványos formanyomtatványon keresztül a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság írásban közli. A Bizottság végrehajtási jogi aktusok révén határozza meg az említett formanyomtatvány tartalmát és formáját. Ezeket a végrehajtási jogi aktusokat a 74. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(6) Vörös kapcsolat létrehozása esetén a MID automatikusan értesítést küld az összekapcsolt adatokért felelős hatóságoknak.

(7) Ha egy, a CIR-hez vagy a SIS-hez hozzáféréssel rendelkező tagállami hatóságnak vagy uniós ügynökségnek arra utaló bizonyítéka van, hogy a MID-ben hibásan rögzítették a vörös kapcsolatot, vagy hogy az adatokat a MID-ben, a CIR-ben vagy a SIS-ben e rendeletet megsértve kezelték, az említett hatóság vagy ügynökség ellenőrzi a CIR-ben és a SIS-ben tárolt vonatkozó adatokat és:

- a) amennyiben a kapcsolat a 29. cikk (2) bekezdésében említett SIS figyelmeztető jelzések egyikéhez kapcsolódik, haladéktalanul tájékoztatja a SIS figyelmeztető jelzést kibocsátó tagállam illetékes SIRENE-irodáját;
- b) minden más esetben haladéktalanul helyesbíti vagy törli a MID-ből a kapcsolatot.

Amennyiben a SIRENE-irodával az első albekezdés a) pontja alapján felveszik a kapcsolatot, az iroda ellenőrzi a tagállam hatósága vagy az uniós ügynökség által benyújtott bizonyítékot, és adott esetben haladéktalanul helyesbíti vagy törli a kapcsolatot a MID-ből.

A bizonyítékot megszerző tagállami hatóság haladéktalanul tájékoztatja a különböző személyazonosságok manuális ellenőrzéséért felelős tagállami hatóságot a vörös kapcsolat esetleges releváns helyesbítéséről vagy törléséről.



## 33. cikk

**Fehér kapcsolat**

(1) A két vagy több uniós információs rendszerben szereplő adatok közötti kapcsolatot a következő esetek bármelyikében fehér kapcsolatként kell besorolni:

- a) az összekapcsolt adatok azonos biometrikus adatokat és azonos vagy hasonló személyazonosító adatokat tartalmaznak;
- b) az összekapcsolt adatok azonos vagy hasonló személyazonosító adatokat, azonos útiokmány-adatokat tartalmaznak, és legalább az uniós információs rendszerek egyike nem tartalmaz az érintett személyre vonatkozó biometrikus adatokat;
- c) az összekapcsolt adatok azonos biometrikus adatokat, azonos útiokmány-adatokat, és hasonló személyazonosító adatokat tartalmaznak;
- d) az összekapcsolt adatok azonos biometrikus adatokat, de hasonló vagy eltérő személyazonosító adatokat tartalmaznak, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy az összekapcsolt adatok – indokolt módon – ugyanazt a személyt jelölik;

(2) A CIR vagy a SIS lekérdezésekor, ha az uniós információs rendszerek közül két vagy több rendszerben szereplő adatok között fehér kapcsolat áll fenn, a MID jelzi, hogy az összekapcsolt adatok között szereplő személyazonosító adatok ugyanannak a személynek felelnek meg. A lekérdezett uniós információs rendszerek olyan választ adnak, amely a személyre vonatkozó valamennyi összekapcsolt adatot feltünteti, amennyiben azok relevánsak, és így egyezést eredményez a fehér kapcsolat által összekapcsolt adatok között, amennyiben a lekérdezést kezdeményező hatóság az uniós vagy a nemzeti jog alapján hozzáféréssel rendelkezik az összekapcsolt adatokhoz.

(3) Ha az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban vagy az ECRIS-TCN-ben szereplő adatok között fehér kapcsolatot hoznak létre, a CIR-ben tárolt egyéni aktát a 19. cikk (2) bekezdésében foglaltak szerint frissíteni kell.

(4) A SIS-be bevitt figyelmeztető jelzések kezelésére vonatkozó, az (EU) 2018/1860, az (EU) 2018/1861 és az (EU) 2018/1862 rendeletekben foglalt rendelkezések sérelme nélkül, valamint a biztonság és a közrend védelme, a bűncselekmények megelőzése, és a nemzeti nyomozások veszélyeztetésének megakadályozása érdekében szükséges korlátozások sérelme nélkül, ha a különböző személyazonosságok manuális ellenőrzését követően fehér kapcsolatot hoznak létre, a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság tájékoztatja az érintett személyt arról, hogy több hasonló vagy különböző személyazonosító adat áll fenn, és a személlyel közli az e rendelet 34. cikkének c) pontjában említett egységes azonosító számot, az e rendelet 34. cikkének d) pontjában említett, különböző személyazonosságok manuális ellenőrzéséért felelős hatóságra való hivatkozást és az e rendelet 49. cikkével összhangban létrehozott webportál internetes címét.

(5) Ha egy tagállami hatóságnak arra utaló bizonyítéka van, hogy a MID-ben hibásan rögzítették a fehér kapcsolatot, vagy hogy a fehér kapcsolat nem naprakész, vagy hogy az adatokat a MID-ben vagy az uniós információs rendszerekben e rendeletet megsértve kezelték, a hatóság ellenőrzi CIR-ben és a SIS-ben tárolt vonatkozó adatokat, és szükség esetén haladéktalanul helyesbíti vagy törli a kapcsolatot a MID-ből. Az említett tagállami hatóság haladéktalanul tájékoztatja a különböző személyazonosságok manuális ellenőrzéséért felelős tagállamot.

(6) A (4) bekezdésben említett információkat szabványos formanyomtatványon keresztül a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság írásban közli. A Bizottság végrehajtási jogi aktusok révén meghatározza az említett formanyomtatvány tartalmát és formáját. Ezeket a végrehajtási jogi aktusokat a 74. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

## 34. cikk

**A személyazonosságot megerősítő dosszié**

A személyazonosságot megerősítő dosszié a következő adatokat tartalmazza:

- a) a 30–33. cikkben szereplő kapcsolatok,
- b) hivatkozás azokra az uniós információs rendszerekre, amelyekben az összekapcsolt adatok szerepelnek;
- c) egységes azonosító szám, amely lehetővé teszi az összekapcsolt adatok lehívását a megfelelő uniós információs rendszerekből;
- d) a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság;
- e) a kapcsolat létrehozásának vagy bármely frissítésének időpontja.

## 35. cikk

**Adatmegőrzés a többszörös személyazonosságot észlelő rendszerben**

A személyazonosságot megerősítő dossziékat és az azokban szereplő adatokat – beleértve a kapcsolatokat is – csak addig lehet tárolni a MID-ben, amíg az összekapcsolt adatok szerepelnek két vagy több uniós információs rendszerben. Ezeket az adatokat automatikusan törölni kell a MID-ből.

## 36. cikk

**Naplóvezetés**

(1) Az eu-LISA-nak a MID-ben végzett összes adatkezelési műveletről naplót kell vezetnie. A napló az alábbiakat tartalmazza:

- a) a lekérdezést kezdeményező tagállamot;
- b) a felhasználó hozzáféréseinek célját;
- c) a lekérdezés napját és időpontját;
- d) a lekérdezés kezdeményezéséhez használt adatok típusát;
- e) az összekapcsolt adatokra való utalást;
- f) a személyazonosságot megerősítő dosszié előzményeit.

(2) Minden tagállam naplót vezet a MID használatára megfelelő felhatalmazással rendelkező hatóságai által és e hatóságok megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről. Minden uniós ügynökség naplót vezet a megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről,

(3) Az (1) és a (2) bekezdésben említett naplókat kizárólag az adatvédelmi ellenőrzés érdekében – ideértve a lekérdezés elfogadhatóságának és az adatkezelés jogszerűségének ellenőrzését –, valamint az adatbiztonság és az adatok sérthetatlensége biztosításának céljára lehet felhasználni. E naplókat megfelelő intézkedésekkel kell védeni a jogosulatlan hozzáféréstől, és létrehozásuk után egy évvel törölni kell. Ha azonban egy már megkezdett ellenőrzési eljáráshoz szükség van rájuk, akkor törlésükre akkor kell sort keríteni, amikor már nem szükségesek az ellenőrzési eljáráshoz.

## VI. FEJEZET

**Az interoperabilitást támogató intézkedések**

## 37. cikk

**Adatminőség**

(1) A tagállamoknak a rendszerbe bevitt adatok minőségével kapcsolatos felelősségének sérelme nélkül az eu-LISA az adatminőség ellenőrzésére irányuló automatizált mechanizmusokat és eljárásokat dolgoz ki az EES-ben, a VIS-ben, az ETIAS-ban, a SIS-ben, a közös BMS-ben és a CIR-ben tárolt adatokra vonatkozóan.

(2) Az eu-LISA mechanizmusokat hajt végre a közös BMS pontosságának értékelésére, valamint közös adatminőségi mutatókat és minőségi minimumkövetelményeket az EES-ben, a VIS-ben, az ETIAS-ban, a SIS-ben, a közös BMS-ben és a CIR-ben szereplő adatok tárolására vonatkozóan.

Kizárólag a minőségi minimumkövetelményeknek megfelelő adatok vihetők be az EES-be, a VIS-be, az ETIAS-ba, a SIS-be, a közös BMS-be, a CIR-be és a MID-be.

(3) Az eu-LISA a tagállamok részére rendszeresen jelentést készít az adatminőség ellenőrzésére irányuló automatizált mechanizmusokról és eljárásokról, valamint a közös adatminőségi mutatókról. Az eu-LISA a Bizottság részére is rendszeresen jelentést készít a felmerült problémákról és az érintett tagállamokról. Az eu-LISA ezt a jelentést kérelemre eljuttatja az Európai Parlamentnek és a Tanácsnak is. Az e bekezdés értelmében készült jelentések nem tartalmazhatnak személyes adatokat.

(4) Az adatminőség ellenőrzésére irányuló automatizált mechanizmusok és eljárások részleteit, valamint az EES-ben, a VIS-ben, az ETIAS-ban, a SIS-ben, a közös BMS-ben és a CIR-ben szereplő adatok tárolására vonatkozó közös adatminőségi mutatók és minőségi minimumkövetelmények részleteit végrehajtási jogi aktusokban kell meghatározni. Ezeket a végrehajtási jogi aktusokat a 74. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(5) A Bizottság az adatminőség ellenőrzésére irányuló automatizált mechanizmusok és eljárások, valamint a közös adatminőségi követelmények és az adatminőségi minimumkövetelmények megállapítása után egy évvel, majd azt követően évente értékeli az adatminőség tagállamok általi végrehajtását, és szükség esetén ajánlásokat tesz. A tagállamok cselekvési tervet nyújtanak be a Bizottságnak az értékelő jelentésben esetlegesen feltárt hiányosságok – és különösen az uniós információs rendszerekben szereplő téves adatokból származó adatminőségi problémák – orvoslására. A tagállamok rendszeresen jelentést tesznek a Bizottságnak a cselekvési terv tekintetében elért minden előrehaladásról a cselekvési terv maradéktalan végrehajtásáig.

A Bizottság továbbítja az értékelő jelentést az Európai Parlamentnek, a Tanácsnak, az európai adatvédelmi biztosnak, az Európai Adatvédelmi Testületnek és az Európai Unió Alapjogi Ügynökségének, amelyet a 168/2007/EK tanácsi rendelet <sup>(39)</sup> hozott létre.

### 38. cikk

#### Egységes üzenetformátum

(1) Létrejön az egységes üzenetformátum (UMF) szabvány. Az UMF a bel- és igazságügy területén működő információs rendszerek, hatóságok vagy szervezetek közötti, határokon átnyúló információcserre bizonyos tartalmi elemeire vonatkozó szabványokat határoz meg.

(2) Az UMF szabványt kell használni az EES, az ETIAS, az ESP, a CIR, a MID adott esetben a bel- és igazságügy területén működő bármely új információcserre-modellnek és információs rendszernek az eu-LISA vagy más uniós ügynökség által történő kidolgozása során.

(3) A Bizottság végrehajtási jogi aktust fogad el az e cikk (1) bekezdésében szereplő UMF szabvány meghatározása és kidolgozása céljából. Ezeket a végrehajtási jogi aktusokat a 74. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

### 39. cikk

#### A jelentések és statisztikák központi adattára

(1) Az EES-t, a VIS-t, az ETIAS-t és a SIS-t szabályozó jogi eszközökkel összhangban e rendszerek célkitűzéseinek támogatása, valamint a rendszerek közötti statisztikai adatok és elemzési jelentések szakpolitikai, működési és adatminőségi célokból történő biztosítása érdekében létrejön a jelentések és statisztikák központi adattára (CRRS).

(2) A CRRS-t, amely az EU) 2017/2226 rendelet 63. cikkében, a 767/2008/EK rendelet 17.cikkében, az (EU) 2018/1240 rendelet 84. cikkében és az (EU) 2018/1861 rendelet 60. cikkében, valamint az (EU) 2018/1860 rendelet 16. cikkében említett adatokat és statisztikákat uniós információs rendszerek szerint logikailag különválasztva tartalmazza, az eu-LISA hozza létre, vezeti be és üzemelteti technikai helyszínein. A CRRS-hez és ellenőrzött és biztonságos módon, egyedi felhasználói profilokkal, kizárólag jelentések és statisztikák készítése céljából lehet hozzáférést biztosítani az (EU) 2017/2226 rendelet 63. cikkében, a 767/2008/EK rendelet 17. cikkében, (EU) 2018/1240 rendelet 84. cikkében és az (EU) 2018/1861 rendelet 60. cikkében említett hatóságok számára.

(3) Az eu-LISA anonimizálja az adatokat, és az ilyen anonimizált adatokat rögzíti a CRRS-ben. Az adatok anonimizálása automatizált módon történik.

A CRRS-ben szereplő adatok nem tehetik lehetővé az egyének azonosítását.

(4) A CRRS a következő elemekből áll:

- a) az adatok anonimizálásához szükséges eszközök;
- b) az anonim adatok adattárából álló központi infrastruktúra;
- c) egy biztonságos kommunikációs infrastruktúra a CRRS-nek az EES-szel, a VIS-szel, az ETIAS-szal és a SIS-szel, valamint a közös BMS-szel, a CIR-rel és a MID központi infrastruktúráival való összekapcsolása céljából.

(5) A Bizottság a 73. cikknek megfelelően felhatalmazáson alapuló jogi aktust fogad el a CRRS működésére irányuló részletes szabályok megállapítására vonatkozóan, beleértve az e cikk (2) és (3) bekezdésében említett személyes adatok kezelésére vonatkozó különleges biztosítékokat, és az adattárra vonatkozó biztonsági szabályokat.

<sup>(39)</sup> A Tanács 168/2007/EK rendelete (2007. február 15.) az Európai Unió Alapjogi Ügynökségének létrehozásáról (HL L 53., 2007.2.22., 1. o.).

## VII. FEJEZET

**Adatvédelem**

## 40. cikk

**Adatkezelő**

(1) A személyes adatoknak a közös BMS keretében történő kezelése tekintetében a tagállamok azon hatóságai, amelyek az EES, a VIS, illetve a SIS vonatkozásában adatkezelőknek minősülnek, az (EU) 2016/679 rendelet 4. cikkének 7. pontja vagy az (EU) 2016/680 irányelv 3. cikkének 8. pontja szerinti adatkezelőknek tekintendők az e rendelet 13. cikkében említett olyan adatokból nyert biometrikus sablonok tekintetében is, amelyeket ők visznek be az alapul szolgáló rendszerekbe, valamint felelősek a biometrikus sablonok közös BMS keretében történő kezeléséért.

(2) A személyes adatoknak CIR-ben történő kezelése tekintetében a tagállamok azon hatóságai, amelyek az EES, a VIS és az ETIAS vonatkozásában adatkezelőknek minősülnek, az (EU) 2016/679 rendelet 4. cikkének 7. pontja szerinti adatkezelőknek tekintendők az e rendelet 18. cikkében említett olyan adatok tekintetében, amelyeket ők visznek be az alapul szolgáló rendszerekbe, valamint felelősek az említett személyes adatok CIR-ben történő kezeléséért.

(3) Az adatok MID keretében történő kezelése tekintetében:

- a) a személyes adatok ETIAS központi egysége általi feldolgozása tekintetében az Európai Határ- és Partvédelmi Ügynökség tekintendő az (EU) 2018/1725 rendelet 3. cikkének 8. pontja szerinti adatkezelőnek;
- b) a személyazonosságot megerősítő dossziéhoz adatokat hozzáadó vagy abban adatokat módosító tagállami hatóságok tekintendők az (EU) 2016/679 rendelet 4. cikkének 7. pontja vagy az (EU) 2016/680 irányelv 3. cikkének 8. pontja szerinti adatkezelőknek, és felelősek a személyes adatok MID-ben történő kezeléséért.

(4) Az adatvédelem – többek között a lekérdezés elfogadhatóságának és az adatkezelés jogszerűségének – ellenőrzése céljából az adatkezelők a 44. cikkben említetteknek megfelelően önellenőrzés céljából hozzáféréssel rendelkeznek a 10., a 16., a 24. és a 36. cikkben említett naplókhoz.

## 41. cikk

**Az adatfeldolgozó**

A közös BMS-ben, a CIR-ben és a MID-ben tárolt személyes adatok kezelése tekintetében az eu-LISA minősül az (EU) 2018/1725 rendelet 3. cikke 12. pontjának a) alpontja szerinti adatfeldolgozónak.

## 42. cikk

**Az adatkezelés biztonsága**

(1) Az eu-LISA, az ETIAS központi egysége, az Europol és a tagállami hatóságok biztosítják a személyes adatok e rendelet alapján történő kezelésének biztonságát. Az eu-LISA, az ETIAS központi egysége, az Europol és a tagállami hatóságok együttműködnek a biztonsággal kapcsolatos feladatok ellátása során.

(2) Az (EU) 2018/1725 rendelet 33. cikkének sérelme nélkül, az eu-LISA megteszi az interoperabilitási elemek és a hozzájuk kapcsolódó kommunikációs infrastruktúra biztonságának garantálásához szükséges intézkedéseket.

(3) Az eu-LISA különösen elfogadja a szükséges intézkedéseket, többek között egy biztonsági tervet, egy üzletmenet-folytonossági és katasztrófa-elhárítási tervet annak érdekében, hogy:

- a) fizikai adatvédelmet valósítson meg, többek között a kritikus infrastruktúra védelmére irányuló vészhelyzeti tervek kidolgozása által;
- b) megtagadja a jogosulatlan személyek hozzáférését az adatkezelő eszközökhöz és berendezésekhez;
- c) megakadályozza az adathordozók jogosulatlan olvasását, másolását, módosítását vagy eltávolítását;
- d) megakadályozza az adatok jogosulatlan bevitelét és a rögzített személyes adatok jogosulatlan ellenőrzését, módosítását vagy törlését;
- e) megakadályozza az adatok jogosulatlan kezelését, valamint jogosulatlan másolását, módosítását vagy törlését;
- f) megakadályozza az automatizált adatkezelő rendszerek jogosulatlan személyek általi, adatátviteli berendezés útján történő használatát;

- g) biztosítsa, hogy az interoperabilitási elemekhez való hozzáférésre jogosult személyek csak a hozzáférési jogosultságuk körébe tartozó adatokhoz férjenek hozzá, mégpedig kizárólag egyéni felhasználói azonosítókkal és titkos hozzáférési módszerekkel;
  - h) biztosítsa, hogy ellenőrizhető és megállapítható legyen, hogy az adatátviteli berendezések használatával mely szerverekhez lehet személyes adatokat továbbítani;
  - i) biztosítsa, hogy ellenőrizhető és megállapítható legyen, hogy ki, mikor, mely adatokat és milyen célból kezelt az interoperabilitási elemekben;
  - j) megakadályozza a személyes adatoknak az interoperabilitási elembe vagy azokból történő továbbítása vagy adathordozón történő szállítása során a személyes adatok jogosulatlan olvasását, másolását, módosítását vagy törlését, különösen a megfelelő titkosítási technikák révén;
  - k) biztosítsa, hogy üzemzavar esetén helyreállítható legyen a telepített rendszerek normál működése;
  - l) garantálja a megbízhatóságot azzal, hogy biztosítja, hogy az interoperabilitási elemek működése során fellépő hibákat minden esetben megfelelően bejelentik;
  - m) figyelemmel kíséri az e bekezdésben említett biztonsági intézkedések eredményességét, és megtegye a belső ellenőrzéssel kapcsolatban szükséges szervezeti intézkedéseket az e rendeletnek való megfelelés biztosítása érdekében, továbbá az új technológiai fejlesztések fényében értékeli az említett biztonsági intézkedéseket.
- (4) A tagállamok, az Europol és az ETIAS központi egysége a (3) bekezdésben említettekkel egyenértékű intézkedéseket hoznak a személyes adatok azon hatóságok általi kezelése tekintetében, amelyek hozzáférésre jogosultak bármely interoperabilitási elemhez.

#### 43. cikk

### Biztonsági incidensek

(1) Biztonsági incidensnek kell tekinteni bármely olyan eseményt, amely kihatással van vagy lehet az interoperabilitási elemek biztonságára és kárt vagy veszteséget okozhat a bennük tárolt adatokban, különösen akkor, ha az adatokhoz jogosulatlan hozzáférés történt, vagy az adatok rendelkezésre állása, sértetlensége, illetve bizalmas jellege kárt szenvedett vagy szenvedhetett.

(2) A biztonsági incidenseket gyors, hatékony és megfelelő reagálással kell kezelni.

(3) A személyes adatok megsértésének az (EU) 2016/679 rendelet 33. cikke, az (EU) 2016/680 irányelv 30. cikke vagy mindkettő szerinti bejelentésének és közlésének sérelme nélkül a tagállamok a Bizottságot, az eu-LISA-t, az illetékes felügyeleti hatóságokat és az európai adatvédelmi biztost haladéktalanul tájékoztatják valamennyi biztonsági incidensről.

Az (EU) 2018/1725 rendelet 34. és 35. cikkének és az (EU) 2016/794 rendelet 34. cikkének sérelme nélkül az ETIAS központi egysége és az Europol haladéktalanul tájékoztatja a Bizottságot az eu-LISA-t és az európai adatvédelmi biztost valamennyi biztonsági incidensről.

Az interoperabilitási elemek központi infrastruktúráját érintő biztonsági incidens esetén az eu-LISA haladéktalanul tájékoztatja a Bizottságot és az európai adatvédelmi biztost.

(4) A tagállamok, az ETIAS központi egysége, valamint az Europol számára haladéktalanul információkat kell szolgáltatni, és az eu-LISA által biztosított incidens-kezelési tervnek megfelelően be kell számolni azokról a biztonsági incidensekről, amelyek hatással vannak vagy hatással lehetnek az interoperabilitási elemek működésére, vagy az adatok rendelkezésre állására, sértetlenségére, illetve bizalmas jellegére.

(5) Az érintett tagállamok, az ETIAS központi egysége, az Europol és az eu-LISA a biztonsági incidensek bekövetkezése esetén együttműködnek. A Bizottság végrehajtási jogi aktusok útján meghatározza ezen együttműködési eljárás részleteit. Ezeket a végrehajtási jogi aktusokat a 74. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

#### 44. cikk

### Önellenőrzés

A tagállamok és a releváns uniós ügynökségek biztosítják, hogy az interoperabilitási elemekhez való hozzáférésre jogosult valamennyi hatóság megtegye az e rendeletnek való megfelelése nyomán követéséhez szükséges intézkedéseket, és szükség esetén együttműködjön a felügyeleti hatósággal.

A 40. cikk szerinti adatkezelők megteszik a szükséges intézkedéseket az adatkezelés e rendelet szerinti megfelelőségének figyelemmel kísérésére, többek a 10., a 16., a 24. és a 36. cikkben említett naplók gyakori ellenőrzése révén, és szükség esetén együttműködnek a felügyeleti hatóságokkal és az európai adatvédelmi biztossal.

#### 45. cikk

### Szankciók

A tagállamok biztosítják, hogy az adatokkal való visszaélésre és az adatok e rendeletbe ütköző kezelésére és megosztására a nemzeti joggal összhangban büntetőszankciók vonatkozzanak. Az előírt szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük.

#### 46. cikk

### Felelősség

(1) A kártérítéshez való jog, valamint az adatkezelőnek vagy adatfeldolgozónak az (EU) 2016/679 rendelet, az (EU) 2016/680 irányelv és az (EU) 2018/1725 rendelet értelmében fennálló felelősségének sérelme nélkül:

- a) minden olyan személy vagy tagállam, aki, illetve amely jogellenes személyesadat-kezelési műveletből vagy bármilyen egyéb, e rendelettel összeegyeztethetetlen tagállami intézkedésből adódóan vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adott tagállamtól kártérítésre jogosult;
- b) minden olyan személy vagy tagállam, aki, illetve amely az Europol, az Európai Határ- és Partvédelmi Ügynökség vagy az eu-LISA e rendelettel összeegyeztethetetlen intézkedéséből adódóan vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért kártérítésre jogosult az adott ügynökségtől.

Az érintett tagállam, az Europol, az Európai Határ- és Partvédelmi Ügynökség vagy az eu-LISA teljes mértékben vagy részben mentesül az első albekezdés szerinti felelőssége alól, ha bizonyítja, hogy a kárt előidéző eseményért nem felelős.

(2) Ha egy tagállam az e rendelet szerinti kötelezettségeinek elmulasztásával kárt okoz az interoperabilitási elemekben, az okozott kárért e tagállamot terheli a felelősség, kivéve és amennyiben az eu-LISA vagy az e rendelet hatálya alá tartozó valamely másik tagállam elmulasztotta meghozni a kár megelőzéséhez vagy hatásának minimalizálásához szükséges észszerű intézkedéseket.

(3) A tagállammal szembeni, az (1) és a (2) bekezdésben említett kártérítési igényekre az alperes tagállam nemzeti joga az irányadó. Az adatkezelővel vagy az eu-LISA-val szembeni, az (1) és a (2) bekezdésben említett kártérítési igényekre a Szerződésekben előírt feltételek vonatkoznak.

#### 47. cikk

### A tájékoztatáshoz való jog

(1) A közös BMS-ben, a CIR-ben vagy a MID-ben tárolandó személyes adatokat gyűjtő hatóság azon személyek rendelkezésére bocsátja az (EU) 2016/679 rendelet 13. és 14. cikkében, az (EU) 2016/680 irányelv 12. és 13. cikkében és az (EU) 2018/1725 rendelet 15. és 16. cikkében előírt információkat, akiknek az adatait gyűjtik. A hatóság az információkat az ilyen adatok gyűjtésének időpontjában közli.

(2) Minden információt – világos és közérthető nyelven – hozzáférhetővé kell tenni egy olyan nyelvi változatban, amelyet az érintett személy megért, vagy amelyről észszerűen feltételezhető, hogy megérti. Ez azt is magában foglalja, hogy a kiskorú érintetteknek a tájékoztatást az életkoruknak megfelelő módon kell megadni.

(3) Azokat a személyeket, akiknek adatait rögzítették az EES-ben, a VIS-ben vagy az ETIAS-ban, az (1) bekezdéssel összhangban tájékoztatni kell a személyes adatok e rendelet alkalmazásában történő kezeléséről, amennyiben:

- a) az EES-ben az (EU) 2017/2226 rendelet 14. cikkének megfelelően egyéni aktát hoznak létre vagy frissítenek;
- b) a VIS-ben a 767/2008/EK rendelet 8. cikkének megfelelően kérelemfájl hoznak létre vagy frissítenek;
- c) az ETIAS-ban az (EU) 2018/1240 rendelet 19. cikkének megfelelően egyéni kérelemfájl hoznak létre vagy frissítenek.

## 48. cikk

**A MID-ben tárolt személyes adatokhoz kapcsolódó hozzáférési, helyesbítési és törlési jog, valamint az adatok kezelésének korlátozása**

(1) Az (EU) 2016/679 rendelet 15–18. cikke, az (EU) 2018/1725 rendelet 17–20. cikke, valamint az (EU) 2016/680 irányelv 14., 15. és 16. cikke értelmében fennálló jogai gyakorlása érdekében bármely személynek jogában áll bármely tagállam illetékes hatóságához fordulni, amely kivizsgálja és megválaszolja a kérelmet.

(2) Az a tagállam, amely a kérelmet megvizsgálja, indokolatlan késedelem nélkül, de legkésőbb a kérelem kézhezvételétől számított 45 napon belül válaszol. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további 15 nappal meghosszabbítható. Az a tagállam, amely a kérelmet megvizsgálja, a kérelem kézhezvételétől számított 45 napon belül tájékoztatja az érintettet a határidő meghosszabbításáról, megjelölve a késedelem okait. A tagállamok dönthetnek úgy, hogy a válaszokat a központi hivatalok adják meg.

(3) Ha a személyes adatok helyesbítése vagy törlése iránti kérelmet a különböző személyazonosságok manuális ellenőrzéséért felelős tagállamtól eltérő tagállamhoz intézik, az a tagállam, amelyhez a kérelmet benyújtották, hét napon belül felveszi a kapcsolatot a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam hatóságával. A különböző személyazonosságok manuális ellenőrzéséért felelős tagállam indokolatlan késedelem nélkül, de legkésőbb az ilyen megkereséstől számított 30 napon belül ellenőrzi az adatok pontosságát és az adatkezelés jogszerűségét. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további 15 nappal meghosszabbítható. A különböző személyazonosságok manuális ellenőrzéséért felelős tagállam tájékoztatja a vele kapcsolatba lépett tagállamot az ilyen meghosszabbításról és a késedelem okáról. Az a tagállam, amely kapcsolatba lépett a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam hatóságával, tájékoztatja az érintett személyt a további eljárásról.

(4) Ha a személyes adatok helyesbítése vagy törlése iránti kérelmet egy olyan tagállamhoz nyújtják be, amelyben az ETIAS központi egysége volt felelős a különböző személyazonosságok manuális ellenőrzéséért, a tagállam, amelyhez a kérelmet benyújtották, hét napon belül felveszi a kapcsolatot az ETIAS központi egységével, és kéri véleményét. Az ETIAS központi egysége indokolatlan késedelem nélkül, de legkésőbb az ilyen megkereséstől számított 30 napon belül véleményt nyilvánít. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további 15 nappal meghosszabbítható. Az érintett személyt a további eljárásról az ETIAS központi egységével kapcsolatba lépett tagállam tájékoztatja.

(5) Amennyiben a vizsgálatot követően megállapítást nyer, hogy a MID-ben tárolt adatok pontatlanok, vagy jogellenesen kerültek rögzítésre, a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam, vagy ha a nincs a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam, vagy ha az ETIAS központi egysége volt a felelős a különböző személyazonosságok manuális ellenőrzéséért, az a tagállam, amelyhez a kérelmet benyújtották, indokolatlan késedelem nélkül helyesbíti vagy törli ezeket az adatokat. Az érintett személyt írásban tájékoztatni kell arról, hogy adatait helyesbítették vagy törölték.

(6) Amennyiben a MID-ben tárolt adatokat valamely tagállam azok megőrzésének ideje alatt módosítja, az említett tagállam elvégzi a 27. cikkben, és adott esetben a 29. cikkben meghatározott adatkezelést annak megállapítása céljából, hogy a módosított adatokat össze kell-e kapcsolni. Amennyiben az adatkezelés nem jelez egyezést, az említett tagállam törli az adatokat a személyazonosságot megerősítő dossziéból. Amennyiben az automatizált adatfeldolgozás egy vagy több egyezést jelez, az említett tagállam e rendelet vonatkozó rendelkezéseivel összhangban létrehozza vagy frissíti a releváns kapcsolatot.

(7) Ha a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam, illetve adott esetben az a tagállam, amelyhez a kérelmet benyújtották, nem ért egyet azzal, hogy a MID-ben tárolt adatok pontatlanok vagy jogellenesen kerültek rögzítésre, e tagállam haladéktalanul közigazgatási határozatot hoz, amely írásbeli magyarázatot nyújt az érintett személynek arról, hogy e tagállam miért nem kívánja helyesbíteni vagy törölni a rá vonatkozó adatokat.

(8) A (7) bekezdésben említett határozat tájékoztatással is kell, hogy szolgáljon az érintett személy részére, ismertetve annak lehetőségét, hogy a személyes adatokhoz való hozzáférés, az adatok helyesbítése, törlése vagy kezelésének korlátozása iránti kérelem tárgyában hozott határozat ellen kifogást nyújthat be, és adott esetben arról, hogy hogyan nyújthat be keresetet vagy panaszt az illetékes hatóságokhoz vagy bíróságokhoz, továbbá ismertetve az esetleges segítségnyújtás lehetőségét, beleértve a felügyeleti hatóságok általi segítségnyújtást is.

(9) A személyes adatokhoz való hozzáférés, az adatok helyesbítése, törlése vagy kezelésének korlátozása iránti kérelmeknek tartalmazniuk kell az érintett személy személyazonosításához szükséges információkat. Ezek az információk kizárólag az e cikkben említett jogok gyakorlásának lehetővé tételére használhatók fel, és ezt követően haladéktalanul törlésre kerülnek.

(10) A különböző személyazonosságok manuális ellenőrzéséért felelős tagállamnak vagy adott esetben annak a tagállamnak, amelyhez a kérelmet benyújtották, írásos bejegyzést kell vezetnie arról, hogy kérelmet nyújtottak be a személyes adatokhoz való hozzáférés, az adatok helyesbítése, törlése vagy kezelésének korlátozása iránt, valamint arról, hogy hogyan kezelték a kérelmet, és haladéktalanul a hatóságok rendelkezésére kell bocsátania ezt a bejegyzést.

(11) Ez a cikk nem érinti az ebben a cikkben meghatározott jogokra vonatkozó, az (EU) 2016/679 rendelet és az (EU) 2016/680 irányelv szerinti korlátozásokat és megszorító feltételeket.

#### 49. cikk

### Webportál

(1) A személyes adatokhoz való hozzáféréshez, az adatok helyesbítéséhez, törléséhez vagy kezelésének korlátozásához való jog gyakorlásának megkönnyítése céljából webportál jön létre.

(2) A webportál tájékoztatást nyújt a 47. és a 48. cikkben említett jogokról és eljárásokról, valamint tartalmaz egy felhasználói felületet, amely lehetővé teszi azon személyek számára, akiknek adatait a MID-ben kezelik, és akiket a 32. cikk (4) bekezdésének megfelelően tájékoztattak a vörös kapcsolat meglétéről, hogy megkapják a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam illetékes hatóságának kapcsolattartási adatait.

(3) A különböző személyazonosságok manuális ellenőrzéséért felelős tagállam illetékes hatósága kapcsolattartási adatainak megszerzése érdekében annak a személynek, akinek adatait a MID-ben kezelik, be kell vinnie a rendszerbe a 34. cikk d) pontjában említett különböző személyazonosságok manuális ellenőrzéséért felelős hatóságra vonatkozó hivatkozást. A webportál felhasználja ezt a hivatkozást a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam illetékes hatósága kapcsolattartási adatainak lekérésére. A webportál tartalmaz egy elektronikus levélmintát is, amely megkönnyíti a portál-felhasználó és a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam illetékes hatósága közötti kommunikációt. Az ilyen elektronikus levél tartalmazza a 34. cikk c) pontjában említett egységes azonosító számot annak érdekében, hogy a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam illetékes hatósága azonosítani tudja az érintett adatokat.

(4) A tagállamok tájékoztatják az eu-LISA-t minden olyan hatóság kapcsolattartási adatairól, amely hatáskörrel rendelkezik a 47. és a 48. cikkben említett bármely kérelem vizsgálatára és megválaszolására, és rendszeresen áttekinti, hogy ezek az adatok naprakészek-e.

(5) Az eu-LISA kifejleszti a webportált, és gondoskodik annak műszaki irányításáról.

(6) A Bizottság a 73. cikkkel összhangban felhatalmazáson alapuló jogi aktust fogad el, amelyben részletes szabályokat határoz meg a webportál működtetésére vonatkozóan, beleértve a felhasználói felületet, azon nyelveket, amelyeken a webportált elérhetővé kell tenni, valamint az elektronikus levélmintát.

#### 50. cikk

### Személyes adatok közlése harmadik országokkal, nemzetközi szervezetekkel és magánfelekkel

Az (EU) 2018/1240 rendelet 65. cikkének, az (EU) 2016/679 rendelet 25. és 26. cikkének, az (EU) 2017/2226 rendelet 41. cikkének, a 767/2008/EK rendelet 31. cikkének, valamint az Interpol-adatbázisok ESP-n keresztül, e rendelet 9. cikkének (5) bekezdésével összhangban történő, olyan lekérdezésének sérelme nélkül, amely megfelel az (EU) 2018/1725 rendelet V. fejezetében és az (EU) 2016/679 rendelet V. fejezetében foglalt rendelkezéseknek, az interoperabilitási elemekben tárolt, kezelt vagy azokon keresztül elért személyes adatok nem továbbíthatók és nem tehetők elérhetővé harmadik országok, nemzetközi szervezetek vagy magánfelek számára.

#### 51. cikk

### A felügyeleti hatóságok által gyakorolt felügyelet

(1) Minden tagállam biztosítja, hogy a felügyeleti hatóságok független módon figyelemmel kísérik, hogy az érintett tagállam jogszerűen kezeli-e e rendelet alapján a személyes adatokat, beleértve az adatok interoperabilitási elemekbe és onnan történő továbbítását is.

(2) Minden tagállam biztosítja, hogy az (EU) 2016/680 irányelv alapján elfogadott nemzeti törvényi, rendeleti és közigazgatási rendelkezések alkalmazása adott esetben kiterjedjen a rendőri hatóságok és a kijelölt hatóságok interoperabilitási elemekhez való hozzáférésére is, az olyan személyek jogaival összefüggésben is, akiknek az adataihoz ilyen módon fértek hozzá.



(3) A felügyeleti hatóságok biztosítják a felelős nemzeti hatóságok által az e rendelet értelmében végzett személyesadat-kezelési műveleteknek a vonatkozó nemzetközi ellenőrzési standardoknak megfelelő, legalább négyévente történő ellenőrzését.

Az említett felügyeleti hatóságok évente közzéteszik a személyes adatok helyesbítésére, törlésére vagy kezelésének korlátozására irányuló kérelmek számát, a kérelmek nyomán hozott intézkedéseket, valamint az érintett személyek kérelme nyomán végzett helyesbítések, törlések és az adatkezelés korlátozásainak számát.

(4) A tagállamok biztosítják, hogy felügyeleti hatóságaik rendelkezzenek az e rendelet alapján rájuk ruházott feladatok ellátásához szükséges erőforrásokkal és szakértelemmel.

(5) A tagállamok az (EU) 2016/679 rendelet 51. cikkének (1) bekezdésében említett felügyeleti hatóság rendelkezésére bocsátják a kért információkat, különösen az e rendelet szerinti felelősségi körüknek megfelelően folytatott tevékenységekre vonatkozó információkat. A tagállamok biztosítják az (EU) 2016/679 rendelet 51. cikkének (1) bekezdésében említett felügyeleti hatóságok számára az e rendelet 10., 16., 24. és 36. cikkében említett naplóihoz való hozzáférést, az e rendelet 22. cikkének (2) bekezdésében említett indokolásukhoz való hozzáférést, valamint mindenkor lehetővé teszik számukra az interoperabilitási célokra használt létesítményeikbe történő bejutást.

#### 52. cikk

### **Az európai adatvédelmi biztos általi ellenőrzések**

Az európai adatvédelmi biztos gondoskodik arról, hogy az eu-LISA, az ETIAS központi egysége és az Europol által e rendelet alkalmazásában végzett személyesadat-kezelési műveleteket a vonatkozó nemzetközi ellenőrzési standardok alapján legalább négyévente ellenőrizzék. Az ellenőrzésről készült jelentést meg kell küldeni az Európai Parlament, a Tanács, az eu-LISA, a Bizottság, a tagállamok és az érintett uniós ügynökség számára. Az eu-LISA, az ETIAS központi egysége és az Europol a jelentések elfogadása előtt lehetőséget kap észrevételeinek megtételére.

Az eu-LISA, az ETIAS központi egysége és az Europol az európai adatvédelmi biztos rendelkezésére bocsátja a kért információkat, hozzáférést biztosít az európai adatvédelmi biztos számára minden általa igényelt dokumentumhoz és a 10., a 16., a 24. és a 36. cikkben említett naplóihoz, valamint mindenkor lehetővé teszi az európai adatvédelmi biztos számára az eu-LISA összes létesítményébe történő bejutást.

#### 53. cikk

### **A felügyeleti hatóságok és az európai adatvédelmi biztos közötti együttműködés**

(1) A felügyeleti hatóságok és az európai adatvédelmi biztos – hatáskörük keretein belül eljárva – tevékenyen együttműködnek egymással felelősségi körük keretein belül, és biztosítják az interoperabilitási elemek használatának és az e rendelet egyéb rendelkezései alkalmazásának összehangolt felügyeletét, különösen akkor, ha az európai adatvédelmi biztos vagy valamely felügyeleti hatóság jelentős eltéréseket talál a tagállamok gyakorlatai között, vagy az interoperabilitási elemek kommunikációs csatornáin zajló, potenciálisan jogellenes adattovábbítást észlel.

(2) Az e cikk (1) bekezdésében említett esetekben az (EU) 2018/1725 rendelet 62. cikkével összhangban összehangolt felügyeletet kell biztosítani.

(3) Az Európai Adatvédelmi Testület 2021. június 12-ig, és azt követően két évente az e cikk szerinti tevékenységeire vonatkozóan együttes jelentést küld az Európai Parlamentnek, a Tanácsnak, a Bizottságnak, az Europolnak, az Európai Határ- és Partvédelmi Ügynökségnek és az eu-LISA-nak. A jelentésben valamennyi tagállamra vonatkozóan szerepelnie kell egy, az adott tagállam felügyeleti hatósága által összeállított fejezetnek.

#### VIII. FEJEZET

### **Feladatkörök**

#### 54. cikk

### **Az eu-LISA feladatai a tervezési és fejlesztési szakaszban**

(1) Az eu-LISA biztosítja az interoperabilitási elemeknek e rendelettel összhangban történő működtetését.

(2) Az interoperabilitási elemek elhelyezését az eu-LISA biztosítja a technikai helyszínein, valamint biztosítja az e rendeletben meghatározott funkciókat a biztonságra, a hozzáférhetőségre, a minőségre és a teljesítményre vonatkozóan az 55. cikk (1) bekezdésében meghatározott feltételekkel összhangban.

(3) Az eu-LISA felelős az interoperabilitási elemek fejlesztéséért, valamint az EES, a VIS, az ETIAS, a SIS az Eurodac, valamint az ECRIS-TCN és az ESP, a közös BMS, a CIR, a MID és a CRRS központi rendszerei közötti interoperabilitás megteremtéséhez szükséges kiigazításokért.

A 66. cikk sérelme nélkül az eu-LISA nem férhet hozzá az ESP-n, a közös BMS-en, a CIR-en vagy a MID-en keresztül kezelt személyes adatokhoz.

Az eu-LISA meghatározza az interoperabilitási elemek – ideértve azok kommunikációs infrastruktúráját is – fizikai felépítését, valamint a központi infrastruktúra és a biztonságos kommunikációs infrastruktúra tekintetében a műszaki előírásokat és azok továbbfejlesztését is, amelyeket a Bizottság kedvező véleményétől függően az igazgatótanács fogad el. Az eu-LISA továbbá minden olyan kiigazítást végrehajt az EES-ben, a VIS-ben, az ETIAS-ban vagy a SIS-ben, amelyre az interoperabilitás megteremtéséhez, valamint az e rendeletben foglaltaknak megfelelően szükség van.

Az eu-LISA e rendelet hatálybalépését, valamint a 8. cikk (2) bekezdésében, a 9. cikk (7) bekezdésében, a 28. cikk (5) és (7) bekezdésében, a 37. cikk (4) bekezdésében, a 38. cikk (3) bekezdésében, a 39. cikk (5) bekezdésében, a 43. cikk (5) bekezdésében és a 78. cikk (10) bekezdésében előírt intézkedéseknek a Bizottság általi elfogadását követően a lehető leghamarabb kifejleszti és végrehajtja az interoperabilitási elemeket.

A fejlesztésnek a műszaki előírások kidolgozását és végrehajtását, a tesztelést és az átfogó projektmenedzsmentet és -koordinációt kell magában foglalnia.

(4) A kialakítás és fejlesztés szakaszában létre kell hozni egy legfeljebb 10 tagból álló programirányítási tanácsot. A programirányítási tanács az eu-LISA igazgatótanácsa által saját tagjai vagy póttagjai közül kinevezett hét tagból, a 75. cikkben említett interoperabilitással foglalkozó tanácsadó csoport elnökéből, az eu-LISA-t képviselő, az ügyvezető igazgató által kinevezett tagból, valamint a Bizottság által kinevezett tagból áll. Az eu-LISA igazgatótanácsa kizárólag azon tagállamokból nevez ki tagokat, amelyekre nézve az uniós jog értelmében teljes mértékben kötelezők valamennyi uniós információs rendszer tekintetében a rendszerek fejlesztését, létrehozását, működtetését és használatát szabályozó jogi eszközök, és amelyek részt fognak venni az interoperabilitási elemekben.

(5) A programirányítási tanács rendszeresen és negyedévente legalább három alkalommal ülésezik. A programirányítási tanács biztosítja az interoperabilitási elemek kialakítási és fejlesztési szakaszának megfelelő irányítását.

A programirányítási tanács minden hónapban írásban beszámol az eu-LISA igazgatótanácsának a projekt előrehaladásáról. A programirányítási tanács nem rendelkezik döntéshozatali hatáskörrel, és az eu-LISA igazgatótanácsának tagjait nem képviselheti.

(6) Az eu-LISA igazgatótanácsa meghatározza a programirányítási tanács eljárási szabályzatát, amely különösen a következőkről rendelkezik:

- a) az elnökség;
- b) az ülések helyszíne;
- c) az ülések előkészítése;
- d) a szakértők részvétele az üléseken;
- e) az igazgatótanácsban részt nem vevő tagállamok teljes körű tájékoztatását biztosító kommunikációs tervek.

Az elnöki tisztelet egy olyan tagállamnak kell betöltenie, amelyre nézve az uniós jog értelmében teljes mértékben kötelezők valamennyi uniós információs rendszer tekintetében a rendszerek fejlesztését, létrehozását, működtetését és használatát szabályozó jogi eszközök, és amely rész fog venni az interoperabilitási elemekben.

A programirányítási tanács tagjainak valamennyi utazási és ellátási költségét az eu-LISA fedezi, és az eu-LISA eljárási szabályzatának 10. cikkét értelemszerűen alkalmazni kell. A programirányítási tanács titkárságát az eu-LISA biztosítja.

A 75. cikkben említett, interoperabilitással foglalkozó tanácsadó csoport rendszeresen ülésezik mindaddig, amíg az interoperabilitási elemek meg nem kezdik a működést. A tanácsadó csoport minden ülés után beszámol a programirányítási tanácsnak. A tanácsadó csoport biztosítja a programirányítási tanács tevékenységét támogató műszaki szakértelmet, valamint nyomon követi a tagállami előkészületek alakulását.

## 55. cikk

**Az eu-LISA feladatköre az üzemeltetés megkezdését követően**

(1) Múltán valamennyi interoperabilitási elem működésbe lépett, az eu-LISA felelős az interoperabilitási elemek központi infrastruktúrájának műszaki irányításáért, ideértve az interoperabilitási elemek karbantartását és technológiai fejlesztését is. Az eu-LISA – költség-haszon elemzés alapján – a tagállamokkal együttműködve biztosítja, hogy a legjobb rendelkezésre álló technológiát alkalmazzák. Az eu-LISA felelős a 6., a 12., a 17., a 25. és a 39. cikkben említett kommunikációs infrastruktúra műszaki irányításáért is.

Az interoperabilitási elemek műszaki irányítása magában foglal minden olyan feladatot és műszaki megoldást, amely a hét minden napján, napi 24 órában, e rendelettel összhangban az interoperabilitási elemek működtetéséhez és a tagállamok és az uniós ügynökségek számára megszakításmentes szolgáltatások nyújtásához szükséges, ideértve azokat a karbantartási munkákat és technikai fejlesztéseket, amelyek az elemek megfelelő műszaki minőségű, a műszaki előírásoknak eleget tévő működéséhez szükségesek, mindenekelőtt a központi infrastruktúrákban történő lekérdezések válaszüzeje tekintetében.

Az interoperabilitási elemek mindegyikét oly módon kell fejleszteni és kezelni, hogy biztosított legyen a gyors, zökkenőmentes, hatékony és ellenőrzött hozzáférés ezen elemekhez és a MID-ben, a közös BMS-ben és a CIR-ben tárolt adatokhoz, valamint a tagállami hatóságok és az uniós ügynökségek operatív igényeinek megfelelő válaszüzeje.

(2) Az Európai Unió tisztviselőire alkalmazandó személyzeti szabályzat 17. cikkének sérelme nélkül, az eu-LISA megfelelő szakmai titoktartási vagy azzal egyenértékű titoktartási szabályokat alkalmaz személyi állományának minden olyan tagjára, aki munkája során az interoperabilitási elemekben tárolt adatokat kell, hogy kezeljen. Ez a kötelezettség ezen személyi állomány hivatali vagy munkaviszonyának megszűnését, vagy tevékenysége megszűntét követően is fennáll.

A 66. cikk sérelme nélkül, az eu-LISA nem férhet hozzá az ESP-n, a közös BMS-n, a CIR-en és a MID-en keresztül kezelt személyes adatokhoz.

(3) Az eu-LISA az adatminőség ellenőrzésére irányuló mechanizmust és eljárásokat dolgoz ki és üzemeltet a közös BMS-ben és a CIR-ben a 37. cikknek megfelelően tárolt adatokra vonatkozóan.

(4) Az eu-LISA ellátja továbbá az interoperabilitási elemek technikai használatára vonatkozó képzéssel kapcsolatos feladatokat.

## 56. cikk

**A tagállamok feladatai**

(1) Az egyes tagállamok felelősek:

- a) az ESP és a CIR kommunikációs infrastruktúrájához való kapcsolódásért;
- b) a meglévő nemzeti rendszereknek és infrastruktúráknak az ESP-vel, a CIR-rel és a MID-del történő integrálásáért;
- c) a meglévő nemzeti infrastruktúrájuk szervezéséért, irányításáért, működtetéséért és karbantartásáért, valamint annak az interoperabilitási elemekkel való összekapcsolásáért;
- d) az illetékes nemzeti hatóságok megfelelő felhatalmazással rendelkező személyi állománya számára az e rendelettel összhangban az ESP-hez, a CIR-hez és a MID-hez biztosított hozzáférés irányításáért és részletes szabályozásáért, valamint a személyi állomány e tagjairól és azok profiljáról összeállítandó lista elkészítéséért és rendszeres frissítéséért;
- e) a CIR-hez személyazonosítás céljából történő hozzáférést lehetővé tévő, a 20. cikk (5) és (6) bekezdésében említett jogalkotási intézkedések elfogadásáért;
- f) a különböző személyazonosságok manuális ellenőrzéséért, a 29. cikkben említettek szerint;
- g) az uniós jogban meghatározott adatminőségi követelményeknek való megfelelésért;

- h) az egyes uniós információs rendszerek szabályainak való maradéktalan megfelelésért a személyes adatok biztonságának és sértetlenségének biztosítása érdekében;
- i) a Bizottságnak a 37. cikk (5) bekezdésében említett, az adatminőségre vonatkozó értékelő jelentésében feltárt hiányosságok orvoslásáért.
- (2) Valamennyi tagállam összekapcsolja kijelölt hatóságait a CIR-rel.

#### 57. cikk

### Az ETIAS központi egységének feladatai

Az ETIAS központi egysége felelős:

- a) a különböző személyazonosságok manuális ellenőrzéséért a 29. cikkel összhangban;
- b) az EES-ben, a VIS-ben, az Eurodacban és a SIS-ben tárolt adatok körében a többszörös személyazonosság észlelését célzó, a 69. cikkben említett ellenőrzés elvégzéséért.

#### IX. FEJEZET

### Más uniós jogi aktusok módosításai

#### 58. cikk

### A 767/2008/EK rendelet módosítása

A 767/2008/EK rendelet a következőképpen módosul:

1. Az 1. cikk a következő bekezdéssel egészül ki:

„A VIS azáltal, hogy az (EU) 2019/817 európai parlamenti és tanácsi rendelet (\*) 17. cikkének (1) bekezdése által létrehozott közös személyazonosítóadat-tárban (CIR) személyazonosító adatokat és útiokmány-adatokat, valamint biometrikus adatokat tárol, hozzájárul az említett rendelet 20. cikkében meghatározott feltételek szerint és célból a VIS-ben nyilvántartott személyek helyes azonosításának megkönnyítéséhez és segítéséhez.

(\*) Az Európai Parlament és a Tanács (EU) 2019/817 (2019. május 20.) rendelete az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízumügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról (HL L 135., 2019.5.22., 27. o.);

2. A 4. cikk a következő pontokkal egészül ki:

„12. »VIS-adatok«: a VIS központi rendszerében és a CIR-ben a 9–14. cikkel összhangban tárolt összes adat;

13. »személyazonosító adatok«: a 9. cikk 4. pontjának a) és aa) alpontjában említett adatok;

14. »ujjnyomata adatok«: az öt ujjnyomatra vonatkozó olyan adat, amelyet a jobb kéz, illetve azok megléte esetén a bal kéz mutató-, középső, gyűrűs- és kisujjáról, valamint hüvelykujjáról kell rögzíteni.”;

3. Az 5. cikk a következő bekezdéssel egészül ki:

„(1a) A CIR a 9. cikk (4) bekezdésének a)–c) pontjában, a 9. cikk (5) és (6) bekezdésében említett adatokat tartalmazza. A fennmaradó VIS-adatokat a VIS központi rendszerében kell tárolni.”;

4. A 6. cikk (2) bekezdése helyébe a következő szöveg lép:

„(2) A VIS-hez az adatokba való betekintés céljából való hozzáférés kizárólag a tagállamok azon hatóságainak megfelelő felhatalmazással rendelkező személyi állománya számára van fenntartva, amely a 15–22. cikkben meghatározott feladatokra hatáskörrel rendelkezik, valamint az (EU) 2019/817 rendelet 20. és 21. cikkében meghatározott célok tekintetében hatáskörrel rendelkező tagállami hatóságok és uniós ügynökségek megfelelően felhatalmazott személyi állománya számára. E hozzáférést olyan mértékűre kell korlátozni, amilyen mértékben az adatok szükségesek a feladataik említett célok szerinti elvégzéséhez, és a hozzáférésnek a kitűzött célokkal arányosnak kell lennie.”;

5. A 9. cikk 4. pontjának a)–c) alpontja helyébe a következő szöveg lép:

„a) vezetéknev (családi név); utónév vagy utónevek (keresztnevek); születési idő; nem;

aa) születéskori vezetéknev (korábbi vezetéknev vagy vezetéknevek); születési hely és ország; jelenlegi állampolgárság és születéskori állampolgárság;

- b) az úti okmány vagy okmányok típusa és száma, valamint az úti okmányt vagy okmányokat kiállító ország három betűből álló kódja;
- c) az úti okmány vagy okmányok érvényességének lejárat dátuma;
- ca) az úti okmányt kiállító hatóság és a kiállítás időpontja;”.

59. cikk

**Az (EU) 2016/399 rendelet módosítása**

A 8. cikk a következő bekezdéssel egészül ki:

„(4a) Amennyiben a belépéskor vagy a kilépéskor a megfelelő adatbázisokban – többek között az (EU) 2019/817 európai parlamenti és tanácsi rendelet (\*) 25. cikkének (1) bekezdésével létrehozott, többszörös személyazonosságot észlelő rendszerben – az említett rendelet 6. cikkének (1) bekezdésével létrehozott európai keresőportálon keresztül végzett lekérdezés sárga kapcsolatot vagy vörös kapcsolatot eredményez, az ellenőrzést végző határőr az összekapcsolt személyazonosító adatok vagy útiokmány-adatok közötti különbségek értékelése céljából lekérdezést végez az említett rendelet 17. cikkének (1) bekezdésével létrehozott közös személyazonosítóadat-tárban, vagy a SIS-ben, vagy mindkettőben. Az ellenőrzést végző határőr elvégez minden olyan további ellenőrzést, amely a kapcsolat besorolására és színére vonatkozó határozat meghozatalához szükséges.

Az (EU) 2019/817 rendelet 69. cikkének (1) bekezdésével összhangban ezt a bekezdést csak a többszörös személyazonosságot észlelő rendszer működésének az említett rendelet 72. cikkének (4) bekezdése szerinti megkezdésétől kezdődően kell alkalmazni.

(\*) Az Európai Parlament és a Tanács (EU) 2019/817 (2019. május 20.) rendelete az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízumügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról (HL L 135., 2019.5.22., 27. o.)”.

60. cikk

**Az (EU) 2017/2226 rendelet módosítása**

Az (EU) 2017/2226 rendelet a következőképpen módosul:

1. Az 1. cikk a következő bekezdéssel egészül ki:

„(3) Az EES azáltal, hogy az (EU) 2019/817 európai parlamenti és tanácsi rendelet (\*) 17. cikkének (1) bekezdése által létrehozott közös személyazonosítóadat-tárban (CIR) személyazonosító adatokat és útiokmány-adatokat, valamint biometrikus adatokat tárol, hozzájárul az említett rendelet 20. cikkében meghatározott feltételek szerint és célból az EES-ben nyilvántartott személyek helyes azonosításának megkönnyítéséhez és segítéséhez.

(\*) Az Európai Parlament és a Tanács (EU) 2019/817 (2019. május 20.) rendelete az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízumügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról (HL L 135., 2019.5.22., 27. o.)”;

2. A 3. cikk (1) bekezdése a következőképpen módosul:

a) a 22. pont szövege helyébe a következő szöveg lép:

„22. »EES-adatok«: a 15–20. cikknek megfelelően az EES központi rendszerében és a CIR-ben tárolt összes adat.”;

b) a szöveg a következő ponttal egészül ki:

„22a. »személyazonosító adatok«: a 16. cikk (1) bekezdésének a) pontjában említett adatok, valamint a 17. cikk (1) bekezdésében és a 18. cikk (1) bekezdésében említett vonatkozó adatok;”

c) a szöveg a következő pontokkal egészül ki:

„32. »ESP«: az (EU) 2019/817 rendelet 6. cikkének (1) bekezdésével létrehozott európai keresőportál;

33. »CIR«: az (EU) 2019/817 rendelet 17. cikkének (1) bekezdésével létrehozott közös személyazonosítóadat-tár;”;

3. A 6. cikk (1) bekezdése a következő ponttal egészül ki:
- „j) a személyek helyes azonosításának biztosítása.”;
4. A 7. cikk a következőképpen módosul:
- a) az (1) bekezdés a következőképpen módosul:
- i,  
a szöveg a következő ponttal egészül ki:
- „aa) a CIR központi infrastruktúrája az (EU) 2019/817 rendelet 17. cikke (2) bekezdésének a) pontjában említettek szerint;”
- ii.  
az f) pont helyébe a következő szöveg lép:
- „f) biztonságos kommunikációs infrastruktúra az EES központi rendszere és az ESP központi infrastruktúrái, valamint a CIR között.”;
- b) a szöveg a következő bekezdéssel egészül ki:
- „(1a) A CIR a 16. cikk (1) bekezdésének a)–d) pontjában, a 17. cikk (1) bekezdésének a), b) és c) pontjában és a 18. cikk (1) és (2) bekezdésében említett adatokat tartalmazza. A többi EES-adatot az EES központi rendszerében kell tárolni.”;
5. A 9. cikk a következő bekezdéssel egészül ki:
- „(4) A CIR-ben tárolt EES-adatokhoz való hozzáférést kizárólag az egyes tagállamok olyan nemzeti hatóságainak megfelelően felhatalmazott személyi állománya, valamint az olyan uniós ügynökségek megfelelően felhatalmazott személyi állománya számára kell fenntartani, amelyek az (EU) 2019/817 rendelet 20. és 21. cikkében meghatározott célok tekintetében illetékesek. E hozzáférést olyan mértékűre kell korlátozni, amilyen mértékben az adatok szükségesek a feladataik említett célok szerinti elvégzéséhez, és a hozzáférésnek a kitűzött célokkal arányosnak kell lennie.”;
6. A 21. cikk a következőképpen módosul:
- a) az (1) bekezdés helyébe a következő szöveg lép:
- „(1) Amennyiben az EES központi rendszerébe vagy a CIR-be történő adatbevitel technikailag kivitelezhetetlen, vagy az EES központi rendszere vagy a CIR meghibásodik, a 16–20. cikkben említett adatokat ideiglenesen a 7. cikk szerinti egységes nemzeti interfészen kell tárolni. Amennyiben erre nincs lehetőség, az adatokat elektronikus formában ideiglenesen helyben kell tárolni. Az adatbevitel technikai kivitelezhetlenségének vagy a meghibásodásnak a megszüntetése után az az adatokat mindkét esetben haladéktalanul be kell vinni az EES központi rendszerébe vagy a CIR-be. A tagállamok megteszik a megfelelő intézkedéseket, és gondoskodnak a szükséges infrastruktúráról, berendezésekről és erőforrásokról annak biztosítása érdekében, hogy az ilyen ideiglenes helyi tárolás bármikor, bármely határátkelőhelyen megvalósítható legyen.”;
- b) a (2) bekezdés első albekezdése helyébe a következő szöveg lép:
- „(2) A határforgalom-ellenőrzés elvégzésére vonatkozó, az (EU) 2016/399 rendelet szerinti kötelezettség sérelme nélkül, a határforgalom-ellenőrzést végző hatóság abban a kivételes helyzetben, amikor technikailag kivitelezhetetlen az adatoknak az EES központi rendszerébe és a CIR-be, vagy az egységes nemzeti interfészbe való bevitele, valamint technikailag kivitelezhetetlen az adatok elektronikus formában történő ideiglenes helyi tárolása is, a biometrikus adatok kivételével az e rendelet 16–20. cikkében említett adatokat manuálisan tárolja, és a harmadik országbeli állampolgárok úti okmányait beléptetőbélyegző- vagy kiléptetőbélyegző-lenyomattal látja el. Az adatokat, amint az technikailag lehetséges, be kell vinni az EES központi rendszerébe és a CIR-be.”;
7. A 23. cikk a következőképpen módosul:
- a) a szöveg a következő bekezdéssel egészül ki:
- „(2a) Az e cikk (1) bekezdése szerinti ellenőrzések céljából a határforgalom-ellenőrzést végző hatóság lekérdezést indít az ESP segítségével a harmadik országbeli állampolgárral kapcsolatos adatoknak az EES és a VIS vonatkozó adataival való összehasonlítása céljából.”;
- b) a (4) bekezdés első albekezdése helyébe a következő szöveg lép:
- „(4) Arra az esetre, ha az e cikk (2) bekezdésében felsorolt alfanumerikus adatok alapján végzett keresés azt mutatja, hogy a harmadik országbeli állampolgárról nem rögzítettek adatokat az EES-ben, ha a harmadik országbeli állampolgár e cikk (2) bekezdése szerinti ellenőrzése nem jár eredménnyel, vagy ha kétségek merülnek fel a harmadik országbeli állampolgár személyazonosságát illetően, a határforgalom-ellenőrzést végző hatóságok számára személyazonosság céljából a 27. cikkel összhangban hozzáférést kell biztosítani az adatokhoz, hogy a 14. cikkel összhangban egyéni aktát hozzanak létre vagy frissítsenek.”;

8. A 32. cikk a következő bekezdéssel egészül ki:

„(1a) Azokban az esetekben, amikor a kijelölt hatóságok az (EU) 2019/817 rendelet 22. cikkével összhangban lekérdezést kezdeményeztek a CIR-ben, az e cikkben meghatározott feltételek teljesülése esetén, és amennyiben az (EU) 2019/817 rendelet 22. cikkének (2) bekezdésében említett válasz alapján kiderül, hogy az EES-ben tárolnak adatokat, a kijelölt hatóságok lekérdezés céljából hozzáférhetnek az EES-hez.”;

9. A 33. cikk a következő bekezdéssel egészül ki:

„(1a) Azokban az esetekben, amikor az Europol az (EU) 2019/817 rendelet 22. cikkével összhangban lekérdezést kezdeményezett a CIR-ben, az e cikkben meghatározott feltételek teljesülése esetén, és amennyiben az (EU) 2019/817 rendelet 22. cikkének (2) bekezdésében említett válasz alapján kiderül, hogy az EES-ben tárolnak adatokat, az Europol lekérdezés céljából hozzáférhet az EES-hez.”;

10. A 34. cikk a következőképpen módosul:

- a) az (1) és a (2) bekezdésben „az EES központi rendszerében” szövegrész helyébe az „a CIR-ben és az EES központi rendszerében” szövegrész lép;
- b) az (5) bekezdésben az „EES központi rendszeréből” szövegrész helyébe az „EES központi rendszeréből és a CIR-ből” szövegrész lép;

11. A 35. cikk (7) bekezdése helyébe a következő szöveg lép:

„(7) Az EES központi rendszere és a CIR azonnali értesítést küld valamennyi tagállamnak az EES vagy a CIR adatainak törléséről, és adott esetben törli őket az azonosított személyek 12. cikk (3) bekezdésében említett listájáról.”;

12. A 36. cikkben „az EES központi rendszere” szövegrész helyébe „az EES központi rendszere és a CIR” szövegrész lép.

13. A 37. cikk a következőképpen módosul:

- a) az (1) bekezdés első albekezdésének helyébe a következő szöveg lép:

„(1) Az eu-LISA felel az EES központi rendszere és a CIR, az egységes nemzeti interfészek, a kommunikációs infrastruktúra, valamint az EES központi rendszere és a VIS központi rendszere közötti biztonságos kommunikációs csatorna fejlesztéséért. Szintén az eu-LISA felel – a 13. cikk (7) bekezdésében említett részletes szabályokkal és a 36. cikk első bekezdésének h) pontja alapján elfogadott feltételekkel összhangban – a 13. cikkben említett webes szolgáltatás fejlesztéséért, valamint a 63. cikk (2) bekezdésében említett adattár fejlesztéséért.”;

- b) a (3) bekezdés első albekezdése helyébe a következő szöveg lép:

„(3) Az eu-LISA felel az EES központi rendszere és a CIR, az egységes nemzeti interfészek, valamint az EES központi rendszere és a VIS központi rendszere közötti biztonságos kommunikációs csatorna üzemeltetési igazgatásáért. Az eu-LISA– költség-haszon elemzés alapján – a tagállamokkal együttműködve biztosítja, hogy az EES központi rendszere és a CIR, az egységes nemzeti interfészek, a kommunikációs infrastruktúra, továbbá az EES központi rendszere és a VIS központi rendszere közötti biztonságos kommunikációs csatorna, csakúgy mint a 13. cikkben említett webes szolgáltatás és a 63. cikk (2) bekezdésében említett adattár tekintetében mindenkor a legjobb rendelkezésre álló technológiát alkalmazzák. Az eu-LISA felel továbbá az EES központi rendszere és az egységes nemzeti interfészek közötti kommunikációs infrastruktúra, a 13. cikkben említett webes szolgáltatás és a 63. cikk (2) bekezdésében említett adattár üzemeltetési igazgatásáért is.”;

14. A 46. cikk (1) bekezdése a következő ponttal egészül ki:

„f) hivatkozást az ESP használatára az EES lekérdezése céljából, az (EU) 2019/817 rendelet 7. cikkének (2) bekezdésében említettek szerint.”;

15. A 63. cikk a következőképpen módosul:

- a) a (2) bekezdés helyébe a következő szöveg lép:

„(2) E cikk (1) bekezdésének alkalmazásában az eu-LISA az ugyanazon bekezdésben említett adatokat az (EU) 2019/817 rendelet 39. cikkében említett, a jelentések és statisztikák központi adattárában tárolja.”;

- b) a (4) bekezdés a következő albekezdéssel egészül ki:

„A napi statisztikákat a jelentések és statisztikák központi adattárában kell tárolni.”.

## 61. cikk

**Az (EU) 2018/1240 rendelet módosítása**

Az (EU) 2018/1240 rendelet a következőképpen módosul:

1. Az 1. cikk a következő bekezdéssel egészül ki:

„(3) A személyazonosító adatoknak és útiokmány-adatoknak az (EU) 2019/817 európai parlamenti és tanácsi rendelet (\*) 17. cikkének (1) bekezdésével létrehozott közös személyazonosítóadat-tárban (a továbbiakban: CIR) történő tárolásával az ETIAS hozzájárul az említett rendelet 20. cikkében említett feltételek szerint és célból az ETIAS-ban nyilvántartott személyek helyes azonosításának megkönnyítéséhez és elősegítéséhez.

(\*) Az Európai Parlament és a Tanács (EU) 2019/817 (2019. május 20.) rendelete az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízumügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról (HL L 135., 2019.5.22., 27. o.)”

2. A 3. cikk (1) bekezdése a következő pontokkal egészül ki:

„23. »CIR«: az (EU) 2019/817 rendelet 17. cikkének (1) bekezdésével létrehozott közös személyazonosítóadat-tár;”

24. »ESP«: az (EU) 2019/817 rendelet 6. cikke (1) bekezdésével létrehozott európai keresőportál;

25. »ETIAS központi rendszere«: a 6. cikk (2) bekezdésének a) pontjában említett központi rendszer a CIR-rel együtt, amennyiben a CIR tartalmazza a 6. cikk (2a) bekezdésében említett adatokat;

26. »személyazonosító adatok«: a 17. cikk (2) bekezdésének a), b) és c) pontjában említett adatok;

27. »útiokmány-adatok«: a 17. cikk (2) bekezdésének d) és e) pontjában említett adatok és az úti okmányt kiállító ország három betűből álló kódja a 19. cikk (3) bekezdésének c) pontjában említettek szerint;”

3. A 4. cikk a következő ponttal egészül ki:

„g) hozzájárulás a személyek helyes személyazonosságának megállapításához.”;

4. A 6. cikk a következőképpen módosul:

a) a (2) bekezdés a következőképpen módosul:

i. az a) pont helyébe a következő szöveg lép:

„a) egy központi rendszer, beleértve a 34. cikkben említett ETIAS figyelőlistát is;”;

ii. a szöveg a következő ponttal egészül ki:

„aa) a CIR;”;

iii. a d) pont helyébe a következő szöveg lép:

„d) egy biztonságos kommunikációs infrastruktúra a központi rendszer és a CIR központi infrastruktúrái között;”;

b) a szöveg a következő bekezdéssel egészül ki:

„(2a) A CIR tartalmazza a személyazonosító adatokat és az útiokmány-adatokat. A fennmaradó adatokat a központi rendszerben kell tárolni.”;

5. A 13. cikk a következőképpen módosul:

a) a cikk a következő bekezdéssel egészül ki:

„(4a) A CIR-ben tárolt ETIAS személyazonosító adatokhoz és útiokmány-adatokhoz való hozzáférést továbbá kizárólag az egyes tagállamok olyan nemzeti hatóságainak megfelelően felhatalmazott személyi állománya, valamint az olyan uniós ügynökségek megfelelően felhatalmazott személyi állománya számára kell fenntartani, amelyek az (EU) 2019/817 rendelet 20. és 21. cikkében meghatározott célok tekintetében illetékesek. E hozzáférést olyan mértékűre kell korlátozni, amilyen mértékben az adatok szükségesek a feladataik említett célok szerinti elvégzéséhez, és a kitűzött célokkal arányosnak kell lennie.”;



b) az (5) bekezdés helyébe a következő szöveg lép:

„(5) Minden tagállam kijelöli az e cikk (1), (2), (4) és (4a) bekezdésében említett illetékes nemzeti hatóságokat, és a 87. cikk (2) bekezdésével összhangban haladéktalanul közli e hatóságok jegyzékét az eu-LISA-val. E jegyzékben fel kell tüntetni, hogy az egyes hatóságok erre megfelelően felhatalmazott személyi állománya milyen célból férhet hozzá az ETIAS információs rendszer adataihoz e cikk (1), (2), (4) és (4a) bekezdéseivel összhangban.”;

6. A 17. cikk (2) bekezdése a következőképpen módosul:

a) az a) pont helyébe a következő szöveg lép:

„a) vezetéknev (családi név), utónév vagy utónevek (keresztnev vagy keresztnevek), születés kori vezetéknev; születési idő, születési hely, nem, jelenlegi állampolgárság;”

b) a bekezdés a következő ponttal egészül ki:

„aa) születési ország, a kérelmező szüleinek utóneve vagy utónevei;”

7. A 19. cikk (4) bekezdésében a „17. cikk (2) bekezdésének a) pontja” szövegrész helyébe a „17. cikk (2) bekezdésének a) és aa) pontja” szövegrész lép.

8. A 20. cikk a következőképpen módosul:

a) a (2) bekezdés első albekezdése helyébe a következő szöveg lép:

„(2) Az ETIAS központi rendszere az ESP használatával lekérdezést indít, hogy összehasonlítsa a 17. cikk (2) bekezdésének a), aa), b), c), d), f), g), j), k) és m) pontjában és a 17. cikk (8) bekezdésében említett vonatkozó adatokat az ETIAS központi rendszerben, a SIS-ben, az EES-ben, a VIS-ben, az Eurodacban, az Europol-adatokban és az Interpol SLTD és TDAWN adatbázisaiban tárolt adatrekordban, fájlban vagy kérelemfájlban rögzített figyelmeztető jelzésben szereplő adatokkal.”;

b) a (4) bekezdésben a „17. cikk (2) bekezdésének a), b), c), d), f), g), j), k) és m) pontjában,” szövegrész helyébe a „17. cikk (2) bekezdésének a), aa), b), c), d), f), g), j), k) és m) pontjában,” szövegrész lép.

c) az (5) bekezdésben a „17. cikk (2) bekezdésének a), c), f), h) és i) pontjában” szövegrész helyébe a „17. cikk (2) bekezdésének a), aa), c), f), h) és i) pontjában” szövegrész lép.

9. A 23. cikk (1) bekezdése helyébe a következő szöveg lép:

„(1) Az ETIAS központi rendszere az ESP használatával lekérdezést kezdeményez, hogy összehasonlítsa a 17. cikk (2) bekezdésének a), aa), b) és d) pontjában említett releváns adatokat a SIS-ben szereplő adatokkal annak megállapítása érdekében, hogy a kérelmező nem áll-e az alábbi figyelmeztető jelzések valamelyikének a hatálya alatt:

a) eltűnt személyekkel kapcsolatos figyelmeztető jelzés;

b) bírósági eljárásban való részvételük érdekében keresett személyekre vonatkozó figyelmeztető jelzés;

c) személyekre vonatkozóan rejtett ellenőrzés vagy célzott ellenőrzés céljából kiadott figyelmeztető jelzés.”;

10. Az 52. cikk a következő bekezdéssel egészül ki:

„(1a) Azokban az esetekben, amikor a kijelölt hatóságok az (EU) 2019/817 rendelet 22. cikkével összhangban lekérdezést indítottak a CIR-ben, e cikknek megfelelően lekérdezés céljából hozzáférhetnek az ETIAS központi rendszerében tárolt kérelemfájlokhoz, amennyiben az (EU) 2019/817 rendelet 22. cikkének (2) bekezdésében említett válasz azt mutatja, hogy az adatokat az ETIAS központi rendszerében tárolt kérelemfájlokban tárolják.”;

11. Az 53. cikk a következő bekezdéssel egészül ki:

„(1a) Azokban az esetekben, amikor az Europol az (EU) 2019/817 rendelet 22. cikkével összhangban lekérdezést kezdeményezett a CIR-ben, e cikknek megfelelően lekérdezés céljából hozzáférhet az ETIAS központi rendszerében tárolt kérelemfájlokhoz, amennyiben az (EU) 2019/817 rendelet 22. cikkének (2) bekezdésében említett válasz azt mutatja, hogy az adatokat az ETIAS központi rendszerében tárolt kérelemfájlokban tárolják.”;

12. A 65. cikk (3) bekezdésének ötödik albekezdésében a „17. cikk (2) bekezdésének a), b), d), e) és f) pontja” szövegrész helyébe a „17. cikk (2) bekezdésének a), aa), b), c), d), e) és f) pontja” szövegrész lép.

13. A 69. cikk (1) bekezdése a következő bekezdéssel egészül ki:

„ca) adott esetben hivatkozás az ESP-nak az ETIAS központi rendszeréből való lekérdezés céljából történő használatára az (EU) 2019/817 rendelet 7. cikkének (2) bekezdésében említettek szerint;”;

14. A 73. cikk (2) bekezdésében a „központi adattárát” szövegrész helyébe „az (EU) 2019/817 rendelet 39. cikkében említett, a jelentések és statisztikák központi adattárát – amennyiben az az ETIAS központi rendszeréből származó adatokat tartalmazza az említett rendelet 84. cikkével összhangban –” szövegrész lép.

15. A 74. cikk (1) bekezdésének első albekezdése helyébe a következő szöveg lép:

„(1) Az ETIAS rendszer üzemeltetésének megkezdését követően az eu-LISA felelős az ETIAS központi rendszere és az egységes nemzeti interfészek technikai irányításáért. Felelős továbbá az ETIAS vizsgálati szabályok kialakításához és aktualizálásához szükséges műszaki tesztelésért. Az eu-LISA-nak – költség-haszon elemzés alapján – a tagállamokkal együttműködve mindenkor gondoskodnia kell a legjobb rendelkezésre álló technológia alkalmazásáról. Az eu-LISA felelős továbbá a 6. cikkben említett következő komponensek technikai irányításáért: az ETIAS központi rendszere és az egységes nemzeti interfészek közötti kommunikációs infrastruktúra, valamint a nyilvánosan elérhető honlap, a mobil eszközökre telepíthető alkalmazás, az e-mail-szolgáltatás, a biztonságos felhasználói fiók-szolgáltatás, a kérelmezők rendelkezésére álló státuszlekérdező eszköz, a kérelmezők hozzájáruló nyilatkozatának megtételéhez használt eszköz, az ETIAS figyelőlistához kapcsolódó vizsgálati eszköz, a fuvarozói portál, a webes szolgáltatás, valamint a kérelmek feldolgozásához használt szoftver.”;

16. A 84. cikk (2) bekezdésének első albekezdése helyébe a következő szöveg lép:

„(2) E cikk (1) bekezdésének alkalmazásában az eu-LISA az ugyanazon bekezdésben említett adatokat az (EU) 2019/817 rendelet 39. cikkében említett, a jelentések és statisztikák központi adattárában tárolja. Az említett rendelet 39. cikkének (1) bekezdésével összhangban a rendszerek közötti statisztikai adatok és elemzési jelentések lehetővé teszik az e cikk (1) bekezdésében felsorolt hatóságok számára a testre szabható jelentések és statisztikák kinyerését, a 33. cikkben említett ETIAS vizsgálati szabályok végrehajtásának támogatását, a biztonsági, az illegális bevándorlással kapcsolatos és a magas szintű járványügyi kockázatok értékelésének javítását, a határforgalom-ellenőrzések hatékonyságának fokozását, valamint az ETIAS központi egysége és az ETIAS nemzeti egységei számára az utazási engedély iránti kérelmek feldolgozásához nyújtott segítséget.”;

17. A 84. cikk (4) bekezdése a következő albekezdéssel egészül ki:

„A napi statisztikákat az (EU) 2019/817 rendelet 39. cikkében említett, a jelentések és statisztikák központi adattárában kell tárolni.”.

## 62. cikk

### Az (EU) 2018/1726 rendelet módosítása

Az (EU) 2018/1726 rendelet a következőképpen módosul:

1. A 12. cikk helyébe a következő szöveg lép:

„12. cikk

#### Adatminőség

(1) Az ügynökség üzemeltetési felelősségi körébe tartozó rendszerekbe bevitt adatokkal kapcsolatos tagállami felelősségek sérelme nélkül az ügynökség, szorosan bevonva tanácsadó csoportját, az ügynökség üzemeltetési felelősségi körébe tartozó valamennyi rendszer tekintetében az adatminőség ellenőrzésére irányuló, automatizált mechanizmusokat és az adatminőségre vonatkozó közös mutatókat, valamint az adatok tárolására vonatkozó minőségi minimumkövetelményeket alakít ki, az említett rendszereket szabályozó jogi eszközök vonatkozó rendelkezéseivel, valamint az (EU) 2019/817 (\*) és az (EU) 2019/818 (\*\*) európai parlamenti és tanácsi rendelet 37. cikkével összhangban.

(2) Az ügynökség az (EU) 2019/817 rendelet és az (EU) 2019/818 rendelet 39. cikkével összhangban létrehozza a jelentések és statisztikák kizárólag anonimizált adatokat tartalmazó központi adattárát, az ügynökség által kezelt nagyméretű IT-rendszerek fejlesztését, létrehozását, működtetését és használatát szabályozó jogi eszközök különös rendelkezéseire is figyelemmel.

(\*) Az Európai Parlament és a Tanács (EU) 2019/817 (2019. május 20.) az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízumügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról (HL L 135., 2019.5.22., 27. o.).

(\*\*) Az Európai Parlament és a Tanács (EU) 2019/818 (2019. május 20.) rendelete az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a rendőrségi és igazságügyi együttműködés, a menekültügy és a migráció területén, valamint az (EU) 2018/1726, az (EU) 2018/1862 és az (EU) 2019/816 rendelet módosításáról. (HL L 135., 2019.5.22., 85. o.).”

2. A 19. cikk (1) bekezdése a következőképpen módosul:

a) a bekezdés a következő ponttal egészül ki:

„eea) elfogadja az interoperabilitási elemek fejlesztésének helyzetéről szóló jelentéseket az (EU) 2019/817 rendelet 78. cikkének (2) bekezdése és az (EU) 2019/818 rendelet 74. cikkének (2) bekezdése alapján;”

b) a ff) pont helyébe a következő szöveg lép:

„ff) elfogadja a SIS II műszaki működéséről szóló jelentéseket az (EU) 2018/1861 európai parlamenti és tanácsi rendelet (\*) 60. cikkének (7) bekezdése és az (EU) 2018/1862 európai parlamenti és tanácsi rendelet (\*\*) 74. cikkének (8) bekezdése szerint, a VIS műszaki működéséről szóló jelentéseket a 767/2008/EK rendelet 50. cikkének (3) bekezdése és a 2008/633/IB határozat 17. cikkének (3) bekezdése szerint, az EES műszaki működéséről szóló jelentéseket az (EU) 2017/2226 rendelet 72. cikkének (4) bekezdése szerint, az ETIAS műszaki működéséről szóló jelentéseket az (EU) 2018/1240 rendelet 92. cikkének (4) bekezdése szerint, az ECRIS-TCN és az ECRIS referenciaalkalmazás műszaki működéséről szóló jelentéseket az (EU) 2019/816 európai parlamenti és tanácsi rendelet (\*\*\*) 36. cikkének (8) bekezdése szerint, valamint az interoperabilitási elemek műszaki működéséről szóló jelentéseket az (EU) 2019/817 rendelet 78. cikkének (3) bekezdése és az (EU) 2019/818 rendelet 74. cikkének (3) bekezdése szerint;

(\*) Az Európai Parlament és a Tanács (EU) 2018/1861 rendelete (2018. november 28.) a határforgalom-ellenőrzés terén a Schengeni Információs Rendszer (SIS) létrehozásáról, működéséről és használatáról, a Schengeni Megállapodás végrehajtásáról szóló egyezmény módosításáról, valamint az 1987/2006/EK rendelet módosításáról és hatályon kívül helyezéséről (HL L 312., 2018.12.7., 14. o.).

(\*\*) Az Európai Parlament és a Tanács (EU) 2018/1862 rendelete (2018. november 28.) a rendőrségi együttműködés és a büntetőügyekben folytatott igazságügyi együttműködés terén a Schengeni Információs Rendszer (SIS) létrehozásáról, működéséről és használatáról, a 2007/533/IB tanácsi határozat módosításáról és hatályon kívül helyezéséről, valamint az 1986/2006/EK európai parlamenti és tanácsi rendelet és a 2010/261/EU bizottsági határozat hatályon kívül helyezéséről (HL L 312., 2018.12.7., 56. o.).

(\*\*\*) Az Európai Parlament és a Tanács (EU) 2019/816 rendelete (2019. április 17.) az Európai Bűnügyi Nyilvántartási Információs Rendszer kiegészítése érdekében a harmadik országbeli állampolgárokkal és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval rendelkező tagállamok azonosítására szolgáló központosított rendszer (ECRIS-TCN) létrehozásáról, valamint az (EU) 2018/1726 rendelet módosításáról (HL L 135., 2019.5.22., 1. o.);

c) a hh) pont helyébe a következő szöveg lép:

„hh) hivatalos észrevételeket fogad el az európai adatvédelmi biztosnak az (EU) 2018/1861 rendelet 56. cikkének (2) bekezdése, a 767/2008/EK rendelet 42. cikkének (2) bekezdése, a 603/2013/EU rendelet 31. cikkének (2) bekezdése, valamint az (EU) 2017/2226 rendelet 56. cikkének (2) bekezdése, az (EU) 2018/1240 rendelet 67. cikke, továbbá az (EU) 2019/816 rendelet 29. cikkének (2) bekezdése, az (EU) 2019/817 rendelet és az (EU) 2019/818 rendelet 52. cikke szerinti vizsgálatokról szóló jelentéseivel kapcsolatban, valamint biztosítja e vizsgálatok megfelelő nyomon követését;”

d) az mm) pont helyébe a következő szöveg lép:

„mm) biztosítja az (EU) 2018/1861 rendelet 41. cikkének (8) bekezdése és az (EU) 2018/1862 rendelet 56. cikkének (7) bekezdése értelmében a SIS-ben tárolt adatok közvetlen keresésére jogosult illetékes hatóságok jegyzékének, valamint a (EU) 2018/1861 rendelet 7. cikkének (3) bekezdése, illetve az (EU) 2018/1862 rendelet 7. cikkének (3) bekezdése alapján a SIS (N.SIS) nemzeti rendszerek és a SIRENE-irodák jegyzékének, továbbá az (EU) 2017/2226 rendelet 65. cikkének (2) bekezdése szerinti illetékes hatóságok listájának, az (EU) 2018/1240 rendelet 87. cikkének (2) bekezdése szerinti illetékes hatóságok listájának, az (EU) 2019/816 rendelet 34. cikkének (2) bekezdése szerinti központi hatóságok listájának, valamint az (EU) 2019/817 rendelet 71. cikkének (1) bekezdése és az (EU) 2019/818 rendelet 67. cikkének (1) bekezdése szerinti hatóságok jegyzékének évenkénti közzétételét;”

3. A 22. cikk (4) bekezdése helyébe a következő szöveg lép:

„(4) Az Europol és az Eurojust megfigyelőként részt vehet az igazgatótanács ülésein, amikor a SIS II-t érintő, a 2007/533/IB határozat alkalmazásával kapcsolatos kérdés van napirenden.

Az Európai Határ- és Partvédelmi Ügynökség megfigyelőként részt vehet az igazgatótanács ülésein, amikor a SIS-t érintő, az (EU) 2016/1624 rendelet alkalmazásával kapcsolatos kérdés van napirenden.

Az Europol megfigyelőként részt vehet az igazgatótanács azon ülésein is, amikor a VIS-t érintő, a 2008/633/IB határozat alkalmazásával kapcsolatos vagy az Eurodacot érintő, a 603/2013/EU rendelet alkalmazásával kapcsolatos kérdés van napirenden.

Az Europol megfigyelőként részt vehet az igazgatótanács azon ülésein, amikor az EES-t érintő, az (EU) 2017/2226 rendelet alkalmazásával kapcsolatos vagy az ETIAS-t érintő, az (EU) 2018/1240 rendelet alkalmazásával kapcsolatos kérdés van napirenden.

Az Európai Határ- és Partvédelmi Ügynökség megfigyelőként részt vehet az igazgatótanács ülésein, amikor az ETIAS-t érintő, az (EU) 2018/1240 rendelet alkalmazásával kapcsolatos kérdés van napirenden.

Az Eurojust, az Europol és az Európai Ügyészség megfigyelőként részt vehet az igazgatótanács ülésein, amikor az (EU) 2019/816 rendelettel kapcsolatos kérdés van napirenden.

Az Europol, Eurojust és az Európai Határ- és Partvédelmi Ügynökség megfigyelőként részt vehet az igazgatótanács ülésein, amikor az (EU) 2019/817, és az (EU) 2019/818 rendelettel kapcsolatos kérdés van napirenden.

Az igazgatótanács megfigyelőként meghívhat bármely más olyan személyt, akinek véleménye érdeklődésre tarthat számot.”

4. A 24. cikk (3) bekezdésének p) pontja helyébe a következő szöveg lép:

„p) a tisztviselők személyzeti szabályzata 17. cikkének sérelme nélkül, megállapítja a titoktartási követelményeket annak érdekében, hogy megfeleljenek az 1987/2006/EK rendelet 17. cikkének, a 2007/533/IB határozat 17. cikkének, a 767/2008/EK rendelet 26. cikke (9) bekezdésének, továbbá a 603/2013/EU rendelet 4. cikke (4) bekezdésének; az (EU) 2017/2226 rendelet 37. cikke (4) bekezdésének, az (EU) 2018/1240 rendelet 74. cikke (2) bekezdésének, az (EU) 2019/816 rendelet 11. cikke (16) bekezdésének, valamint az (EU) 2019/817 rendelet és az (EU) 2019/818 rendelet 55. cikke (2) bekezdésének;”

5. A 27. cikk a következőképpen módosul:

a) az (1) bekezdés a következő ponttal egészül ki:

„da) az interoperabilitással foglalkozó tanácsadó csoport;”

b) a (3) bekezdés helyébe a következő szöveg lép:

„(3) Az Europol, az Eurojust, valamint az Európai Határ- és Partvédelmi Ügynökség egyaránt kinevezhet egy-egy képviselőt a SIS II tanácsadó csoportba.

Az Europol képviselőt nevezhet ki továbbá a VIS, az Eurodac és az EES-ETIAS tanácsadó csoportba.

Az Európai Határ- és Partvédelmi Ügynökség kinevezhet továbbá egy képviselőt az EES-ETIAS tanácsadó csoportba.

Az Eurojust, az Europol és az Európai Ügyészség szintén kinevezhet egy-egy képviselőt az ECRIS-TCN-nel foglalkozó tanácsadó csoportba.

Az Europol, az Eurojust, valamint az Európai Határ- és Partvédelmi Ügynökség kinevezhet egy-egy képviselőt az interoperabilitással foglalkozó tanácsadó csoportba.”

### 63. cikk

#### Az (EU) 2018/1861 rendelet módosítása

Az (EU) 2018/1861 rendelet a következőképpen módosul:

1. A 3. cikk a következő pontokkal egészül ki:

„22. »ESP«: az (EU) 2019/817 európai parlamenti és tanácsi rendelet (\*) 6. cikkének (1) bekezdésével létrehozott európai keresőportál;

23. »közös BMS«: az (EU) 2019/817 rendelet 12. cikkének (1) bekezdésével létrehozott közös biometrikus megfeleltetési szolgáltatás;

24. »CIR«: az (EU) 2019/817 rendelet 17. cikkének (1) bekezdésével létrehozott közös személyazonosítóadat-tár;

25. »MID«: az (EU) 2019/817 rendelet 25. cikkének (1) bekezdésével létrehozott, többszörös személyazonosságot észlelő rendszer;

(\*) Az Európai Parlament és a Tanács (EU) 2019/817 (2019. május 20.) rendelete az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízumügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról (HL L 135., 2019.5.22., 27. o.);

2. A 4. cikk a következőképpen módosul:

a) az (1) bekezdés b) és c) pontja helyébe a következő szöveg lép:

- „b) az egyes tagállamok nemzeti rendszere (a továbbiakban: N.SIS), amely a SIS központi rendszerrel kommunikáló nemzeti adatrendszerekből áll, ideértve legalább egy nemzeti vagy közös tartalék N.SIS-t;
- c) a CS-SIS, a tartalék CS-SIS és az NI-SIS közötti kommunikációs infrastruktúra (a továbbiakban: kommunikációs infrastruktúra), amely a SIS-adatok, valamint a 7. cikk (2) bekezdésében említett SIRENE-irodák közötti adatsere céljára rendelt kódolt virtuális hálózatot képez; és
- d) egy biztonságos kommunikációs infrastruktúra a CS-SIS, illetve az ESP, a közös BMS és a MID központi infrastruktúrái között.”;

b) a cikk a következő bekezdésekkel egészül ki:

„(8) Az (1)–(5) bekezdés sérelme nélkül a SIS-adatok az ESP útján is kereshetők.

(9) Az (1)–(5) bekezdés sérelme nélkül a SIS-adatok az (1) bekezdés d) pontjában említett biztonságos kommunikációs infrastruktúrán keresztül is továbbíthatók. Ezeket az adattovábbításokat olyan mértékre kell korlátozni, amilyen mértékben az adatok szükségesek az (EU) 2019/817 rendeletben említett célokhoz.”;

3. A 7. cikk a következő bekezdéssel egészül ki:

„(2a) A SIRENE-irodák biztosítják továbbá a különböző személyazonosságok manuális ellenőrzését az (EU) 2019/817 rendelet 29. cikkével összhangban. A SIRENE-irodák az e feladat elvégzéséhez szükséges mértékben hozzáféréssel rendelkeznek a CIR-ben és a MID-ben tárolt adatokhoz az (EU) 2019/817 rendelet 21. és 26. cikkében meghatározott célokra.”;

4. A 12. cikk (1) bekezdése helyébe a következő szöveg lép:

„(1) A tagállamok gondoskodnak arról, hogy a személyes adatokhoz való minden hozzáférést és a személyes adatok CS-SIS-szel való valamennyi cseréjét naplózzák az N.SIS-ben a lekérdezés jogszerűségének ellenőrzése, az adatkezelés jogszerűségének ellenőrzése, az önellenőrzés, az N.SIS megfelelő működésének biztosítása, továbbá az adatok sértetlensége és biztonsága érdekében. Ez nem vonatkozik a 4. cikk (6) bekezdésének a), b) és c) pontjában említett automatikus adatkezelési módokra.

A tagállamok gondoskodnak arról, hogy az ESP-n keresztül a személyes adatokhoz való minden hozzáférést szintén naplózzák a lekérdezés jogszerűségének ellenőrzése, az adatkezelés jogszerűségének ellenőrzése, az önellenőrzés, továbbá az adatok sértetlensége és biztonsága érdekében.”;

5. A 34. cikk (1) bekezdése a következő ponttal egészül ki:

„g) a különböző személyazonosságok ellenőrzése és a személyazonossággal való visszaélés elleni küzdelem az (EU) 2019/817 rendelet V. fejezetének megfelelően.”

6. A 60. cikk (6) bekezdése helyébe a következő szöveg lép:

„(6) A 15. cikk (4) bekezdése és e cikk (3), (4) és (5) bekezdésének alkalmazása céljából az eu-LISA-nak a 15. cikk (4) bekezdésében és az e cikk (3) bekezdésében említett adatokat oly módon kell tárolnia, amely nem teszi lehetővé egyének személyazonosságának megállapítását az (EU) 2019/817 rendelet 39. cikkében említett jelentések és statisztikák központi adattárában.

Az eu-LISA lehetőséget nyújt a Bizottságnak és az e cikk (5) bekezdésében említett szervezeteknek arra, hogy személyre szabott jelentéseket és statisztikákat kérjenek le. Kérelemre az eu-LISA az (EU) 2019/817 rendelet 39. cikkével összhangban jelentéstételi és statisztikai célból hozzáférést biztosít a tagállamok, a Bizottság, az Európai és az Európai Határ- és Partvédelmi Ügynökség számára a központi adattárhoz.”.

#### 64. cikk

### A 2004/512/EK határozat módosítása

A 2004/512/EK tanácsi határozat 1. cikke (2) bekezdése helyébe a következő szöveg lép:

„(2) A Vízuminformációs Rendszer egy centralizált architektúrán alapul, és a következőkből áll:

- a) az (EU) 2019/817 európai parlamenti és tanácsi rendelet (\*) 17. cikke (2) bekezdésének a) pontjában említett közös személyazonosítóadat-tár központi infrastruktúrája;
- b) egy központi információs rendszer (a továbbiakban: Központi Vízuminformációs Rendszer – CS-VIS);

- c) a tagállamok megfelelő illetékes nemzeti hatóságaival kapcsolatot biztosító tagállami interfészek (a továbbiakban: Nemzeti Interfész – NI-VIS),
- d) a Központi Vízüminformációs Rendszer és a Nemzeti Interfészek közötti kommunikációs infrastruktúra;
- e) az EES központi rendszere és a CS-VIS közötti biztonságos kommunikációs csatorna;
- f) biztonságos kommunikációs infrastruktúra a VIS központi rendszere, illetve az (EU) 2019/817 rendelet 6. cikkének (1) bekezdése által létrehozott európai keresőportál és az (EU) 2019/817 rendelet 17. cikkének (1) bekezdése által létrehozott közös személyazonosítóadat-tár központi infrastruktúrája között.

(\*) Az Európai Parlament és a Tanács (EU) 2019/817 (2019. május 20.) rendelete az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízümügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról (HL L 135., 2019.5.22., 27. o.).

#### 65. cikk

### A 2008/633/IB határozat módosítása

A 2008/633/IB határozat a következőképpen módosul:

1. Az 5. cikk a következő bekezdéssel egészül ki:

„(1a) Azokban az esetekben, amikor a kijelölt hatóságok az (EU) 2019/817 európai parlamenti és tanácsi rendelet (\*) 22. cikkével összhangban lekérdezést kezdeményeztek a közös személyazonosítóadat-tárban (CIR), az e cikkben meghatározott hozzáférési feltételek teljesülése esetén betekintés céljából hozzáférhetnek a VIS-hez, amennyiben az említett rendelet 22. cikkének (2) bekezdésében említett válasz alapján kiderül, hogy a VIS-ben adatokat tárolnak.

(\*) Az Európai Parlament és a Tanács (EU) 2019/817 (2019. május 20.) rendelete az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízümügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról (HL L 135., 2019.5.22., 27. o.).

2. A 7. cikk a következő bekezdéssel egészül ki:

„(1a) Azokban az esetekben, amikor az Europol az (EU) 2019/817 rendelet 22. cikkével összhangban lekérdezést kezdeményezett a CIR-ben, az e cikkben meghatározott hozzáférési feltételek teljesülése esetén betekintés céljából az Europol hozzáférhet a VIS-hez, amennyiben az említett rendelet 22. cikkének (2) bekezdésében említett válasz alapján kiderül, hogy a VIS-ben adatokat tárolnak.”

#### X. FEJEZET

### Záró rendelkezések

#### 66. cikk

### Jelentéstétel és statisztika

(1) A tagállamok illetékes hatóságainak, a Bizottságnak és az eu-LISA-nak a megfelelő felhatalmazással rendelkező személyi állománya kizárólag jelentések és statisztikák összeállítása céljából betekintés céljából hozzáféréssel rendelkezik az ESP-vel kapcsolatos következő adatokhoz:

- a) az ESP-felhasználói profilonkénti lekérdezések száma;
- b) az Interpol egyes adatbázisaira vonatkozó lekérdezések száma.

Az adatok alapján nem válhat lehetővé az egyének azonosítása.

(2) A tagállamok illetékes hatóságainak, a Bizottságnak és az eu-LISA-nak a megfelelő felhatalmazással rendelkező személyi állománya kizárólag jelentések és statisztikák összeállítása céljából betekintés céljából hozzáféréssel rendelkezik a CIR-rel kapcsolatos következő adatokhoz:

- a) a 20., a 21. és a 22. cikk szerinti célokból folytatott lekérdezések száma;
- b) a személy állampolgársága, neme és születési éve;

- c) az úti okmány típusa és a kiállító ország három betűből álló kódja;
- d) a biometrikus adatokkal és azok nélkül végzett keresések száma.

Az adatok alapján nem válhat lehetővé az egyének azonosítása.

(3) A tagállamok illetékes hatóságainak, a Bizottságnak és az eu-LISA-nak a megfelelő felhatalmazással rendelkező személyi állománya kizárólag jelentések és statisztikák összeállítása céljából betekintés céljából hozzáféréssel rendelkezik a MID-del kapcsolatos következő adatokhoz:

- a) a biometrikus adatokkal és azok nélkül végzett keresések száma;
- b) a kapcsolatok száma valamennyi kapcsolat-típus esetében és az összekapcsolt adatokat tartalmazó uniós információs rendszerek;
- c) az az időszak, amelyen keresztül a sárga és vörös kapcsolat a rendszerben maradt.

Az adatok alapján nem válhat lehetővé az egyének azonosítása.

(4) Az Európai Határ- és Partvédelmi Ügynökség megfelelő felhatalmazással rendelkező személyi állománya betekintés céljából hozzáférhet az e cikk (1), (2) és (3) bekezdésében szereplő adatokhoz az (EU) 2016/1624 európai parlamenti és tanácsi rendelet <sup>(40)</sup> 11. és 13. cikkében említett kockázatelemzések és sebezhetőségi értékelések elvégzése céljából.

(5) Az Europol megfelelően felhatalmazott személyi állománya betekintés céljából hozzáférhet az e cikk (2) és (3) bekezdésében említett adatokhoz az (EU) 2016/794 rendelet 18. cikke (2) bekezdésének b) és c) pontjában említett stratégiai, tematikus és operatív elemzések elvégzése céljából.

(6) Az (1), a (2) és a (3) bekezdés alkalmazásában az említett bekezdésekben említett adatokat az eu-LISA a CRRS-ben tárolja. A CRRS-ben szereplő adatok alapján nem válhat lehetővé az egyének azonosítása, ugyanakkor az adatok az (1), a (2) és a (3) bekezdésben felsorolt hatóságok számára lehetővé teszik, hogy személyre szabott jelentéseket és statisztikákat kérjenek le a határforgalom-ellenőrzés hatékonyságának fokozása, a vízumkérelmek kezelésének megkönnyítése, valamint a tényeken alapuló uniós migrációs és biztonsági szakpolitikák kialakításának elősegítése érdekében.

(7) Kérés esetén a Bizottság az Európai Unió Alapjogi Ügynökségének rendelkezésére bocsátja a releváns információkat e rendelet alapvető jogokra gyakorolt hatásának értékelése céljából.

#### 67. cikk

### **Az európai keresőportál használatára vonatkozó átmeneti időszak**

(1) Az ESP működésbe lépésétől számított két éven keresztül a 7. cikk (2) és (4) bekezdésében foglalt kötelezettségek nem alkalmazandók, és az ESP használata nem kötelező.

(2) A Bizottság felhatalmazást kap arra, hogy a 73. cikknek megfelelően felhatalmazáson alapuló jogi aktust fogadjon el, amelyben módosítja e rendeletet az e cikk (1) bekezdésében említett időszak egyszeri, legfeljebb 1 évvel történő meghosszabbítása révén, amennyiben az ESP végrehajtásának értékelése azt mutatja, hogy e meghosszabbítás különösen szükséges annak fényében, hogy az ESP működtetésének megkezdése milyen hatással járna a határforgalom-ellenőrzés megszervezésére és időtartamára.

#### 68. cikk

### **A közös személyazonosítóadat-tárhoz terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából történő hozzáférésre vonatkozó rendelkezésekre alkalmazandó átmeneti időszak**

A 22. cikket, a 60. cikk 8. és 9. pontját, a 61. cikk 10. és 11. pontját, valamint a 65. cikket a CIR működése megkezdésének 72. cikk (3) bekezdésében említett időpontjától kell alkalmazni.

<sup>(40)</sup> Az Európai Parlament és a Tanács (EU) 2016/1624 rendelete (2016. szeptember 14.) az Európai Határ- és Parti Őrségről és az (EU) 2016/399 európai parlamenti és tanácsi rendelet módosításáról, valamint a 863/2007/EK európai parlamenti és tanácsi rendelet, a 2007/2004/EK tanácsi rendelet és a 2005/267/EK tanácsi határozat hatályon kívül helyezéséről (HL L 251., 2016.9.16., 1. o.).

## 69. cikk

**Átmeneti időszak a többszörös személyazonosság észlelése vonatkozásában**

(1) Azon időpontot követően egy éven át, amikor az eu-LISA a 72. cikk (4) bekezdésének b) pontjában említettek szerint bejelentette, hogy sikeresen lezárult a MID tesztelése, a MID működésének megkezdése előtt az ETIAS központi egysége felelős a többszörös személyazonosság észlelésére irányuló vizsgálat elvégzéséért az EES-ben, a VIS-ben, az Eurodacban és a SIS-ben tárolt adatok felhasználásával. A többszörös személyazonosság észlelésére irányuló vizsgálatokat kizárólag biometrikus adatok felhasználásával lehet elvégezni.

(2) Amennyiben a lekérdezés egy vagy több egyezést jelez és az összekapcsolt fájlokban szereplő személyazonosító adatok azonosak vagy hasonlóak, a 33. cikknek megfelelően fehér kapcsolatot kell létrehozni.

Amennyiben a lekérdezés egy vagy több egyezést jelez, és az összekapcsolt fájlokban szereplő személyazonosító adatok nem tekinthetők hasonlóknak, a 30. cikknek megfelelően sárga kapcsolatot kell létrehozni, és a 29. cikk szerinti eljárást kell alkalmazni.

Amennyiben több egyezés is szerepel, az egyezést kiváltó valamennyi adatelem között kapcsolatot kell létrehozni.

(3) Sárga kapcsolat létrehozása esetén a MID az ETIAS központi egysége számára hozzáférést biztosít a különböző uniós információs rendszerekben található személyazonosító adatokhoz.

(4) A SIS-ben szereplő figyelmeztető jelzéssel történő kapcsolat létrehozása esetén – kivéve az (EU) 2018/1860 rendelet 3. cikkében, illetve az (EU) 2018/1861 rendelet 24. és 25. cikkében, vagy az (EU) 2018/1862 rendelet 38. cikkében szereplő figyelmeztető jelzéseket – a MID a figyelmeztető jelzést létrehozó tagállam SIRENE-irodája számára hozzáférést biztosít a különböző információs rendszerekben található személyazonosító adatokhoz.

(5) Az ETIAS központi egysége vagy az e cikk (4) bekezdésében említett esetekben a figyelmeztető jelzést létrehozó tagállam SIRENE-irodája hozzáféréssel rendelkezik a személyazonosság-megerősítő dossziében szereplő adatokhoz, értékeli a különböző személyazonosságokat, a 31., a 32. és a 33. cikkel összhangban frissíti a kapcsolatot, és azt hozzáadja a személyazonosság-megerősítő dossziéhez.

(6) Az ETIAS központi egysége csak akkor értesíti a Bizottságot a 71. cikk (3) bekezdésének megfelelően, ha az összes sárga kapcsolatot manuálisan ellenőrizték és besorolásukat zöld, fehér vagy vörös kapcsolattá frissítették.

(7) A tagállamok szükség esetén segítséget nyújtanak az ETIAS központi egysége számára az e cikk szerinti többszörös személyazonosság észlelésére irányuló vizsgálat végrehajtásában.

(8) A Bizottság felhatalmazást kap arra, hogy a 73. cikknek megfelelően felhatalmazáson alapuló jogi aktust fogadjon el e rendelet módosítására az e cikk (1) bekezdésben említett időszak hat hónappal történő meghosszabbítása révén, amely két alkalommal alkalmanként hat hónappal meghosszabbítható. A meghosszabbítás csak azt követően adható meg, hogy felmérték a többszörös személyazonosság észlelésére irányuló vizsgálat lezárultához szükséges becsült időt, amely azt mutatja, hogy az (1) bekezdésben említett határidő lejárt vagy a folyamatban lévő meghosszabbítás lejárt előtt a többszörös személyazonosság észlelésére irányuló vizsgálat nem zárulhat le az ETIAS központi egységétől független okokból, és nem alkalmazhatók korrekciós intézkedések. Az értékelést legkésőbb az említett határidő lejártáig vagy a folyamatban lévő meghosszabbítás lejártáig három hónappal kell elvégezni.

## 70. cikk

**Költségek**

(1) Az ESP, a közös BMS, a CIR és a MID létrehozásával és működtetésével kapcsolatban felmerült költségeket az Unió általános költségvetéséből kell fedezni.

(2) A meglévő nemzeti határinfrastruktúrák integrációja, azoknak az egységes nemzeti interfészekhez való kapcsolódása, valamint az egységes nemzeti interfészek elhelyezésével kapcsolatban felmerülő költségeket az Unió általános költségvetéséből kell fedezni.

Ez alól kivételt képeznek az alábbi költségek:

- a) a tagállamok projektirányítási irodái (találkozók, kiküldetések, irodák);
- b) a nemzeti IT-rendszerek elhelyezése (helyszín, végrehajtás, villamos energia, hűtés);
- c) a nemzeti IT-rendszerek üzemeltetése (üzemeltetői és támogatási szerződések);
- d) a nemzeti kommunikációs hálózatok tervezése, fejlesztése, bevezetése, üzemeltetése és karbantartása;



(3) Az Európai Unió általános költségvetésének más forrásaiból e célból nyújtott további finanszírozás sérelme nélkül 32 077 000 EUR összeg igénybevételére kerül sor az 515/2014/EU rendelet 5. cikke (5) bekezdésének b) pontja szerinti 791 000 000 EUR összegű keretből az e rendelet végrehajtásával kapcsolatos, az e cikk (1) és (2) bekezdésében előírt végrehajtási költségek fedezésére.

(4) A (3) bekezdésben említett keretből az eu-LISA számára 22 861 000 EUR-t, az Europol számára 9 072 000 EUR-t és az Európai Unió Bűnüldözési Képzési Ügynöksége (CEPOL) számára 144 000 EUR-t kell elkülöníteni azért, hogy ezek az ügynökségek az e rendelet szerinti feladataik ellátásában támogatáshoz jussanak. E finanszírozást közvetett irányítás keretében kell végrehajtani.

(5) A kijelölt hatóságoknál felmerülő költségeket az e hatóságokat kijelölő tagállamoknak kell viselniük. Az egyes tagállamok viselik a kijelölt hatóságok CIR-hez való kapcsolódásának költségeit.

Az Europolnál felmerülő költségeket, beleértve a CIR-hez való kapcsolódást is, az Europol viseli.

#### 71. cikk

### Értesítések

(1) A tagállamok értesítik az eu-LISA-t a 7., a 20., a 21. és a 26. cikkben említett azon hatóságokról, amelyek használati jogosultsággal vagy hozzáféréssel rendelkeznek az ESP-hez, a CIR-hez, illetve a MID-hez.

E hatóságok összesített jegyzékét közzé kell tenni az *Európai Unió Hivatalos Lapjában* az egyes interoperabilitási elemeknek a 72. cikk szerinti működésbe lépését követő három hónapon belül. A jegyzék módosulása esetén az eu-LISA évente frissített összesített jegyzéket tesz közzé.

(2) Az eu-LISA értesíti a Bizottságot a 72. cikk (1) bekezdésének b) pontjában, (2) bekezdésének b) pontjában, (3) bekezdésének b) pontjában, (4) bekezdésének b) pontjában, (5) bekezdésének b) pontjában és (6) bekezdésének b) pontjában említett teszt sikeres befejezéséről.

(3) Az ETIAS központi egysége értesíti a Bizottságot a 69. cikkben említett átmeneti időszak sikeres befejezéséről.

(4) A Bizottság egy folyamatosan frissített nyilvános honlapon a tagállamok és a nyilvánosság rendelkezésére bocsátja az (1) bekezdés szerint bejelentett információkat.

#### 72. cikk

### A működés megkezdése

(1) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusban meghatározza azt az időpontot, amikor az ESP megkezdzi működését:

- a) elfogadták a 8. cikk (2) bekezdésében, a 9. cikk (7) bekezdésében és a 43. cikk (5) bekezdésében említett intézkedéseket;
- b) az eu-LISA bejelentette, hogy sikeresen lezárult az ESP átfogó tesztelése, amelyet az eu-LISA az ESP használatára jogosult tagállami hatóságokkal és uniós ügynökségekkel együttműködve hajtott végre;
- c) Az eu-LISA érvényesítette a 8. cikk (1) bekezdésében említett adatok összegyűjtésére és továbbítására vonatkozó technikai és jogi előírásokat, és azokról értesítette a Bizottságot.

Az ESP csak azt követően kérdezheti le az Interpol-adatbázisokat, hogy a technikai intézkedések lehetővé teszik a 9. cikk (5) bekezdésének való megfelelést. Ha a 9. cikk (5) bekezdésének való megfelelés nem teljesíthető, akkor az ESP nem végez lekérdezést az Interpol-adatbázisokban, de ez nem késleltetheti az ESP működésének megkezdését.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

(2) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusban meghatározza azt az időpontot, amikor a közös BMS megkezdzi működését:

- a) elfogadták a 13. cikk (5) bekezdésében és a 43. cikk (5) bekezdésében említett intézkedéseket;
- b) az eu-LISA bejelentette, hogy sikeresen lezárult a közös BMS átfogó tesztelése, amelyet az eu-LISA a tagállamok hatóságaival együttműködve hajtott végre;

- c) az eu-LISA érvényesítette a 13. cikkben említett adatok összegyűjtésére és továbbítására vonatkozó technikai és jogi előírásokat, és azokról értesítette a Bizottságot;
- d) az eu-LISA bejelentette az (5) bekezdés b) pontjában említett teszt sikeres befejezését.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

(3) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusban meghatározza azt az időpontot, amikor a CIR megkezdzi működését:

- a) elfogadták a 43. cikk (5) bekezdésében és a 78. cikk (10) bekezdésében említett intézkedéseket;
- b) az eu-LISA bejelentette, hogy sikeresen lezárult a CIR átfogó tesztelése, amelyet az eu-LISA a tagállamok hatóságaival együttműködve hajtott végre;
- c) az eu-LISA érvényesítette a 18. cikkben említett adatok összegyűjtésére és továbbítására vonatkozó technikai és jogi előírásokat, és azokról értesítette a Bizottságot;
- d) az eu-LISA bejelentette az (5) bekezdés b) pontjában említett teszt sikeres befejezését.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

(4) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusban meghatározza azt az időpontot, amikor a MID megkezdzi működését:

- a) elfogadták a 28. cikk (5) és (7) bekezdésében, a 32. cikk (5) bekezdésében, a 33. cikk (6) bekezdésében, a 43. cikk (5) bekezdésében és a 49. cikk (6) bekezdésében említett intézkedéseket;
- b) az eu-LISA bejelentette, hogy sikeresen lezárult a MID átfogó tesztelése, amelyet az eu-LISA a tagállamok hatóságaival és az ETIAS központi egységével együttműködve hajtott végre;
- c) az eu-LISA érvényesítette a 34. cikkben említett adatok összegyűjtésére és továbbítására vonatkozó technikai és jogi előírásokat, és azokról értesítette a Bizottságot;
- d) az ETIAS központi egysége értesítette a Bizottságot a 71. cikk (3) bekezdésében foglaltaknak megfelelően;
- e) az eu-LISA bejelentette, hogy sikeresen lezárultak az (1) bekezdés b) pontjában, a (2) bekezdés b) pontjában, a (3) bekezdés b) pontjában és az (5) bekezdés b) pontjában említett tesztek.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

(5) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusokban meghatározza azt az időpontot, amelytől kezdődően az adatminőség ellenőrzésére irányuló automatizált mechanizmusokat és eljárásokat, a közös adatminőségi mutatókat és az adatminőségi minimumkövetelményeket alkalmazni kell:

- a) elfogadták a 37. cikk (4) bekezdésében említett intézkedéseket;
- b) az eu-LISA bejelentette, hogy sikeresen lezárult az adatminőség ellenőrzésére irányuló automatizált mechanizmusok és eljárások, a közös adatminőségi mutatók és az adatminőségi minimumkövetelmények átfogó tesztelése, amelyet az eu-LISA a tagállamok hatóságaival együttműködve hajtott végre.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

(6) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusban meghatározza azt az időpontot, amikor a CRRS megkezdzi működését:

- a) elfogadták a 39. cikk (5) bekezdésében és a 43. cikk (5) bekezdésében említett intézkedéseket;
- b) az eu-LISA bejelentette, hogy sikeresen lezárult a CRRS átfogó tesztelése, amelyet az eu-LISA a tagállamok hatóságaival együttműködve hajtott végre;
- c) az eu-LISA érvényesítette a 39. cikkben említett adatok összegyűjtésére és továbbítására vonatkozó technikai és jogi előírásokat, és azokról értesítette a Bizottságot.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

(7) A Bizottság tájékoztatja az Európai Parlamentet és a Tanácsot az (1) bekezdés b) pontjának, az (1) bekezdés b) pontjának, a (2) bekezdés b) pontjának, a (3) bekezdés b) pontjának, a (4) bekezdés b) pontjának, az (5) bekezdés b) pontjának és a (6) bekezdés b) pontjának megfelelően végzett tesztek eredményéről.

(8) A tagállamok, az ETIAS központi egysége és az Europol az (1), a (2), a (3), illetve a (4) bekezdéssel összhangban a Bizottság által meghatározott időponttól megkezdik az egyes interoperabilitási elemek alkalmazását.

## 73. cikk

**A felhatalmazás gyakorlása**

(1) A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozóan a Bizottság részére adott felhatalmazás feltételeit ez a cikk határozza meg.

(2) A Bizottságnak a 28. cikk (5) bekezdésében, a 39. cikk (5) bekezdésében, a 49. cikk (6) bekezdésében, a 67. cikk (2) bekezdésében és a 69. cikk (8) bekezdésében említett, felhatalmazáson alapuló jogi aktusok elfogadására vonatkozó felhatalmazása öt éves időtartamra szól 2019. június 11-től kezdődő hatállyal. A Bizottság legkésőbb kilenc hónappal az öt éves időtartam letelte előtt jelentést készít a felhatalmazásról. A felhatalmazás hallgatólagosan meghosszabbodik a korábbival megegyező időtartamra, amennyiben az Európai Parlament vagy a Tanács nem ellenzi a meghosszabbítást legkésőbb három hónappal minden egyes időtartam letelte előtt.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 28. cikk (5) bekezdésében, a 39. cikk (5) bekezdésében, a 49. cikk (6) bekezdésében, a 67. cikk (2) bekezdésében és az 69. cikk (8) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon, vagy a benne megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(4) A felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban foglalt elveknek megfelelően konzultál az egyes tagállamok által kijelölt szakértőkkel.

(5) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

(6) A 28. cikk (5) bekezdése, a 39. cikk (5) bekezdése, a 49. cikk (6) bekezdése, a 67. cikk (2) bekezdése és a 69. cikk (8) bekezdése értelmében elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő két hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve, ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam két hónappal meghosszabbodik.

## 74. cikk

**Bizottsági eljárás**

(1) A Bizottság munkáját egy bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.

(2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikkét kell alkalmazni.

Ha a bizottság nem nyilvánít véleményt, a Bizottság nem fogadhatja el a végrehajtási jogi aktus tervezetét, és a 182/2011/EU rendelet 5. cikke (4) bekezdésének harmadik albekezdése alkalmazandó.

## 75. cikk

**Tanácsadó csoport**

Az eu-LISA tanácsadó csoportot hoz létre. Az interoperabilitási elemek kialakításának és fejlesztésének szakaszában az 54. cikk (4), (5) és (6) bekezdésének rendelkezéseit kell alkalmazni.

## 76. cikk

**Képzés**

Az eu-LISA az (EU) 2018/1726 rendeletnek megfelelően ellátja az interoperabilitási elemek technikai használatára vonatkozó képzés nyújtásával kapcsolatos feladatokat.

A tagállamok hatóságai és az uniós ügynökségek az interoperabilitási elemek használatával történő adatkezelésre felhatalmazott személyi állományuk számára megfelelő képzési programot biztosítanak az adatbiztonságról, az adatminőségről, az adatvédelmi szabályokról, az adatkezelési eljárásokról és a tájékoztatási kötelezettségről a 32. cikk (4) bekezdése, a 33. cikk (4) bekezdése és a 47. cikk szerint.

Szükség esetén uniós szintű közös képzéseket kell szervezni az említett témákról a tagállamok hatóságai és az uniós ügynökségek interoperabilitási elemek használatával történő adatkezelésre felhatalmazott személyi állományuk közötti együttműködés fokozása és a bevált gyakorlatok megosztása céljából. Különös figyelmet kell fordítani a többszörös személyazonosság észlelésére irányuló eljárásra, többek között a különböző személyazonosságok manuális ellenőrzésére és az ezzel járó, az alapvető jogokkal kapcsolatos biztosítékok garantálása iránti igényre.

## 77. cikk

**Gyakorlati kézikönyv**

A Bizottság a tagállamokkal, az eu-LISA-val és más érintett uniós ügynökségekkel szorosan együttműködve rendelkezésre bocsátja az interoperabilitási elemek bevezetésével és igazgatásával kapcsolatos gyakorlati kézikönyvet. A gyakorlati kézikönyv technikai és üzemeltetési iránymutatásokat és ajánlásokat foglal magában, illetve példákkal szolgál a bevált gyakorlatokra. A Bizottság a gyakorlati kézikönyvet ajánlás formájában fogadja el.

## 78. cikk

**Nyomon követés és értékelés**

(1) Az eu-LISA biztosítja azoknak az eljárásoknak a kialakítását, amelyekkel nyomon követhető egyrészt a tervezéssel és a költségekkel kapcsolatos célok fényében az interoperabilitási elemek fejlesztése és egységes nemzeti interfészhez való kapcsolódása, másrészt pedig a technikai eredményekkel, a költséghatékonysággal, a biztonsággal és a szolgáltatás minőségével kapcsolatos célok fényében az interoperabilitási elemek működése.

(2) Az eu-LISA 2019. december 12-ig, majd azt követően hathavonta az interoperabilitási elemek fejlesztési szakasza során jelentést készít az Európai Parlamentnek és a Tanácsnak arról, hogy hol tart az interoperabilitási elemek fejlesztése és egységes nemzeti interfészhez való kapcsolódása. A fejlesztés befejeztével jelentést kell benyújtani az Európai Parlamentnek és a Tanácsnak, amely részletesen bemutatja a célok – különösen a tervezéssel és a költségekkel kapcsolatos célok – megvalósítását és az esetleges eltérések indokait.

(3) Az eu-LISA az egyes interoperabilitási elemek működésének 72. cikk szerinti megkezdését követően négy évvel, majd azt követően négyévente jelentést nyújt be az Európai Parlamentnek, a Tanácsnak és a Bizottságnak az interoperabilitási elemek műszaki működéséről, beleértve azok biztonságosságát is.

(4) Ezenkívül az eu-LISA minden egyes jelentése után egy évvel a Bizottság átfogó értékelést készít az interoperabilitási elemekről, beleértve a következőket:

- a) e rendelet alkalmazásának értékelése;
- b) e rendelet elért eredményeinek a célkitűzések fényében történő vizsgálata, valamint az alapvető jogokra gyakorolt hatás vizsgálata, ideértve különösen az interoperabilitási elemek megkülönböztetésmentességhez való jogra gyakorolt hatásának értékelését;
- c) a webportál működésének értékelése, beleértve a webportál használatára és a megoldott kérelmek számára vonatkozó adatokat;
- d) az interoperabilitási elemek alapjául szolgáló megfontolások változatlan helytállóságának értékelése;
- e) az interoperabilitási elemek biztonságosságának értékelése;
- f) a CIR személyazonosítás céljából történő használatának értékelése;
- g) a CIR terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából történő használatának értékelése;
- h) a rendszer működéséből fakadó következmények értékelése, beleértve a határátkelőhelyeken a forgalom áramlására gyakorolt aránytalan hatásokat, valamint az Unió általános költségvetésére hatást gyakorló következményeket;
- i) az Interpol-adatbázisokban az ESP-n keresztül végzett keresések értékelése, beleértve az Interpol-adatbázisok lekérdezéséből eredő egyezések számára és a felmerült problémákra vonatkozó adatokat.

Az e bekezdés első albekezdése szerinti átfogó értékelések szükség esetén ajánlásokat tartalmaznak. A Bizottság továbbítja az értékelésről szóló jelentést az Európai Parlamentnek, a Tanácsnak, az európai adatvédelmi biztosnak és az Európai Unió Alapjogi Ügynökségének.

(5) A Bizottság 2020. június 12-ig, majd ezt követően mindaddig, amíg a Bizottság el nem fogadta a 72. cikkben említett végrehajtási jogi aktusokat, minden évben jelentést nyújt be az Európai Parlamentnek és a Tanácsnak az e rendelet teljes körű alkalmazására vonatkozó előkészületek aktuális állásáról. Ennek a jelentésnek részletes információkat kell tartalmaznia a felmerült költségekről, valamint minden olyan kockázatról, amely hatással lehet az összköltségre.

(6) A Bizottság két évvel a MID működésének a 72. cikk (4) bekezdése szerinti megkezdése után megvizsgálja a MID hatását a megkülönböztetésmentességhez való jogra. Az első jelentést követően a MID megkülönböztetésmentességhez való jogra gyakorolt hatásának vizsgálata az e cikk (4) bekezdésének b) pontjában említett vizsgálat részét képezi.

(7) A tagállamok és az Europol az eu-LISA és a Bizottság rendelkezésére bocsátják a (3)–(6) bekezdésben említett jelentések elkészítéséhez szükséges információkat. Ez a tájékoztatás nem veszélyeztetheti a kijelölt hatóságok munkamódszereit, és nem tartalmazhat a kijelölt hatóságok információforrásait, személyi állományának tagjait, illetve nyomozásait felfedő információt.

(8) Az eu-LISA a Bizottság rendelkezésére bocsátja a (4) bekezdésben említett átfogó értékelés elkészítéséhez szükséges információkat.

(9) Az érzékeny információk közzétételére irányadó nemzeti jogszabályok rendelkezéseinek tiszteletben tartása mellett, valamint a biztonság és a közrend védelme, a bűnmegelőzés, valamint a nemzeti nyomozások veszélyeztetésének megakadályozása érdekében szükséges korlátozások sérelme nélkül minden tagállam és az Europol éves jelentést készít a CIR-ben tárolt adatok terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából történő hozzáférés eredményességéről, amely jelentés információkat és statisztikákat tartalmaz az alábbiakról:

- a) a betekintés pontos célja, beleértve a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények típusait;
- b) azon megalapozott gyanú alapos indokai, miszerint a gyanúsított, az elkövető vagy az áldozat az (EU) 2017/2226 rendelet, a 767/2008/EK rendelet vagy az (EU) 2018/1240 rendelet hatálya alá tartozik;
- c) a CIR-hez terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából történő hozzáférés iránti kérelmek száma;
- d) a sikeres személyazonosítást eredményező esetek száma és típusa;
- e) a sürgősségi eseteket megalapozó kivételek szükségessége és alkalmazása, beleértve azokat az eseteket, amikor a központi hozzáférési pont az utólagos ellenőrzés során nem találta indokoltnak a sürgősséget.

A tagállamok és az Europol által készített éves jelentéseket a következő év június 30-ig kell megküldeni a Bizottságnak.

(10) A tagállamok rendelkezésére kell bocsátani egy olyan műszaki megoldást, amely kezeli a felhasználók 22. cikkben említett hozzáférés iránti kérelmeit, és megkönnyíti az e cikk (7) és a (9) bekezdése szerinti információknak az említett bekezdésekben említett jelentések és statisztikák összeállítására céljából történő összegyűjtését. A Bizottság végrehajtási jogi aktusokat fogad el a műszaki megoldások előírásaival kapcsolatban. Ezeket a végrehajtási jogi aktusokat a 74. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

#### 79. cikk

### Hatálybalépés és alkalmazhatóság

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

E rendelet ESP-vel kapcsolatos rendelkezéseit a Bizottság által a 72. cikk (1) bekezdésével összhangban meghatározott időponttól kell alkalmazni.

E rendelet közös BMS-szel kapcsolatos rendelkezéseit a Bizottság által a 72. cikk (2) bekezdésével összhangban meghatározott időponttól kell alkalmazni.

E rendelet CIR-rel kapcsolatos rendelkezéseit a Bizottság által a 72. cikk (3) bekezdésével összhangban meghatározott időponttól kell alkalmazni.

E rendelet MID-del kapcsolatos rendelkezéseit a Bizottság által a 72. cikk (4) bekezdésével összhangban meghatározott időponttól kell alkalmazni.

E rendeletnek az adatminőség ellenőrzésére irányuló, automatizált mechanizmusokkal és eljárásokkal, az adatminőségre vonatkozó közös mutatókkal és az adatminőségi minimumkövetelményekkel kapcsolatos rendelkezéseit a Bizottság által a 72. cikk (5) bekezdésével összhangban meghatározott időpontoktól kell alkalmazni.

E rendelet CRRS-szel kapcsolatos rendelkezéseit a Bizottság által a 72. cikk (6) bekezdésével összhangban meghatározott időponttól kell alkalmazni.

A 6., a 12., a 17., a 25., a 38., a 42., az 54., az 56., az 57., a 70., a 71., a 73., a 74., a 75. és a 77. cikket, valamint a 78. cikk (1) bekezdését 2019. június 11-től kell alkalmazni.

E rendeletet az Eurodac tekintetében a 603/2013/EU rendelet átdolgozott változata alkalmazásának kezdőnapjától kell alkalmazni.

Ez a rendelet a Szerződéseknek megfelelően teljes egészében kötelező és közvetlenül alkalmazandó a tagállamokban.

Kelt Brüsszelben, 2019. május 20-án.

*az Európai Parlament részéről*

*az elnök*

A. TAJANI

*a Tanács részéről*

*az elnök*

G. CIAMBA

---

**AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/818 RENDELETE****(2019. május 20.)****az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a rendőrségi és igazságügyi együttműködés, a menekültügy és a migráció területén, valamint az (EU) 2018/1726, az (EU) 2018/1862 és az (EU) 2019/816 rendelet módosításáról**

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen 16. cikkének (2) bekezdésére, 74. cikkére, 78. cikke (2) bekezdésének e) pontjára, 79. cikke (2) bekezdésének c) pontjára, 82. cikke (1) bekezdésének d) pontjára, 85. cikkének (1) bekezdésére, 87. cikke (2) bekezdésének a) pontjára, valamint 88. cikkének (2) bekezdésére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére <sup>(1)</sup>,

a Régiók Bizottságával folytatott konzultációt követően,

rendes jogalkotási eljárás keretében <sup>(2)</sup>,

mivel:

- (1) „A határigazgatás és a biztonság erősítését szolgáló, szilárd és intelligens információs rendszerek” című, 2016. április 6-i közleményében a Bizottság hangsúlyozta, hogy javítani kell az uniós adatkezelés keretét a határ- és biztonsági ellenőrzés területén. A közlemény az uniós határigazgatási, biztonsági, és migrációkezelési információs rendszerek közötti interoperabilitás megteremtésére irányuló folyamatot kezdeményezett az e rendszerekkel kapcsolatos, a nemzeti hatóságok munkáját akadályozó strukturális hiányosságok kezelése, valamint annak biztosítása céljából, hogy a határőrök, a vámhatóságok, a rendőrtisztek és az igazságügyi hatóságok rendelkezzenek a szükséges információkkal.
- (2) Az „Ütemterv a bel- és igazságügyi területen alkalmazott információcsere és információkezelés javítására, beleértve az interoperabilitást biztosító megoldásokat is” című, 2016. június 6-i dokumentumban a Tanács számos jogi, műszaki és operatív kihívást azonosított az uniós információs rendszerek interoperabilitása terén, és megoldások keresését sürgette.
- (3) A 2017. évi bizottsági munkaprogrammal kapcsolatos stratégiai prioritásokról szóló, 2016. július 6-i állásfoglalásában <sup>(3)</sup> az Európai Parlament javaslatokat terjesztett elő a meglévő uniós információs rendszerek javítására és fejlesztésére, az információs hiányosságok kezelésére, az interoperabilitás előmozdítására, valamint az információk kötelező uniós szintű megosztására, amelyet megfelelő adatvédelmi biztosítékok kísérnek.
- (4) Az Európai Tanács 2016. december 15-i következtetéseiben az uniós információs rendszerek és adatbázisok interoperabilitása terén további eredmények elérése érdekében a munka folytatását sürgette.
- (5) Az információs rendszerekkel és az interoperabilitással foglalkozó magas szintű szakértői csoport 2017. május 11-i zárójelentésében arra a következtetésre jutott, hogy az interoperabilitáshoz vezető gyakorlati megoldások irányába való elmozdulás szükséges és technikailag megvalósítható, és hogy az interoperabilitás elvileg működési előnyökkel járhat és az adatvédelmi követelményeknek eleget téve megvalósítható.
- (6) A „Hetedik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról” című, 2017. május 16-i közleményében a Bizottság – 2016. április 6-i közleményével, valamint az információs rendszerekkel és az interoperabilitással foglalkozó magas szintű szakértői csoport megállapításaival és ajánlásaival összhangban – új megközelítésbe helyezte az adatkezelést a határigazgatás, a biztonság és a migráció terén, amelynek értelmében a biztonság, a határigazgatás és a migrációkezelés terén használt valamennyi uniós információs rendszer interoperabilis módon, az alapvető jogok maradéktalan tiszteletben tartásával működik.

<sup>(1)</sup> HL C 283., 2018.8.10., 48. o.

<sup>(2)</sup> Az Európai Parlament 2019. április 16-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2019. május 14-i határozata.

<sup>(3)</sup> HL C 101., 2018.3.16., 116. o.

- (7) Az információcsere javítását és az uniós információs rendszerek interoperabilitásának biztosítását célzó további lépésekről szóló, 2017. június 9-i következtetéseiben a Tanács felkérte a Bizottságot, hogy valósítsa meg a magas szintű szakértői csoport által az interoperabilitás biztosítása érdekében javasolt megoldásokat.
- (8) Az Európai Tanács 2017. június 23-i következtetéseiben hangsúlyozta az adatbázisok közötti interoperabilitás javításának szükségességét, és felkérte a Bizottságot, hogy a lehető legrövidebb időn belül dolgozzon ki jogszabálytervezeteket az információs rendszerekkel és az interoperabilitással foglalkozó magas szintű szakértői csoport javaslatai alapján.
- (9) A külső határokon végzett határellenőrzések hatékonyságának és eredményességének javítása, az illegális bevándorlás megelőzéséhez és az ellene vívott küzdelemhez való hozzájárulás, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló uniós térség magas szintű biztonságának elősegítése – beleértve a közbiztonság és a közrend fenntartását, valamint a tagállamok területén a biztonság védelmét –, a közös vízümpolitika végrehajtásának javítása, a nemzetközi védelem iránti kérelmek vizsgálatának elősegítése, a terrorista bűncselekmények és egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez és nyomozásához való hozzájárulás, a személyazonosságukat igazolni nem tudó ismeretlen személyek vagy a természeti katasztrófák, balesetek vagy terrortámadások esetében az azonosítatlan emberi maradványok azonosításának elősegítése céljából, az uniós migrációs és menekültügyi rendszerbe, az uniós biztonsági intézkedésekbe és az Unió külső határainak igazgatására vonatkozó képességébe vetett közbizalom fenntartása érdekében meg kell valósítani az uniós információs rendszerek, azaz a határregisztrációs rendszer („Entry/Exit System”, a továbbiakban: EES), a Vízuminformációs Rendszer („Visa Information System”, a továbbiakban: VIS), az Európai Utasinformációs és Engedélyezési Rendszer („European Travel Information and Authorisation System”, a továbbiakban: ETIAS), az Eurodac, a Schengeni Információs Rendszer („Schengen Information System”, a továbbiakban: SIS), valamint a harmadik országok állampolgáira vonatkozó Európai Bűnügyi Nyilvántartási Információs Rendszer („European Criminal Records Information System for Third-Country Nationals”, a továbbiakban: ECRIS-TCN) interoperabilitását, hogy ezek az uniós információs rendszerek és az azokban található adatok kiegészítsék egymást, tiszteletben tartva ugyanakkor az egyének alapvető jogait és különösen a személyes adatok védelméhez való jogot. Ehhez létre kell hozni – interoperabilitási elemekként – az európai keresőportált („European search portal”, a továbbiakban: ESP), a közös biometrikus megfeleltetési szolgáltatást („shared biometric matching service”, a továbbiakban: közös BMS), a közös személyazonosítótárat („common identity repository”, a továbbiakban: CIR) és a többszörös személyazonosságot felismerő rendszert („multiple-identity detector”, a továbbiakban: MID).
- (10) Az uniós információs rendszerek közötti interoperabilitásnak lehetővé kell tennie, hogy az említett rendszerek kiegészítsék egymást, a személyek – köztük a személyazonosságukat igazolni nem tudó ismeretlen személyek vagy az azonosítatlan emberi maradványok – helyes azonosításának megkönnyítése, a személyazonossággal való visszaélés elleni küzdelemhez való hozzájárulás, az egyes uniós információs rendszerekre vonatkozó adatminőségi követelmények javítása és harmonizálása, az uniós információs rendszerek tagállamok általi műszaki és operatív alkalmazásának megkönnyítése, a vonatkozó uniós információs rendszereket szabályozó adatbiztonsági és adatvédelmi biztosítékok megerősítése, az EES-hez, a VIS-hez, az ETIAS-hoz és az Eurodachoz terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése és nyomozása céljából történő hozzáférés egyszerűsítése, valamint az EES, a VIS, az ETIAS, az Eurodac, a SIS és az ECRIS-TCN célkitűzéseinek támogatása érdekében.
- (11) Az interoperabilitási elemeknek az EES-t, a VIS-t, az ETIAS-t, az Eurodacot, a SIS-t és az ECRIS-TCN-t kell lefedniük. Emellett az Europol-adatokat is le kell fedniük, de csak olyan mértékben, hogy az Europol-adatok az említett uniós információs rendszerekkel egyidejűleg lekérdeezhetőek legyenek.
- (12) Az interoperabilitási elemeknek olyan személyes adatait kell kezelniük, akiknek személyes adatait az alapul szolgáló uniós információs rendszerekben kezelik, vagy az Europol kezeli.
- (13) Az ESP-t annak elősegítése érdekében kell létrehozni, hogy a tagállami hatóságok és az uniós ügynökségek gyors, zökkenőmentes, hatékony, szisztematikus és ellenőrzött módon hozzáférjenek az uniós információs rendszerekhez, az Europol-adatokhoz és a Nemzetközi Bűnügyi Rendőrség Szervezete (Interpol) adatbázisaihoz, amennyiben ez feladataik hozzáférési jogosultságaikkal összhangban történő ellátásához szükséges. Az ESP-t továbbá annak érdekében is létre kell hozni, hogy támogassa az EES, a VIS, az ETIAS, az Eurodac, a SIS, az ECRIS-TCN és az Europol-adatok célkitűzéseit. Az ESP rendeltetése, hogy valamennyi megfelelő uniós információs rendszer, valamint az Europol-adatok és az Interpol-adatbázisok egyidejű lekérdezésének lehetővé tétele révén egyedüli lekérdezési pontként vagy „üzenetközvetítőként” szolgáljon a különböző központi rendszerek kereséséhez és a szükséges információk zökkenőmentes lehívásához, az alapul szolgáló rendszerek hozzáférési és adatvédelmi követelményeinek teljes körű tiszteletben tartása mellett.
- (14) Az ESP kialakításának biztosítania kell, hogy az Interpol-adatbázisok lekérdezésekor az ESP-felhasználó által a lekérdezés kezdeményezéséhez használt adatok ne kerüljenek megosztásra az Interpol adatainak tulajdonosaival. Az ESP kialakításának azt is biztosítania kell, hogy az Interpol adatbázisainak lekérdezésére kizárólag az alkalmazandó uniós és nemzeti joggal összhangban kerülhessen sor.



- (15) Azon ESP-felhasználóknak, akik az (EU) 2016/794 európai parlamenti és tanácsi rendelet <sup>(4)</sup> szerint hozzáféréssel rendelkeznek az Europol-adatokhoz, képeseknek kell lenniük az Europol-adatoknak azokkal az uniós információs rendszerekkel történő egyidejű lekérdezésére, amelyekhez hozzáférésük van. Az ilyen lekérdezéseket követő minden további adatkezelésnek az (EU) 2016/794 rendelettel összhangban kell történnie, az adatszolgáltató által előírt hozzáférési vagy felhasználási korlátozásokat is ideértve.
- (16) Az ESP-t úgy kell kialakítani és konfigurálni, hogy az effajta lekérdezéseket csak a személyekkel vagy úti okmányokkal kapcsolatos azon adatok felhasználásával tegye lehetővé, amelyek szerepelnek valamelyik uniós információs rendszerben, az Europol-adatokban vagy az Interpol-adatbázisokban.
- (17) A megfelelő uniós információs rendszerek szisztematikus használatának biztosítása érdekében az ESP-t kell használni a CIR, az EES, a VIS, az ETIAS, az Eurodac és az ECRIS-TCN lekérdezésére. Továbbra is fenn kell tartani azonban a különböző uniós információs rendszerekhez való nemzeti kapcsolódást tartalékmegoldásként technikai problémák esetére. Az ESP-t az uniós ügynökségeknek is használniuk kell a központi SIS-nek a hozzáférési jogosultságaikkal összhangban és feladataik ellátása érdekében történő lekérdezése céljából. Az ESP további eszközt jelent a központi SIS, az Europol-adatok és az Interpol-adatbázisok lekérdezéséhez, kiegészítve a meglévő célzott interfészeket.
- (18) A biometrikus adatok – például az ujjnyomatok és arcképmások – egyediek, ezért a személyek azonosítása céljából sokkal megbízhatóbbak, mint az alfanumerikus adatok. A közös BMS a megfelelő uniós információs rendszerek és az egyéb interoperabilitási elemek munkájának támogatását és megkönnyítését szolgáló technikai eszköz kell, hogy legyen. A közös BMS fő célja, hogy megkönnyítse a több adatbázisban nyilvántartott személyek azonosítását azáltal, hogy a számos összetevő helyett egyetlen technológiai összetevőt használ az adott személy különböző rendszerekben tárolt biometrikus adatainak összevetéséhez. A közös BMS növeli a biztonságot, valamint pénzügyi, fenntartási és működési előnyökkel jár. Valamennyi automatikus ujjnyomat-azonosító rendszer, beleértve az Eurodachoz, a VIS-hez és a SIS-hez jelenleg használt rendszereket is, valódi biometrikus minták jellemzőinek leképezése útján nyert adatokból összeállított biometrikus sablonokat használ. A közös BMS egyetlen helyszínen gyűjti össze és tárolja az összes ilyen biometrikus sablont – logikailag különválasztva azon információs rendszerek szerint, amelyekből az adatok származnak –, ezáltal megkönnyíti a biometrikus sablonokat használó rendszerek közötti összehasonlításokat, és lehetővé teszi az EU központi rendszereinek méretgazdaságos fejlesztését és fenntartását.
- (19) A közös BMS-ben tárolt biometrikus sablonok a valódi biometrikus minták jellemzőinek leképezése útján nyert adatokból kell, hogy álljanak és azokat úgy kell létrehozni, hogy a kinyerési eljárást fordított irányba ne lehessen végrehajtani. A biometrikus sablonokat biometrikus adatokból kell létrehozni, de oly módon, hogy ugyanazokat a biometrikus adatokat ne lehessen kinyerni a biometrikus sablonokból. Mivel tenyérnyomatokra vonatkozó adatokat és DNS-profilokat kizárólag a SIS-ben tárolnak, és azok nem használhatók más információs rendszerekben lévő adatokkal való összehasonlításra, a szükségesség és az arányosság elvével összhangban a közös BMS nem tárolhat DNS-profilokat vagy tenyérnyomatokra vonatkozó adatokból létrehozott biometrikus sablonokat.
- (20) A biometrikus adatok különleges személyes adatnak minősülnek. E rendeletben meg kell határozni az ilyen adatok – kizárólag az érintett személyek azonosítása céljából megengedett – kezelésének jogalapját és az arra vonatkozó biztosítékokat.
- (21) Az EES, a VIS, az ETIAS, az Eurodac és az ECRIS-TCN megkívánja azon személyek pontos azonosítását, akiknek személyes adatait e rendszerekben tárolják. A CIR-nek ezért elő kell segítenie az említett rendszerekben nyilvántartott személyek pontos azonosítását.
- (22) Az említett uniós információs rendszerekben tárolt személyes adatok vonatkozhatnak ugyanazokra a személyekre, de eltérő vagy hiányos személyazonosság alapján. A tagállamok hatékony módszerekkel rendelkeznek az állampolgáraik vagy a területükön állandó lakóhellyel rendelkező személyek azonosítására. Az uniós információs rendszerek közötti interoperabilitás hozzájárul az említett rendszerekben szereplő személyek pontosabb azonosításához. A CIR-nek tárolnia kell azon személyes adatokat, amelyek szükségesek azon személyek pontosabb azonosításának lehetővé tételéhez, akiknek adatait e rendszerek tárolják, többek között személyazonosító adataikat, útiokmány-adataikat és biometrikus adataikat, függetlenül attól, hogy az adatokat mely rendszerbe gyűjtötték be. A CIR-ben csak azokat a személyes adatokat lehet tárolni, amelyek a pontos személyazonosság-ellenőrzések végzéséhez elengedhetetlenül szükségesek. A CIR-ben rögzített személyes adatokat csak az alapul szolgáló rendszerek céljaihoz feltétlenül szükséges ideig lehet megőrizni, és azokat automatikusan törölni kell, ha az adatokat logikai elkülönítésüknek megfelelően törlik az alapul szolgáló rendszerekből.

<sup>(4)</sup> Az Európai Parlament és a Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Uniói Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről (HL L 135., 2016.5.24., 53. o.).

- (23) Az új kezelési művelet, amely ezen adatoknak a CIR-ben történő tárolásából áll az egyes különálló rendszerekben történő tárolás helyett, azért szükséges, hogy növelni lehessen az azonosítás pontosságát az ilyen adatok automatizált összehasonlítása és megfeleltetése révén. Az a tény, hogy a CIR tárolja a személyazonosító adatokat, az útiokmány-adatokat és a biometrikus adatokat, nem akadályozhatja az adatoknak az EES, a VIS, az ETIAS, az Eurodac vagy az ECRIS-TCN céljából történő kezelését, tekintve, hogy a CIR az említett alapul szolgáló rendszerek új közös eleme.
- (24) A CIR-ben ezért egyéni aktát kell létrehozni az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban vagy az ECRIS-TCN-ben nyilvántartott minden egyes személyre vonatkozóan annak érdekében, hogy megvalósítható legyen a schengeni térségben történő helyes személyazonosításra irányuló célkitűzés, valamint a MID támogatása érdekében, amelynek kettős célja a jóhiszemű utazók személyazonosságának ellenőrzésének megkönnyítése és a személyazonossággal való visszaélés elleni küzdelem. Az egyéni akta az adott személyhez kapcsolható összes lehetséges személyazonosító információt egyetlen helyen kell, hogy tárolja és hozzáférhetővé kell, hogy tegye a megfelelő felhatalmazással rendelkező végfelhasználók számára.
- (25) A CIR-nek ezáltal meg kell könnyítenie és egyszerűsíteni kell a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséért, felderítéséért és nyomozásáért felelős hatóságok hozzáférését az olyan uniós információs rendszerekhez, amelyeket nem kizárólag súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából hoztak létre.
- (26) A CIR az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban és az ECRIS-TCN-ben nyilvántartott személyek személyazonosító adatait, útiokmány-adatait és biometrikus adatait tartalmazó közös adattárként kell, hogy szolgáljon. A CIR-nek e rendszerek műszaki felépítésének részét kell képeznie, és az azok közötti közös elemként az említett rendszerek által kezelt személyazonosító adatok, útiokmány-adatok és biometrikus adatok tárolására és lekérdezésére kell szolgálnia.
- (27) A CIR-ben szereplő bejegyzéseket logikailag el kell különíteni egymástól azáltal, hogy mindegyik esetében automatikusan feltüntetésre kerül, hogy név szerint melyik rendszerhez tartozik. A CIR hozzáférés-ellenőrzésének ezeket a címkéket kell használnia a bejegyzéshez való hozzáférés engedélyezése vagy megtagadása céljából.
- (28) Amennyiben egy tagállami rendőri hatóság úti okmány vagy az adott személy személyazonosságát hitelt érdemlően igazoló más dokumentum hiányában nem tud azonosítani egy személyt, vagy amennyiben kétség merül fel az adott személy által rendelkezésre bocsátott személyazonosító adatokat, illetve az úti okmány hitelességét vagy birtokosának személyazonosságát illetően, vagy ha a személy nem képes az együttműködésre vagy megtagadja azt, a rendőri hatóságnak jogosultsággal kell rendelkeznie arra, hogy a szóban forgó személy azonosítása céljából lekérdezést végeztesse a CIR-ben. E célból a rendőri hatóságoknak nyomatvételi munkaálomások (live-scan) alkalmazásával ujjnyomatokat kell venniük, feltéve, hogy az eljárást az adott személy jelenlétében indították meg. A CIR ilyen lekérdezése 12 év alatti kiskorúak személyazonosságának megállapítása céljából nem megengedett, kivéve, ha ezt a gyermek mindenek felett álló érdeke megkívánja.
- (29) Amennyiben a személy biometrikus adatai nem használhatók, vagy ha az ilyen adatokkal történő lekérdezés sikertelen, a lekérdezést a személy személyazonosító adataival és útiokmány-adataival együttesen kell elvégezni. Amennyiben a lekérdezés nyomán kiderül, hogy a CIR tartalmaz az adott személyre vonatkozó adatokat, a tagállami hatóságok számára hozzáférést kell biztosítani a CIR-hez az érintett személy személyazonosító adataiba és útiokmány-adataiba való betekintés céljából anélkül, hogy a CIR megjelölne, hogy ezek az adatok melyik uniós információs rendszerben található.
- (30) A tagállamoknak nemzeti jogalkotási intézkedéseket kell elfogadniuk, amelyekben kijelölik azokat a nemzeti hatóságokat, amelyek hatáskörrel rendelkeznek arra, hogy a CIR használatával személyazonosság-ellenőrzést végezzenek, valamint – az arányosság elvével összhangban – meghatározzák az ilyen ellenőrzések végzésére vonatkozó eljárásokat, azok feltételeit és kritériumait. Nemzeti jogszabálynak kell rendelkeznie különösen az említett hatóságok személyi állományának tagja előtt megjelent személyek személyazonosságának ellenőrzése során a biometrikus adatok gyűjtésére vonatkozó hatáskörrel.
- (31) E rendelet ezen túlmenően új lehetőséget kell, hogy bevezessen a tagállamok terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséért, felderítéséért és nyomozásáért felelős kijelölt hatóságai és az Europol számára az EES-ben, a VIS-ben, az ETIAS-ban vagy az Eurodacban található, a személyazonosító adatokon vagy útiokmány-adatokon felüli adatokhoz való egyszerűbb hozzáférésre is. Ezen adatok szükségesek lehetnek a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez vagy nyomozásához, ha alapos okkal feltételezhető, hogy az azokba való betekintés jelentősen hozzájárul a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez vagy nyomozásához, különösen, ha fennáll annak a gyanúja, hogy a terrorista bűncselekmény vagy egyéb súlyos bűncselekmény elkövetésével gyanúsított személy, az ilyen bűncselekmények elkövetője vagy áldozata olyan személy, akinek adatait az EES-ben, a VIS-ben, az ETIAS-ban vagy az Eurodacban tárolják.

- (32) Az uniós információs rendszerekben található adatokhoz a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása érdekében szükséges teljes körű hozzáférést – a CIR-ben található személyazonosító vagy útiokmány-adatoktól eltérő adatokhoz való hozzáféréseken felül – továbbra is az alkalmazandó jogi eszközök szabályozzák. A terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséért, felderítéséért és nyomozásáért felelős kijelölt hatóságok és az Europol nem tudják előre, hogy az uniós információs rendszerek közül melyik tartalmazza az általuk vizsgálandó személyek adatait. Ez gyakran késedelmet és hatékonysági problémákat eredményez. A kijelölt hatóság által felhatalmazott végfelhasználó számára ezért lehetővé kell tenni annak megismerését, hogy az említettek közül melyik uniós információs rendszer rögzíti a lekérdezés eredményének megfelelő adatokat. Ennek megfelelően a rendszerben talált egyezés automatizált ellenőrzését követően az érintett rendszer megjelölésre kerülne (úgynevezett „egyezés-megjelölés” funkció).
- (33) Ebben az összefüggésben a CIR-től kapott válasz nem értelmezhető vagy nem használható alapként vagy indokként következtetések levonásához vagy intézkedések megtételéhez valamely személy tekintetében, hanem csak az alapul szolgáló uniós információs rendszerekhez való hozzáférési kérelem benyújtására használható, az e hozzáférést szabályozó, megfelelő jogi eszközben megállapított feltételeknek és eljárásoknak megfelelően. Minden ilyen hozzáférés e rendelet VII. fejezetének hatálya alá, és esettől függően az (EU) 2016/679 európai parlamenti és tanácsi rendelet <sup>(5)</sup>, az (EU) 2016/680 európai parlamenti és tanács irányelv <sup>(6)</sup> vagy az (EU) 2018/1725 európai parlamenti és tanács rendelet <sup>(7)</sup> hatálya alá tartozik.
- (34) Általános szabályként, amennyiben az egyezés-megjelölés azt jelzi, hogy az adatok szerepelnek az Eurodacban, a kijelölt hatóságoknak vagy az Europolnak teljes körű hozzáférést kell kérnie legalább az egyik érintett uniós információs rendszerhez. Amennyiben a teljes körű hozzáférést kivételesen nem kérik, például azért, mert a kijelölt hatóságok vagy az Europol más módon már megszerezték az adatokat, vagy az adatok megszerzését a nemzeti jog már nem teszi lehetővé, a hozzáférés iránti kérelem elmulasztásának indokolását rögzíteni kell.
- (35) A CIR-ben végzett lekérdezések naplóiban jelezni kell a lekérdezések célját. Amennyiben az ilyen lekérdezés végzése a kétlépcsős adatbetekintési megközelítés alkalmazásával történt, a naplóknak tartalmazniuk kell a nyomozás vagy az ügy nemzeti aktájára való hivatkozást, ami azt jelzi, hogy a lekérdezést terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából kezdeményezték.
- (36) A CIR-nek a kijelölt hatóságok és az Europol általi, egyezés-megjelölés típusú válasz megszerzése céljából történő lekérdezése – amely válasz arra utal, hogy az adat szerepel az EES-ben, a VIS-ben, az ETIAS-ban vagy az Eurodacban – a személyes adatok automatizált kezelését teszi szükségessé. Az egyezés-megjelölés nem fedheti fel az érintett személy személyes adatait, csak arra utalhat, hogy bizonyos adatait tárolja valamelyik rendszer. A felhatalmazással rendelkező végfelhasználó pusztán az egyezés-megjelölés előfordulása alapján nem hozhat elmarasztaló határozatot az érintett személyre vonatkozóan. A végfelhasználó hozzáférése az egyezés-megjelöléshez ezért nagyon korlátozott mértékű beavatkozást valósít meg az érintett személy személyes adatainak védelméhez való jogába, míg a kijelölt hatóságok és az Europol számára lehetővé teszi, hogy hatékonyabban kérelmezhesék a személyes adatokhoz való hozzáférést.
- (37) A MID létrehozása a CIR működésének támogatása, valamint az EES, a VIS, az ETIAS, az Eurodac, a SIS és az ECRIS-TCN célkitűzéseinek támogatása érdekében szükséges. Annak érdekében, hogy hatékonyan teljesítsék célkitűzéseiket, az összes említett uniós információs rendszer szükségessé teszi azon személyek pontos azonosítását, akiknek személyes adatait azokban tárolják.
- (38) Az uniós információs rendszerek céljainak jobb megvalósítása érdekében az e rendszereket használó hatóságoknak képeseknek kell lenniük arra, hogy kellően megbízhatóan tudják ellenőrizni azon személyek személyazonosságát, akiknek adatait különböző rendszerekben tárolják. Egy adott önálló rendszerben tárolt

<sup>(5)</sup> Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

<sup>(6)</sup> Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (HL L 119., 2016.5.4., 89. o.).

<sup>(7)</sup> Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o.).

személyazonosító adatok vagy útiokmány-adatok helytelenek, hiányosak vagy csalárdak lehetnek, és jelenleg nincs mód arra, hogy észleljék a helytelen, hiányos vagy csalárd személyazonosító adatokat vagy útiokmány-adatokat a más rendszerben tárolt adatokkal történő összehasonlítás révén. E helyzet orvoslása érdekében egy olyan uniós szintű technikai eszközt kell létrehozni, amely lehetővé teszi a személyek e célokból történő pontos azonosítását.

- (39) A MID-nek a különböző uniós információs rendszerekben található adatok között kapcsolatokat kell létrehoznia és tárolnia a többszörös személyazonosságok észlelése érdekében, a jóhiszemű utazók személyazonosság-ellenőrzésének megkönnyítése és a személyazonossággal való visszaélés elleni küzdelem kettős célját követve. A MID csak olyan személyekre vonatkozó adatok közötti kapcsolatokat tartalmazhat, amelyek egynél több uniós információs rendszerben szerepelnek. Az összekapcsolt adatok körét szigorúan azokra az adatokra kell korlátozni, amelyek annak ellenőrzéséhez szükségesek, hogy egy adott személy indokoltan vagy indokolatlanul szerepel-e különböző személyazonosságokkal a különböző rendszerekben, vagy annak tisztázásához szükségesek, hogy két, hasonló személyazonosító adatokkal rendelkező személy esetében nem lehet szó ugyanarról a személyről. Az egyéni aktáknak a különböző rendszerek közötti összekapcsolása céljából az ESP-n és a közös BMS-en keresztül történő adatkezelést a lehető legkisebb mértékűre kell szorítani, ezért annak a többszörös személyazonosságot használók észlelésére kell korlátozódnia, amit abban a pillanatban kell elvégezni, amikor a CIR-ben tárolt adatokkal rendelkező valamelyik rendszerhez, vagy a SIS-hez új adatot adnak hozzá. A MID-nek biztosítékokat kell magában foglalnia az olyan személyekkel szembeni esetleges hátrányos megkülönböztetéssel és kedvezőtlen döntéshozattal szemben, akik jogszerűen rendelkeznek több személyazonossággal.
- (40) Ez a rendelet új adatkezelési műveleteket ír elő az érintett személyek pontos azonosítása céljából. Ez az Európai Unió Alapjogi Chartájának 7. és 8. cikke által védett alapvető jogaikba való beavatkozásnak minősül. Mivel az uniós információs rendszerek hatékony alkalmazása az érintett személyek helyes azonosításától függ, az ilyen beavatkozást ugyanazok a célkitűzések indokolják, mint amelyek érdekében az egyes rendszereket létrehozták: az Unió határainak hatékony igazgatása, az Unió belső biztonsága és az uniós menekültügyi és vízumpolitika hatékony végrehajtása.
- (41) Az ESP-nek és a közös BMS-nek össze kell hasonlítania a CIR és a SIS személyekre vonatkozó adatait, amikor valamelyik nemzeti hatóság vagy uniós ügynökség új bejegyzést hoz létre vagy tölt fel. Az ilyen összehasonlítást automatizált módon kell végezni. A CIR és a SIS a közös BMS-t arra kell, hogy használja, hogy a biometrikus adatok alapján észlelje az esetleges kapcsolatokat. A CIR és a SIS az ESP-t arra kell, hogy használja, hogy az alfanumerikus adatok alapján észlelje az esetleges kapcsolatokat. A CIR-nek és a SIS-nek képesnek kell lennie az egyes személyekre vonatkozóan különböző rendszerekben tárolt azonos vagy hasonló adatok azonosítására. Amennyiben ilyen eset áll fenn, létre kell hozni egy kapcsolatot, amely jelzi, hogy ugyanarról a személyről van szó. A CIR-t és a SIS-t úgy kell konfigurálni, hogy észleljék a kisebb átírási vagy helyesírási hibákat annak érdekében, hogy ezek ne okozzanak indokolatlan akadályokat az érintett személy számára.
- (42) A nemzeti hatóságnak vagy uniós ügynökségnek, amely rögzítette az adatokat a megfelelő uniós információs rendszerben, meg kell erősítenie vagy módosítania kell ezeket a kapcsolatokat. Ennek a nemzeti hatóságnak vagy uniós ügynökségnek hozzáféréssel kell rendelkeznie a CIR-ben vagy a SIS-ben és a MID-ben tárolt adatokhoz a különböző személyazonosságok manuális ellenőrzése céljából.
- (43) A különböző személyazonosságok manuális ellenőrzését annak a hatóságnak kell biztosítania, amely létrehozta vagy aktualizálta azokat az adatokat, amelyek más uniós információs rendszerben tárolt adatokkal kapcsolatot létrehozva egyezést eredményeztek. A különböző személyazonosságok manuális ellenőrzéséért felelős hatóságnak azt kell értékelnie, hogy indokoltan vagy indokolatlanul áll-e fenn az ugyanarra a személyre vonatkozó többszörös személyazonosság. Ezt az értékelést lehetőség szerint az érintett személy jelenlétében kell elvégezni, és szükség esetén további pontosítást vagy információt kell kérni tőle. Az ilyen értékelést haladéktalanul el kell végezni, az információk pontosságára vonatkozó uniós jogi és nemzeti jogi követelményekkel összhangban.
- (44) A SIS-el kapcsolatban az átadási vagy kiadási letartóztatás céljából körözött személyekre, eltűnt vagy különleges bánásmódot igénylő személyekre, a bírósági eljárásban való közreműködés céljából keresett személyekre vagy rejtett ellenőrzés, kikérdezés vagy célzott ellenőrzés miatt keresett személyekre vonatkozó figyelmeztető jelzésekhez kötődő kapcsolatok tekintetében a különböző személyazonosságok manuális ellenőrzéséért felelős hatóságnak a figyelmeztető jelzést létrehozó tagállam SIRENE-irodájának kell lennie. A SIS figyelmeztető jelzések

e kategóriái érzékenyek, ezért azokat nem feltétlenül kell megosztani a más uniós információs rendszerekben ezen adatokkal összekapcsolt adatokat létrehozó vagy frissítő hatóságokkal. A SIS-adatokkal való kapcsolat létrehozása nem sértheti az (EU) 2018/1860<sup>(8)</sup>, az (EU) 2018/1861<sup>(9)</sup> és az (EU) 2018/1862<sup>(10)</sup> európai parlamenti és tanácsi rendeletnek megfelelően meghozandó intézkedéseket.

- (45) E kapcsolatok létrehozása az érintett személyek irányába átláthatóságot követel meg. Az alkalmazandó uniós adatvédelmi szabályoknak megfelelő szükséges biztosítékok végrehajtásának megkönnyítése érdekében azon személyeket, akik a különböző személyazonosságok manuális ellenőrzését követően vörös vagy fehér kapcsolattal rendelkeznek, írásban kell tájékoztatni a biztonság és közrend védelme, a bűncselekmények megelőzése és a nemzeti nyomozások veszélyeztetésének megakadályozása érdekében szükséges korlátozások sérelme nélkül. Az ilyen személyek kapnak egy egységes azonosító számot, amely lehetővé teszi számukra azon hatóság azonosítását, amelyhez jogaik gyakorlása érdekében fordulniuk kell.
- (46) Sárga kapcsolat létrehozása esetén a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság számára hozzáférést kell biztosítani a MID-hez. Vörös kapcsolat fennállása esetén azon tagállami hatóságok és uniós ügynökségek számára is hozzáférést kell biztosítani a MID-hez, amelyek hozzáféréssel rendelkeznek a CIR-ben szereplő legalább egy uniós információs rendszerhez vagy a SIS-hez. A vörös kapcsolat azt kell, hogy jelezze, hogy az adott személy indokolatlan módon használ különböző személyazonosságokat, vagy hogy valaki más személyazonosságát használja.
- (47) A tagállami hatóságok és az uniós ügynökségek akkor is hozzáférhetnek a MID-hez, ha két uniós információs rendszer adatai között fehér vagy zöld kapcsolat áll fenn, amennyiben az ilyen hatóság vagy ügynökség mindkét információs rendszerhez hozzáfér. Az ilyen hozzáférést kizárólag azzal a céllal kell biztosítani, hogy a hatóság vagy ügynökség észlelje azokat a lehetséges eseteket, amikor az adatokat helytelenül kapcsolták össze, vagy hogy az adatokat a MID-ben, a CIR-ben és a SIS-ben e rendeletet megsértve kezelték, és megtegye a helyzet javításához szükséges intézkedéseket, és frissítse vagy törölje a kapcsolatot.
- (48) A szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai uniós ügynökségnek (eu-LISA) az adatminőség ellenőrzésére irányuló, automatizált mechanizmusokat és az adatminőségre vonatkozó közös mutatókat kell létrehoznia. Az eu-LISA felelősségi körébe kell, hogy tartozzon egy központi adatminőség-ellenőrzési kapacitás kiépítése, valamint rendszeres adatelemzési jelentések készítése az uniós információs rendszerek tagállamok általi végrehajtásának javítása érdekében. A közös adatminőségi mutatóknak tartalmazniuk kell az uniós információs rendszerekben vagy az interoperabilitási elemekben szereplő adatok tárolására vonatkozó minőségi minimumkövetelményeket. Az ilyen adatminőségi követelmények célja az uniós információs rendszerekbe és az interoperabilitási elemekbe történő láthatóan helytelen vagy következtelen adatbevitel automatikus azonosítása annak érdekében, hogy az adatbevitelt végző tagállam képes legyen ellenőrizni az adatokat, és szükség esetén korrekciós intézkedéseket alkalmazni.
- (49) A Bizottságnak értékelnie kell az eu-LISA minőségi jelentéseit, és szükség esetén ajánlásokat kell intéznie a tagállamokhoz. A tagállamok feladata kell, hogy legyen egy olyan cselekvési terv elkészítése, amely ismerteti az adatok minőségével kapcsolatos hiányosságok orvoslását célzó intézkedéseket, valamint a tagállamoknak rendszeresen be kell számolniuk az elért eredményekről.
- (50) Az egységes üzenetformátum (UMF) a bel- és igazságügy területén működő információs rendszerek, hatóságok vagy szervezetek közötti strukturált, határokon átnyúló információcserére vonatkozó normaként kell, hogy szolgáljon. Az UMF-nek közös kifejezéseket és logikai struktúrákat kell meghatároznia a kölcsönös információcserére körében szereplő adatok vonatkozásában az interoperabilitás megkönnyítése céljából, a cserélt tartalmak következetes és szemantikailag egyenértékű módon történő létrehozásának és olvasásának lehetővé tétele által.
- (51) Megfontolás tárgyát képezheti az UMF szabvány alkalmazása a VIS-ben, a SIS-ben, valamint a bel- és igazságügy területén működő, bármely meglévő vagy új, a tagállamok által kidolgozott információcsere-modell és információs rendszer esetében.

<sup>(8)</sup> Az Európai Parlament és a Tanács (EU) 2018/1860 rendelete (2018. november 28.) a Schengeni Információs Rendszernek a jogellenesen tartózkodó harmadik országbeli állampolgárok visszaküldése céljából történő használatáról (HL L 312., 2018.12.7., 1. o.).

<sup>(9)</sup> Az Európai Parlament és a Tanács (EU) 2018/1861 rendelete (2018. november 28.) a határforgalom-ellenőrzés terén a Schengeni Információs Rendszer (SIS) létrehozásáról, működéséről és használatáról, a Schengeni Megállapodás végrehajtásáról szóló egyezmény módosításáról, valamint az 1987/2006/EK rendelet módosításáról és hatályon kívül helyezéséről (HL L 312., 2018.12.7., 14. o.).

<sup>(10)</sup> Az Európai Parlament és a Tanács (EU) 2018/1862 rendelete (2018. november 28.) a rendőrségi együttműködés és a büntetőügyekben folytatott igazságügyi együttműködés terén a Schengeni Információs Rendszer (SIS) létrehozásáról, működéséről és használatáról, a 2007/533/IB tanácsi határozat módosításáról és hatályon kívül helyezéséről, valamint az 1986/2006/EK európai parlamenti és tanácsi rendelet és a 2010/261/EU bizottsági határozat hatályon kívül helyezéséről (HL L 312., 2018.12.7., 56. o.).

- (52) Létre kell hozni a jelentések és statisztikák központi adattárát (CRRS), amely rendszerek közötti statisztikai adatokat és elemzési jelentéseket készít szakpolitikai, működési és adatminőségi célokból, a vonatkozó jogi eszközöknek megfelelően. Az eu-LISA-nak kell létrehoznia, bevezetnie és technikai helyszínein üzemeltetnie a CRRS-t. A CRRS az uniós információs rendszerekből, a CIR-ből, a MID-ből és a közös BMS-ből származó anonimizált statisztikai adatokat tartalmaz. A CRRS-ben szereplő adatok nem tehetik lehetővé az egyének azonosítását. Az eu-LISA-nak automatikusan anonimizálnia kell az adatokat, és csak ilyen anonimizált adatokat rögzíthet a CRRS-ben. Az adatok anonimizálásának folyamatát automatizálni kell, és az eu-LISA személyi állománya nem kaphat közvetlen hozzáférést az uniós információs rendszerekben vagy az interoperabilitási elemekben tárolt személyes adatokhoz.
- (53) A személyes adatoknak a nemzeti hatóságok által az e rendelet szerinti interoperabilitási célból történő kezelésére az (EU) 2016/679 rendelet alkalmazandó, kivéve, ha az adatkezelést a tagállamok kijelölt hatóságai vagy központi hozzáférési pontjai terrorcselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából végzik.
- (54) Ha a személyes adatok tagállami szintű, e rendelet szerinti interoperabilitási célból történő kezelését az illetékes hatóságok terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából végzik, az (EU) 2016/680 irányelv alkalmazandó.
- (55) Az (EU) 2016/679 rendelet, az (EU) 2018/1725 rendelet vagy adott esetben az (EU) 2016/680 irányelv alkalmazandó a személyes adatok harmadik országok vagy nemzetközi szervezetek számára e rendelet szerinti továbbítására is. Az (EU) 2016/679 rendelet V. fejezete vagy adott esetben az (EU) 2016/680 irányelv V. fejezete szerinti adattovábbítási indokok sérelme nélkül, valamely harmadik ország bíróságának azon ítéletét, valamint valamely harmadik ország közigazgatási hatóságának azon határozatát, amely személyes adatok továbbítását vagy közzétételét írja elő egy adatkezelő vagy adatfeldolgozó számára, kizárólag akkor kell elismerni vagy bármilyen módon végrehajtani, ha a kérelmező harmadik ország és az Unió vagy valamely tagállam között nemzetközi megállapodás van hatályban.
- (56) A személyes adatoknak az (EU) 2018/1862 rendelet és az (EU) 2019/816 európai parlamenti és tanácsi rendelet<sup>(1)</sup> által szabályozott rendszerekben történő kezelésére az említett rendeletek adatvédelemre vonatkozó különös rendelkezései alkalmazandók.
- (57) A személyes adatoknak az eu-LISA és az Unió más intézményei és szervei által feladataik ellátása során történő, e rendelet szerinti kezelésére az (EU) 2018/1725 rendelet alkalmazandó, az (EU) 2016/794 rendelet sérelme nélkül, amely a személyes adatok Europol általi kezelésére alkalmazandó.
- (58) A személyes adatok tagállamok általi kezelésének jogszerűségét az (EU) 2016/679 rendeletben vagy az (EU) 2016/680 irányelvben említett felügyeleti hatóságoknak kell felügyelniük. Az európai adatvédelmi biztosnak felügyelnie kell az uniós intézményeknek és szervezeteknek a személyes adatok kezeléséhez kapcsolódó tevékenységét. Az európai adatvédelmi biztosnak és a felügyeleti hatóságoknak együtt kell működniük egymással a személyes adatok interoperabilitási elemek által történő kezelésének nyomon követése során. Ahhoz, hogy az európai adatvédelmi biztos elláthassa az e rendelet alapján ráruházott feladatokat, megfelelő forrásokra, többek között emberi és pénzügyi forrásokra van szükség.
- (59) Az európai adatvédelmi biztossal a 45/2001/EK európai parlamenti és tanácsi rendelet<sup>(2)</sup> 28. cikkének (2) bekezdésével összhangban konzultációt folytattak, és a biztos 2018. április 16-án véleményt nyilvánított<sup>(3)</sup>.
- (60) A 29. cikk szerinti adatvédelmi munkacsoport 2018. április 11-én véleményt nyilvánított.
- (61) Mind a tagállamoknak, mind az eu-LISA-nak biztonsági tervet kell fenntartaniuk a biztonsági kötelezettségek teljesítésének megkönnyítése érdekében, és együtt kell működniük egymással a biztonsági problémák kezelése terén. Az eu-LISA-nak emellett biztosítani kell a legújabb technológiafejlesztések folyamatos használatát az interoperabilitási elemek fejlesztésével, kialakításával és kezelésével összefüggésben az adatok sértetlenségének

<sup>(1)</sup> Az Európai Parlament és a Tanács (EU) 2019/816 rendelete (2019. április 17.) az Európai Bűnügyi Nyilvántartási Információs Rendszer kiegészítése érdekében a harmadik országbeli állampolgárokkal és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval rendelkező tagállamok azonosítására szolgáló központosított rendszer (ECRIS-TCN) létrehozásáról, valamint az (EU) 2018/1726 rendelet módosításáról (Lásd e Hivatalos Lap 1. oldalát).

<sup>(2)</sup> Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő kezelése tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról (HL L 8., 2001.1.12., 1. o.).

<sup>(3)</sup> HL C 233., 2018.7.4., 12. o.

biztosítása érdekében. Az eu-LISA e tekintetben fennálló kötelezettségei közé tartozik a jogosulatlan személyek, például külső szolgáltatók személyi állománya interoperabilitási elemeken keresztül kezelt személyes adatokhoz való hozzáféréseinek megakadályozásához szükséges intézkedések elfogadása. A szolgáltatásnyújtásra irányuló szerződések odaítélésakor a tagállamoknak és az eu-LISA-nak fontolóra kell vennie minden olyan intézkedést, amely a személyes adatok és az egyének magánéletének védelmére vagy az alapvető biztonsági érdekek védelmére vonatkozó jogszabályoknak vagy rendelkezéseknek való megfelelés biztosításához szükséges, az (EU) 2018/1046 európai parlamenti és tanácsi rendelet<sup>(14)</sup>, valamint a vonatkozó nemzetközi egyezmények alapján. Az eu-LISA az interoperabilitási elemek fejlesztése során a beépített és alapértelmezett adatvédelem elveit követi.

- (62) A statisztikák és a jelentéstétel céljainak támogatása érdekében az e rendeletben említett illetékes hatóságok, uniós intézmények és ügynökségek felhatalmazással rendelkező személyi állománya számára hozzáférést kell biztosítani az egyes interoperabilitási elemekhez kapcsolódó bizonyos adatokba való betekintés céljából oly módon, hogy a személyek azonosítása ne váljon lehetővé.
- (63) Annak érdekében, hogy a tagállami hatóságok és az uniós ügynökségek alkalmazkodni tudjanak az ESP használatára vonatkozó új követelményekhez, átmeneti időszakot kell biztosítani. Hasonlóképpen, a MID koherens és optimális működésének lehetővé tétele érdekében annak megkezdésére vonatkozóan átmeneti intézkedéseket kell megállapítani.
- (64) Mivel e rendelet célját – nevezetesen az uniós információs rendszerek közötti interoperabilitás keretének létrehozását – a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban a fellépés léptéke és hatása miatt e cél jobban megvalósítható, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés (EUSZ) 5. cikkében foglalt szubsidiaritási elvnek megfelelően. Az említett cikkben foglalt arányosság elvének megfelelően ez a rendelet nem lépi túl az e cél eléréséhez szükséges mértéket.
- (65) Az 515/2014/EU európai parlamenti és tanácsi rendelet<sup>(15)</sup> szerinti intelligens határellenőrzésre elkülönített költségvetés fennmaradó összegét át kell csoportosítani erre a rendeletre az 515/2014/EU rendelet 5. cikke (5) bekezdése b) pontjának megfelelően, az interoperabilitási elemek fejlesztési költségeinek fedezésére.
- (66) E rendelet egyes részletes technikai vonatkozásainak kiegészítése érdekében a Bizottságot fel kell hatalmazni arra, hogy az Európai Unió működéséről szóló szerződés (EUMSZ) 290. cikkének megfelelően jogi aktusokat fogadjon el az alábbiakra vonatkozóan:
- az ESP átmeneti használati időszakának meghosszabbítása;
  - az ETIAS központi egysége által végzett többszörös személyazonosság-észlelés átmeneti időszakának meghosszabbítása;
  - az eljárások tekintetében azon esetek meghatározására, amikor a személyazonosító adatok azonosaknak vagy hasonlóaknak tekinthetők;
  - a CRRS működésére vonatkozó szabályok, többek között a személyes adatok kezelésének speciális biztosítékai és az adattárra alkalmazandó biztonsági szabályok; valamint
  - a webportál működtetésére vonatkozó részletes szabályok.

Különösen fontos, hogy a Bizottság az előkészítő munkája során megfelelő konzultációkat folytasson, többek között szakértői szinten is, és hogy e konzultációkra a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásnak<sup>(16)</sup> megfelelően kerüljön sor. A felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg kap kézhez minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein.

- (67) E rendelet végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni azon időpontok meghatározására vonatkozóan, amikortól az ESP, a közös BMS, a CIR, a MID és a CRRS megkezdí működését.

<sup>(14)</sup> Az Európai Parlament és a Tanács (EU, Euratom) 2018/1046 rendelete (2018. július 18.) az Unió általános költségvetésére alkalmazandó pénzügyi szabályokról, az 1296/2013/EU, az 1301/2013/EU, az 1303/2013/EU, az 1304/2013/EU, az 1309/2013/EU, az 1316/2013/EU, a 223/2014/EU és a 283/2014/EU rendelet és az 541/2014/EU határozat módosításáról, valamint a 966/2012/EU, Euratom rendelet hatályon kívül helyezéséről (HL L 193., 2018.7.30., 1. o.).

<sup>(15)</sup> Az Európai Parlament és a Tanács 515/2014/EU rendelete (2014. április 16.) a Belső Biztonsági Alap részét képező, a külső határok és a vízumügy pénzügyi támogatására szolgáló eszköz létrehozásáról és az 574/2007/EK határozat hatályon kívül helyezéséről (HL L 150., 2014.5.20., 143. o.).

<sup>(16)</sup> HL L 123., 2016. 5.12., 1. o.

- (68) A Bizottságra végrehajtási hatásköröket kell ruházni emellett az alábbiakra vonatkozó részletes szabályok elfogadására: az ESP felhasználói profiljainak technikai részleteire; azon technikai megoldás követelményeire, amely megkönnyíti az uniós információs rendszerek, az Europol-adatok és az Interpol-adatbázisok ESP-n keresztül történő lekérdezését, és az ESP válaszainak formátumára; a MID-ben a különböző uniós információs rendszerekből származó adatok közötti kapcsolatok létrehozásának technikai szabályaira; vörös kapcsolat létrehozása esetén az érintett tájékoztatására szolgáló formanyomtatvány tartalmára és formájára; a közös BMS teljesítményével kapcsolatos követelményekre és teljesítményének nyomon követésére; az adatminőség ellenőrzésére irányuló automatizált mechanizmusokra, eljárásokra és mutatókra; az UMF-re vonatkozó szabvány kidolgozására; a biztonsági incidensek esetén irányadó együttműködési eljárásra; valamint a tagállamok számára a felhasználói hozzáférési kérelmek kezelését szolgáló technikai megoldás követelményeire vonatkozóan. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek <sup>(17)</sup> megfelelően kell gyakorolni.
- (69) Mivel az interoperabilitási elemek jelentős mennyiségű különleges személyes adat kezelésével járnak, fontos, hogy azok a személyek, akiknek az adatait a szóban forgó interoperabilitási elemeken keresztül kezelik, hatékonyan tudják gyakorolni az őket érintettként megillető jogokat az (EU) 2016/679 rendeletben, az (EU) 2016/680 irányelvben és az (EU) 2018/1725 rendeletben előírt módon. Az érintettek rendelkezésére kell bocsátani egy webportált, amely megkönnyíti számukra a személyes adataikhoz való hozzáféréshez, az adatok helyesbítéséhez, törléséhez és kezelésének korlátozásához való joguk gyakorlását. Ezt a webportált az eu-LISA-nak kell létrehoznia és kezelnie.
- (70) Az adatvédelem egyik legfőbb elve az adattakarékosság: az (EU) 2016/679 rendelet 5. cikke (1) bekezdésének c) pontja értelmében a személyes adatok kezelésének az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lennie, és a szükségesre kell korlátozódnia. Emiatt az interoperabilitási elemek nem irányozhatják elő új személyes adatok tárolását, kivéve azokat a kapcsolatokat, amelyek a MID-ben kerülnek tárolásra, és amelyek e rendelet céljai szempontjából a szükséges minimumot jelentik.
- (71) E rendeletnek egyértelmű rendelkezéseket kell tartalmaznia a személyes adatok jogellenes kezelésével, valamint az e rendelettel összeegyeztethetetlen bármely egyéb cselekménnyel kapcsolatos felelősségre és az abból fakadó kártérítési jogosultságra vonatkozóan, az (EU) 2016/679 rendelet, az (EU) 2016/680 irányelv és az (EU) 2018/1725 rendelet alapján fennálló adatkezelői és adatfeldolgozói felelősség és az abból fakadó kártérítési jogosultság sérelme nélkül. Az eu-LISA-nak felelősséggel kell tartoznia mindazon kárért, amelyet adatkezelői minőségében okoz az e rendelet által kifejezetten rá ruházott kötelezettségek nem teljesítése által vagy azáltal, hogy az adatkezelő tagállam jogszerű utasításai által szabott kereteken kívül vagy azokkal ellentétes módon járt el.
- (72) Ez a rendelet nem érinti a 2004/38/EK európai parlamenti és tanácsi irányelv <sup>(18)</sup> alkalmazását.
- (73) Az EUSZ-hez és az EUMSZ-hez csatolt, Dánia helyzetéről szóló 22. jegyzőkönyv 1. és 2. cikke értelmében Dánia nem vesz részt ennek a rendeletnek az elfogadásában, az rá nézve nem kötelező és nem alkalmazandó. Mivel e rendelet – annyiban, amennyiben rendelkezései a SIS-nek az (EU) 2018/1862 rendelet által szabályozott részére vonatkoznak – a schengeni vívmányokon alapul, Dánia az említett jegyzőkönyv 4. cikkének megfelelően az e rendeletről szóló tanácsi döntést követő hat hónapos időszakon belül határoz arról, hogy azt nemzeti jogában végrehajtja-e.
- (74) Annyiban, amennyiben e rendelet rendelkezései a SIS-nek az (EU) 2018/1862 rendelet által szabályozott részére vonatkoznak, az Egyesült Királyság az EUSZ-hez és az EUMSZ-hez csatolt, az Európai Unió keretébe beillesztett schengeni vívmányokról szóló 19. jegyzőkönyv 5. cikkének (1) bekezdésével, valamint a 2000/365/EK tanácsi határozat <sup>(19)</sup> 8. cikkének (2) bekezdésével összhangban részt vesz ebben a rendeletben. Továbbá annyiban, amennyiben e rendelet rendelkezései az Eurodacra és az ECRIS-TCN-re vonatkoznak, az EUSZ-hez és az EUMSZ-hez csatolt, az Egyesült Királyságnak és Írországnak a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség tekintetében fennálló helyzetéről szóló 21. jegyzőkönyv 3. cikkével összhangban az Egyesült Királyság 2018. május 18-i levelében bejelentette, hogy részt kíván venni ennek a rendeletnek az elfogadásában és alkalmazásában.

<sup>(17)</sup> Az Európai Parlament és a Tanács 182/2011/EU rendelete (2011. február 16.) a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról (HL L 55., 2011.2.28., 13. o.).

<sup>(18)</sup> Az Európai Parlament és a Tanács 2004/38/EK irányelve (2004. április 29.) az Unió polgárainak és családtagjaiknak a tagállamok területén történő szabad mozgáshoz és tartózkodáshoz való jogáról, valamint az 1612/68/EGK rendelet módosításáról, továbbá a 64/221/EGK, a 68/360/EGK, a 72/194/EGK, a 73/148/EGK, a 75/34/EGK, a 75/35/EGK, a 90/364/EGK, a 90/365/EGK, és a 93/96/EGK irányelv hatályon kívül helyezéséről. (HL L 158., 2004.4.30., 77. o.).

<sup>(19)</sup> A Tanács 2000/365/EK határozata (2000. május 29.) Nagy-Britannia és Észak-Írország Egyesült Királyságának a schengeni vívmányok egyes rendelkezéseinek alkalmazásában való részvételére vonatkozó kéréséről (HL L 131., 2000.6.1., 43. o.).



- (75) Amennyiben, amennyiben e rendelet rendelkezései a SIS-nek az (EU) 2018/1862 rendelet által szabályozott részére vonatkoznak, Írország elviekben részt vehet e rendelet alkalmazásában az EUSZ-hez és az EUMSZ-hez csatolt, az Európai Unió keretébe beillesztett schengeni vívmányokról szóló 19. jegyzőkönyv 5. cikkének (1) bekezdésével, valamint a 2002/192/EK tanácsi határozat<sup>(20)</sup> 6. cikkének (2) bekezdésével összhangban. Továbbá amennyiben, amennyiben e rendelet rendelkezései az Eurodacra és az ECRIS-TCN-re vonatkoznak, az EUSZ-hez és az EUMSZ-hez csatolt, az Egyesült Királyságnak és Írországnak a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség tekintetében fennálló helyzetéről szóló 21. jegyzőkönyv 1. és 2. cikkével összhangban, az említett jegyzőkönyv 4. cikkének sérelme nélkül, Írország nem vesz részt ennek a rendeletnek az elfogadásában, az rá nézve nem kötelező és nem alkalmazandó. Mivel ilyen körülmények között nem lehet biztosítani, hogy ez a rendelet az EUMSZ 288. cikkében előírtaknak megfelelően teljes egészében alkalmazandó legyen Írországra, Írország nem vesz részt e rendeletnek az elfogadásában, az rá nézve nem kötelező és nem alkalmazandó, a 19. és a 21. jegyzőkönyvben megállapított jogainak sérelme nélkül.
- (76) Izland és Norvégia tekintetében e rendelet – amennyiben rendelkezései a SIS-nek az (EU) 2018/1862 rendelet által szabályozott részére vonatkoznak – az Európai Unió Tanácsa, valamint az Izlandi Köztársaság és a Norvég Királyság közötti, az utóbbiaknak a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról szóló megállapodás<sup>(21)</sup> értelmében a schengeni vívmányok azon rendelkezéseinek továbbfejlesztését képezi, amelyek az 1999/437/EK tanácsi határozat<sup>(22)</sup> 1. cikkének G. pontjában említett területhez tartoznak.
- (77) Svájc tekintetében e rendelet – amennyiben rendelkezései a SIS-nek az (EU) 2018/1862 rendelet által szabályozott részére vonatkoznak – az Európai Unió, az Európai Közösség és a Svájci Államszövetség közötti, a Svájci Államszövetségnek a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról szóló megállapodás<sup>(23)</sup> értelmében a schengeni vívmányok azon rendelkezéseinek továbbfejlesztését képezi, amelyek az 1999/437/EK határozatnak a 2008/146/EK tanácsi határozat<sup>(24)</sup> 3. cikkével együtt értelmezett 1. cikke G. pontjában említett területhez tartoznak.
- (78) Liechtenstein tekintetében ez a rendelet – amennyiben rendelkezései a SIS-nek az (EU) 2018/1862 rendelet által szabályozott részére vonatkoznak – az Európai Unió, az Európai Közösség, a Svájci Államszövetség és a Liechtensteini Hercegség közötti, a Liechtensteini Hercegségnek az Európai Unió, az Európai Közösség és a Svájci Államszövetség közötti, a Svájci Államszövetségnek a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról szóló megállapodáshoz való csatlakozásáról szóló jegyzőkönyv<sup>(25)</sup> értelmében a schengeni vívmányok azon rendelkezéseinek továbbfejlesztését képezi, amelyek az 1999/437/EK határozatnak a 2011/350/EU tanácsi határozat<sup>(26)</sup> 3. cikkével együtt értelmezett 1. cikke G. pontjában említett területhez tartoznak.
- (79) Ez a rendelet tiszteletben tartja az alapvető jogokat és különösen az Európai Unió Alapjogi Chartájában elismert elveket, és végrehajtása során e jogoknak és elveknek megfelelően kell eljárni.
- (80) Annak érdekében, hogy e rendelet illeszkedjen a hatályos jogi keretbe, az (EU) 2018/1726 európai parlamenti és tanácsi rendeletet<sup>(27)</sup>, valamint az (EU) 2018/1862 és az (EU) 2019/816 rendeletet megfelelően módosítani kell,

<sup>(20)</sup> A Tanács 2002/192/EK határozata (2002. február 28.) Írországnak a schengeni vívmányok egyes rendelkezései alkalmazásában való részvételére vonatkozó kéréséről (HL L 64., 2002.3.7., 20. o.).

<sup>(21)</sup> HL L 176., 1999.7.10., 36. o.

<sup>(22)</sup> A Tanács 1999/437/EK határozata (1999. május 17.) az Európai Unió Tanácsa, valamint az Izlandi Köztársaság és a Norvég Királyság között, e két államnak a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról kötött megállapodás alkalmazását szolgáló egyes szabályokról (HL L 176., 1999.7.10., 31. o.).

<sup>(23)</sup> HL L 53., 2008.2.27., 52. o.

<sup>(24)</sup> A Tanács 2008/149/IB határozata (2008. január 28.) az Európai Unió, az Európai Közösség és a Svájci Államszövetség közötti, a Svájci Államszövetségnek a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról szóló megállapodásnak az Európai Unió nevében történő megkötéséről (HL L 53., 2008.2.27., 50. o.).

<sup>(25)</sup> HL L 160., 2011.6.18., 21. o.

<sup>(26)</sup> A Tanács 2011/350/EU határozata (2011. március 7.) az Európai Unió, az Európai Közösség, a Svájci Államszövetség és a Liechtensteini Hercegség közötti, a Liechtensteini Hercegségnek az Európai Unió, az Európai Közösség és a Svájci Államszövetség közötti, a Svájci Államszövetségnek a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló, különösen a belső határokon történő ellenőrzés megszüntetéséhez és a személyek mozgásához kapcsolódó társulásáról szóló megállapodáshoz való csatlakozásáról szóló jegyzőkönyvnek az Európai Unió nevében történő megkötéséről (HL L 160., 2011.6.18., 19. o.).

<sup>(27)</sup> Az Európai Parlament és a Tanács (EU) 2018/1726 rendelete (2018. november 14.) a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai uniós ügynökségről (eu-LISA), az 1987/2006/EK rendelet és a 2007/533/IB tanácsi határozat módosításáról, valamint az 1077/2011/EU rendelet hatályon kívül helyezéséről (HL L 295., 2018.11.21., 99. o.).

ELFOGADTA EZT A RENDELETET:

## I. FEJEZET

### Általános rendelkezések

#### 1. cikk

#### Tárgy

(1) Ez a rendelet az (EU) 2019/817 európai parlamenti és tanácsi rendelettel <sup>(28)</sup> együtt létrehozza a határregisztrációs rendszer (EES), a Vízuminformációs Rendszer (VIS), az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS), az Eurodac, a Schengeni Információs Rendszer (SIS) és a harmadik országok állampolgáira vonatkozó Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS-TCN) interoperabilitását biztosító keretet.

(2) A keret az alábbi interoperabilitási elemeket foglalja magában:

- a) az európai keresőportál (ESP);
- b) a közös biometrikus megfeleltetési szolgáltatás (közös BMS);
- c) közös személyazonosítóadat-tár (CIR);
- d) a többszörös személyazonosságot észlelő rendszer (MID).

(3) Ez a rendelet ezen felül rendelkezéseket állapít meg az adatminőségre vonatkozó követelményekre, az egységes üzenetformátumra (UMF), és a jelentések és statisztikák központi adattárára (CRRS) vonatkozóan, valamint az interoperabilitási elemek kialakítása, fejlesztése és működése tekintetében a tagállamok és a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagy méretű IT-rendszereinek üzemeltetési igazgatását végző európai ügynökség (eu-LISA) feladataira vonatkozóan.

(4) Ez a rendelet módosítja továbbá a tagállamok kijelölt hatóságainak és a Bűnüldözési Együttműködés Európai Uniói Ügynökségének (Europol) az EES-hez, a VIS-hez, az ETIAS-hoz és az Eurodachoz a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából való hozzáféréssel kapcsolatos eljárásokat és feltételeket.

(5) Ez a rendelet meghatározza továbbá a személyek személyazonosságának ellenőrzésére és a személyek azonosítására szolgáló keretrendszert.

#### 2. cikk

### Célkitűzések

(1) Az interoperabilitás biztosítása révén e rendelet célkitűzései a következők:

- a) a külső határokon a határforgalom-ellenőrzések hatékonyságának és eredményességének javítása;
- b) az illegális bevándorlás megelőzéséhez és az ellene folytatott küzdelemhez való hozzájárulás,
- c) hozzájárulás az Unióban a szabadság, a biztonság és a jog érvényesülésén alapuló uniós térség magas fokú biztonságához, beleértve a tagállamok területén a közbiztonság és a közrend fenntartását és a biztonság védelmét is;
- d) a közös vízümpolitika végrehajtásának javítása;
- e) segítségnyújtás a nemzetközi védelem iránti kérelmek vizsgálatához;
- f) hozzájárulás a terrorista bűncselekmények és egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez és nyomozásához;
- g) a személyazonosságukat igazolni nem tudó ismeretlen személyek vagy természeti katasztrófa, baleset vagy terroristámadás esetén az azonosítatlan emberi maradványok azonosításának elősegítése.

(2) Az (1) bekezdésben említett célokat az alábbiak révén kell megvalósítani:

- a) a személyek helyes azonosításának biztosítása;
- b) a személyazonossággal való visszaélés elleni küzdelemhez való hozzájárulás;

<sup>(28)</sup> Az Európai Parlament és a Tanács (EU) 2019/817 rendelete (2019. május 20.) az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízumügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726, az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról (lásd e Hivatalos Lap 27. oldalát).

- c) az adatminőség javítása és az uniós információs rendszerekben tárolt adatokra vonatkozó minőségi követelmények harmonizálása az egyes rendszereket szabályozó jogi eszközök adatkezelési követelményeinek, valamint az adatvédelmi előírások és elvek egyidejű tiszteletben tartása mellett;
- d) az uniós információs rendszerek tagállami technikai és operatív végrehajtásának megkönnyítése és támogatása;
- e) az egyes uniós információs rendszerekre vonatkozó adatbiztonsági és adatvédelmi feltételek megerősítése, egyszerűsítése és egységesebbé tétele, a bizonyos adatkategóriák esetében biztosított különös védelem és biztosítékok sérelme nélkül;
- f) a kijelölt hatóságok EES-hez, VIS-hez, ETIAS-hoz és Eurodachoz való hozzáféréseinek észszerűsítése, a hozzáférés szükséges és arányos feltételeinek biztosítása mellett;
- g) az EES, a VIS, az ETIAS, az Eurodac, a SIS és az ECRIS-TCN céljainak támogatása.

### 3. cikk

#### Hatály

- (1) Ez a rendelet az Eurodac, a SIS és az ECRIS-TCN vonatkozásában alkalmazandó.
- (2) Ez a rendelet az Europol-adatokra is alkalmazandó olyan mértékben, amely lehetővé teszi azok egyidejű lekérdezését az (1) bekezdésben említett uniós információs rendszerekkel.
- (3) E rendelet azokra a személyekre alkalmazandó, akiknek személyes adatai az (1) bekezdésben említett uniós információs rendszerekben, és a (2) bekezdésben említett Europol-adatok között kezelhetők.

### 4. cikk

#### Fogalommeghatározások

E rendelet alkalmazásában:

- 1. „külső határok”: az (EU) 2016/399 európai parlamenti és tanácsi rendelet <sup>(29)</sup> 2. cikkének 2. pontjában meghatározott külső határok;
- 2. „határforgalom-ellenőrzés”: az (EU) 2016/399 rendelet 2. cikkének 11. pontjában meghatározott határforgalom-ellenőrzés;
- 3. „határforgalom-ellenőrzést végző hatóság”: az a határőr, akit a nemzeti jognak megfelelően határforgalom-ellenőrzés elvégzésére kijelöltek;
- 4. „felügyeleti hatóságok”: az (EU) 2016/679 rendelet 51. cikkének (1) bekezdésében említett felügyeleti hatóság és az (EU) 2016/680 irányelv 41. cikkének (1) bekezdésében említett felügyeleti hatóság;
- 5. „ellenőrzés”: az adatcsoportok összehasonlításának folyamata, amelynek célja a közölt személyazonosság érvényességének megállapítása (egy az egyhez megfeleltetés);
- 6. „személyazonosítás”: egy személy személyazonosságának több adatcsoport és adatbázis összehasonlításával történő megállapítása (egy a többhöz megfeleltetés);
- 7. „alfanumerikus adatok”: betűkből, számokból, speciális karakterekből, szóközökből és központozási jelekből álló adatok;
- 8. „személyazonosító adatok”: a 27. cikk (3) bekezdésének a)–e) pontjában említett adatok;
- 9. „ujjnyomatadatok”: ujjnyomatok és látens ujjnyomok képmásai, amelyek egyedi jellegűnek és a bennük foglalt referenciapontoknak köszönhetően lehetővé teszik az adott személy személyazonosságával kapcsolatos pontos és kétséget kizáró összehasonlításokat;

<sup>(29)</sup> Az Európai Parlament és a Tanács (EU) 2016/399 rendelete (2016. március 9.) a személyek határátlépésére irányadó szabályok uniós kódexéről (Schengeni határ-ellenőrzési kódex) (HL L 77., 2016.3.23., 1. o.).

10. „arckép más”: a személy arcáról készült digitális felvételek;
11. „biometrikus adatok”: az ujjnyomatadatok vagy az arckép más, vagy mindkettő;
12. „biometrikus sablon”: a biometrikus adatok jellemzőinek leképezése útján nyert matematikai ábrázolás, ami a személyazonosítások és az ellenőrzések elvégzéséhez szükséges jellegzetességekre korlátozódik;
13. „úti okmány”: útlevél vagy azzal egyenértékű egyéb okmány, amely feljogosítja birtokosát a külső határ átlépésére és vízummal látható el;
14. „úti okmány-adatok”: az úti okmány típusa, száma és a kibocsátó ország, az úti okmány érvényességének lejárat dátuma és az úti okmányt kiállító ország hárombetűs kódja;
15. „uniós információs rendszerek”: az EES, a VIS, az ETIAS, az Eurodac, a SIS és az ECRIS-TCN;
16. „Europol-adatok”: az Europol által az (EU) 2016/794 rendelet 18. cikke (2) bekezdésének a), b) és c) pontjában említett célból kezelt személyes adatok;
17. „Interpol-adatbázisok”: az Interpol ellopott és elvesztett úti okmányokat tartalmazó adatbázisa (SLTD adatbázis) és az Interpol-körzésben megjelölt úti okmányok adatbázisa (TDAWN adatbázis);
18. „egyezés”: olyan megfelelés megléte, ami a valamely információs rendszerben vagy adatbázisban rögzített vagy rögzítés alatt álló személyes adatok automatizált összehasonlításának eredménye;
19. „rendőri hatóság”: az (EU) 2016/680 irányelv 3. cikkének 7. pontja szerinti illetékes hatóság;
20. „kijelölt hatóságok”: az (EU) 2017/2226 európai parlamenti és tanácsi rendelet <sup>(30)</sup> 3. cikke (1) bekezdésének 26. pontjában, a 2008/633/IB tanácsi határozat <sup>(31)</sup> 2. cikke (1) bekezdésének e) pontjában és az (EU) 2018/1240 európai parlamenti és tanácsi rendelet <sup>(32)</sup> 3. cikke (1) bekezdésének 21. pontjában meghatározott kijelölt hatóságok;
21. „terrorista bűncselekmény”: az a nemzeti jog szerinti bűncselekmény, amely megfelel az (EU) 2017/541 európai parlamenti és tanácsi irányelvben <sup>(33)</sup> említett bűncselekmények valamelyikének, vagy azzal egyenértékű;
22. „súlyos bűncselekmény”: az a bűncselekmény, amely megfelel a 2002/584/IB tanácsi kerethatározat <sup>(34)</sup> 2. cikkének (2) bekezdésében említett valamely bűncselekménynek, vagy azzal egyenértékű, amennyiben esetében a nemzeti jog alapján kiszabható büntetési tétel felső határa legalább három év szabadságvesztés vagy szabadságelvonással járó intézkedés;
23. „határregisztrációs rendszer” vagy „EES”: az (EU) 2017/2226 rendelet által létrehozott határregisztrációs rendszer;
24. „vízuminformációs rendszer” vagy „VIS”: a 767/2008/EK európai parlamenti és tanácsi rendelettel <sup>(35)</sup> létrehozott vízuminformációs rendszer;
25. „Európai Utasinformációs és Engedélyezési Rendszer” vagy „ETIAS”: az (EU) 2018/1240 rendelettel létrehozott Európai Utasinformációs és Engedélyezési Rendszer;

<sup>(30)</sup> Az Európai Parlament és a Tanács (EU) 2017/2226 rendelete (2017. november 30.) a tagállamok külső határait átlépő harmadik országbeli állampolgárok belépésére és kilépésére, valamint beléptetésének megtagadására vonatkozó adatok rögzítésére szolgáló határregisztrációs rendszer (EES) létrehozásáról és az EES-hez való bűnüldözési célú hozzáférés feltételeinek meghatározásáról, valamint a Schengeni Megállapodás végrehajtásáról szóló egyezmény, a 767/2008/EK rendelet és az 1077/2011/EU rendelet módosításáról. HL L 327., 2017.12.9., 20. o.).

<sup>(31)</sup> A Tanács 2008/633/IB határozata (2008. június 23.) a vízuminformációs rendszerhez (VIS) a tagállamok kijelölt hatóságai, valamint az Europol számára a terrorcselekmények és egyéb súlyos bűncselekmények megelőzése, felderítése és kivizsgálása érdekében, betekintés céljából történő hozzáférésről. (HL L 218., 2008.8.13., 129. o.)

<sup>(32)</sup> Az Európai Parlament és a Tanács (EU) 2018/1240 rendelete (2018. szeptember 12.) az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS) létrehozásáról, valamint az 1077/2011/EU rendelet, az 515/2014/EU rendelet, az (EU) 2016/399 rendelet, az (EU) 2016/1624 rendelet és az (EU) 2017/2226 rendelet módosításáról (HL L 236., 2018.9.19., 1. o.).

<sup>(33)</sup> Az Európai Parlament és a Tanács (EU) 2017/541 irányelve (2017. március 15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról (HL L 88., 2017.3.31., 6. o.).

<sup>(34)</sup> A Tanács 2002/584/IB kerethatározata (2002. június 13.) az európai elfogatóparancsról és a tagállamok közötti átadási eljárásokról (HL L 190., 2002.7.18., 1. o.).

<sup>(35)</sup> Az Európai Parlament és a Tanács 767/2008/EK rendelete (2008. július 9.) a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről (VIS-rendelet) (HL L 218., 2008.8.13., 60. o.).

26. „Eurodac”: a 603/2013/EU európai parlamenti és tanácsi rendelettel <sup>(36)</sup> létrehozott Eurodac;
27. „Schengeni Információs Rendszer” vagy „SIS”: az (EU) 2018/1860, az (EU) 2018/1861 és az (EU) 2018/1862 rendelettel létrehozott Schengeni Információs Rendszer;
28. „ECRIS-TCN”: az (EU) 2019/816 rendelettel létrehozott, a harmadik országbeli állampolgárokkal és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval rendelkező tagállamok azonosítására szolgáló központosított rendszer.

#### 5. cikk

### Megkülönböztetésmentesség és alapvető jogok

A személyes adatok e rendelet alkalmazásában történő kezelése nem eredményezheti a személyek semmilyen fajta, például nem, fajon, bőrszínen, etnikai vagy társadalmi származáson, genetikai jellemzőkön, nyelven, valláson vagy meggyőződésen, politikai vagy más véleményen, nemzeti kisebbséghez való tartozáson, vagyoni helyzeten, születésen, fogyatékoságon, életkoron vagy szexuális irányultáson alapuló megkülönböztetését. A személyes adatok kezelése során teljes mértékben tiszteletben kell tartani az emberi méltóságot és sérthetlenséget, valamint az alapvető jogokat, többek között a magánélet tiszteletben tartására és a személyes adatok védelmére vonatkozó jogot. Különös figyelmet kell fordítani a gyermekekre, az idősekre, a fogyatékosággal élő személyekre és a nemzetközi védelemre szoruló személyekre. A gyermek mindenképp felett álló érdekeire kiemelt figyelmet kell fordítani.

## II. FEJEZET

### Európai keresőportál

#### 6. cikk

### Európai keresőportál

- (1) Az európai keresőportál (ESP) létrehozásának célja a tagállami hatóságok és az uniós ügynökségek gyors, akadálytalan, hatékony, szisztematikus és ellenőrzött hozzáféréseinek megkönnyítése az uniós információs rendszerekhez, az Europol-adatokhoz és az Interpol-adatbázisokhoz feladataik ellátása céljából, összhangban hozzáférési jogosultságokkal és az EES, a VIS, az ETIAS, az Eurodac, a SIS és az ECRIS-TCN céljaival és célkitűzéseivel.
- (2) Az ESP összetevői:
  - a) egy keresőportált is tartalmazó központi infrastruktúra, amely lehetővé teszi az EES, a VIS, az ETIAS, az Eurodac, a SIS, az ECRIS-TCN, valamint az Europol-adatok és az Interpol-adatbázisok egyidejű lekérdezését;
  - b) egy biztonságos kommunikációs csatorna az ESP, a tagállamok és az uniós ügynökségek között, amelyek jogosultak az ESP használatára;
  - c) egy biztonságos kommunikációs infrastruktúra az ESP és az EES, a VIS, az ETIAS, az Eurodac, a központi SIS, az ECRIS-TCN, az Europol-adatok és az Interpol-adatbázisok között, valamint az ESP és a CIR és a MID központi infrastruktúrái között.
- (3) Az eu-LISA kifejleszti az ESP-t, és gondoskodik annak műszaki irányításáról.

#### 7. cikk

### Az európai keresőportál használata

(1) Az ESP használatára kizárólag azon tagállami hatóságok és uniós ügynökségek jogosultak, amelyek az uniós információs rendszereket szabályozó jogi eszközökkel összhangban hozzáféréssel rendelkeznek legalább egy uniós információs rendszerhez, e rendelettel összhangban hozzáféréssel rendelkeznek a CIR-hez és a MID-hez, az (EU) 2016/794 rendelettel összhangban hozzáféréssel rendelkeznek az Europol-adatokhoz, vagy az ilyen hozzáférést szabályozó uniós vagy nemzeti joggal összhangban hozzáféréssel rendelkeznek az Interpol-adatbázisokhoz.

Ezek a tagállami hatóságok és uniós ügynökségek csak az említett uniós információs rendszereket szabályozó jogi eszközökben, az (EU) 2016/794 rendeletben és az e rendeletben meghatározott célokból használhatják az ESP-t és az általa rendelkezésre bocsátott adatokat.

<sup>(36)</sup> Az Európai Parlament és a Tanács 603/2013/EU rendelete (2013. június 26.) a harmadik országbeli állampolgár vagy hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról szóló 604/2013/EU rendelet hatékony alkalmazása érdekében az ujjlenyomatok összehasonlítását szolgáló Eurodac létrehozásáról, továbbá a tagállamok bűnüldöző hatóságai és az Europol által az Eurodac-adatokkal való, bűnüldözési célú összehasonlítások kérelmezéséről, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző ügynökség létrehozásáról szóló 1077/2011/EU rendelet módosításáról (HL L 180., 2013.6.29., 1. o.).

(2) Az (1) bekezdésben említett tagállami hatóságok és uniós ügynökségek az ESP-t személyekre vagy azok úti okmányaira vonatkozó adatoknak az Eurodac és az ECRIS-TCN központi rendszereiben történő keresésére használják, az említett uniós információs rendszereket szabályozó jogi eszközökben említett és a nemzeti jog szerinti hozzáférési jogosultságaikkal összhangban. Az ESP-t ezen kívül – e rendeletben meghatározott hozzáférési jogosultságaikkal összhangban és a 20., a 21. és a 22. cikk szerinti célokból – a CIR lekérdezésére is használják.

(3) Az (1) bekezdésben említett tagállami hatóságok az ESP-t személyekre vagy azok úti okmányaira vonatkozó adatoknak az (EU) 2018/1860 és az (EU) 2018/1861 rendeletben említett központi SIS-ben történő keresésére használhatják.

(4) Ha az uniós jog ekként rendelkezik, az (1) bekezdésben említett uniós ügynökségek az ESP-t személyekre vagy azok úti okmányaira vonatkozó adatoknak a központi SIS-ben történő keresésére használják.

(5) Az (1) bekezdésben említett tagállami hatóságok és uniós ügynökségek az ESP-t személyekre vagy úti okmányaira vonatkozó adatoknak az Europol-adatokban történő keresésére használhatják, amennyiben az uniós jog és a nemzeti jog ekként rendelkezik, az abban foglalt hozzáférési jogosultságaikkal összhangban.

## 8. cikk

### Az európai keresőportál felhasználói számára készült profilok

(1) Az ESP használatának lehetővé tétele érdekében az eu-LISA a tagállamokkal együttműködve a (2) bekezdésben említett technikai részletekkel és hozzáférési jogokkal összhangban profilt hoz létre minden egyes ESP-felhasználói kategória és a lekérdezések célja alapján. Minden egyes profil az uniós és a nemzeti joggal összhangban az alábbi információkat foglalja magában:

- a) a lekérdezéshez használandó adatmezők;
- b) azok az uniós információs rendszerek, Europol-adatok és Interpol-adatbázisok, amelyeket le kell, illetve amelyeket le lehet kérdezni, és amelyek a felhasználónak választ kell, hogy adjanak;
- c) az uniós információs rendszerek, az Europol-adatok és az Interpol-adatbázisok azon konkrét adatai, amelyek lekérdezhetők;
- d) az egyes válaszokban rendelkezésre bocsátható adatkategóriák.

(2) A Bizottság végrehajtási jogi aktusokat fogad el az (1) bekezdésben említett profilok technikai részleteinek meghatározása céljából, az ESP-felhasználóknak az uniós információs rendszereket szabályozó jogi eszközök és a nemzeti jog szerinti hozzáférési jogosultságaival összhangban. Ezeket a végrehajtási jogi aktusokat a 70. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(3) Az (1) bekezdésben említett profilokat az eu-LISA a tagállamokkal együttműködésben rendszeresen, legalább évente egyszer felülvizsgálja és szükség esetén frissíti.

## 9. cikk

### Lekérdezések

(1) Az ESP-felhasználó a lekérdezést alfanumerikus vagy biometrikus adatok ESP-be történő bevétele révén kezdeményezi. Ha lekérdezést kezdeményeztek, az ESP a felhasználó által bevitt adatokkal és a felhasználói profilnak megfelelően egyidejűleg végez lekérdezést az EES-ben, az ETIAS-ban, a VIS-ben, a SIS-ben, az Eurodacban, az ECRIS-TCN-ben, a CIR-ben, az Europol-adatokban és az Interpol-adatbázisokban.

(2) Az ESP útján történő lekérdezés kezdeményezéséhez használt adatkategóriák megfelelnek a különböző uniós információs rendszerek, az Europol-adatok és az Interpol-adatbázisok lekérdezésére felhasználható, személyekre vagy úti okmányokra vonatkozó adatkategóriáknak, a rájuk irányadó jogi eszközöknek megfelelően.

(3) Az eu-LISA a tagállamokkal együttműködésben az ESP vonatkozásában a 38. cikkben említett UMF-n alapuló interfészvezérlési dokumentációt alkalmaz.

(4) A lekérdezés ESP-felhasználó általi kezdeményezése esetén az EES, az ETIAS, a VIS, a SIS, az Eurodac, az ECRIS-TCN, a CIR és a MID, valamint az Europol-adatok és az Interpol-adatbázisok a lekérdezésre válaszként rendelkezésre bocsátják az általuk tárolt adatokat.

A 20. cikk sérelme nélkül az ESP által adott válasznak jeleznie kell, hogy az adatok mely uniós információs rendszerben vagy adatbázisban található meg.

Az ESP nem szolgáltat információkat az olyan uniós információs rendszerekben tárolt olyan adatokról, olyan Europol-adatokról és az olyan Interpol-adatbázisokról, amelyekhez a felhasználónak az alkalmazandó uniós és nemzeti jog szerint nincs hozzáférése.

(5) Az ESP-n keresztül kezdeményezett, Interpol-adatbázisokra irányuló lekérdezéseket úgy kell elvégezni, hogy az információk ne jussanak az Interpol-riasztás rögzítőjének tudomására.

(6) Az ESP választ ad a felhasználónak, amint az egyik uniós információs rendszerben, az Europol-adatok között vagy az Interpol-adatbázisokban rendelkezésre áll az adat. Ezek a válaszok csak azokat az adatokat tartalmazzák, amelyekhez a felhasználó az uniós és a nemzeti jog alapján hozzáféréssel rendelkezik.

(7) A Bizottság végrehajtási jogi aktust fogad el az uniós információs rendszerek, az Europol-adatok és az Interpol-adatbázisok ESP általi lekérdezésére vonatkozó technikai eljárásnak és az ESP által adott válaszok formátumának meghatározására. Ezeket a végrehajtási jogi aktusokat a 70. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

#### 10. cikk

##### Naplóvezetés

(1) Az (EU) 2018/1862 rendelet 12. és 18. cikkének, az (EU) 2019/816 rendelet 29. cikkének, valamint az (EU) 2016/794 rendelet 40. cikkének sérelme nélkül, az eu-LISA az ESP-n végzett valamennyi adatkezelési műveletről naplót vezet. A napló az alábbiakat tartalmazza:

- a) a lekérdezést kezdeményező tagállam vagy uniós ügynökség és a használt, ESP profil;
- b) a lekérdezés napja és időpontja;
- c) azon uniós információs rendszerek és Europol-adatok, amelyekben lekérdezést végeztek.

(2) Minden tagállam naplót vezet az ESP használatára megfelelő felhatalmazással rendelkező hatóságai által és e hatóságok megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről. Minden uniós ügynökség naplót vezet a megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről.

(3) Az (1) és a (2) bekezdésben említett naplókat kizárólag az adatvédelmi ellenőrzés érdekében – ideértve a lekérdezés elfogadhatóságának és az adatkezelés jogszerűségének ellenőrzését –, valamint az adatbiztonság és az adatok sértetlensége biztosításának céljára lehet felhasználni. E naplókat megfelelő intézkedésekkel kell védeni a jogosulatlan hozzáféréstől, és létrehozásuk után egy évvel törölni kell. Ha azonban egy már megkezdett ellenőrzési eljáráshoz szükség van rájuk, akkor törlésükre akkor kell sort keríteni, amikor már nem szükségesek az ellenőrzési eljáráshoz.

#### 11. cikk

##### Tartalékeljárások arra az esetre, ha az európai keresőportál használata műszakilag lehetetlen

(1) Ha az ESP-t annak meghibásodása miatt azt műszakilag lehetetlen egy vagy több uniós információs rendszer vagy a CIR lekérdezésére használni, az eu-LISA automatikusan értesíti erről az ESP-felhasználókat.

(2) Ha az ESP-t valamely tagállam nemzeti infrastruktúrájának meghibásodása miatt műszakilag lehetetlen egy vagy több uniós információs rendszer vagy a CIR lekérdezésére használni, e tagállam automatikusan értesíti erről az eu-LISA-t és a Bizottságot.

(3) Az e cikk (1) vagy (2) bekezdésében említett esetekben a műszaki hiba orvoslásáig a 7. cikk (2) és (4) bekezdésében foglalt kötelezettség nem alkalmazandó, és a tagállamok az uniós információs rendszerekhez vagy a CIR-hez közvetlenül férnek hozzá, ha az uniós vagy a nemzeti jog ezt előírja.

(4) Ha az ESP-t valamely uniós ügynökség infrastruktúrájának meghibásodása miatt műszakilag lehetetlen egy vagy több uniós információs rendszer vagy a CIR lekérdezésére használni, az adott ügynökség automatikusan értesíti erről az eu-LISA-t és a Bizottságot.

### III. FEJEZET

#### Közös biometrikus megfeleltetési szolgáltatás

#### 12. cikk

#### Közös biometrikus megfeleltetési szolgáltatás

(1) Létrejön a 13. cikkben említett, a CIR-ben és a SIS-ben tárolt biometrikus adatokból kinyert biometrikus sablonokat tároló és több uniós információs rendszer biometrikus adatokkal történő lekérdezését lehetővé tevő közös biometrikus megfeleltetési szolgáltatás (közös BMS) a CIR és a MID támogatása, valamint az EES, a VIS, az Eurodac, a SIS és az ECRIS-TCN célkitűzéseinek elősegítése céljából.

- (2) A közös BMS a következőkből áll:
- olyan központi infrastruktúra, amely az EES, a VIS, a SIS, az Eurodac és az ECRIS-TCN központi rendszereinek helyébe lép, amennyiben tárolja a biometrikus sablonokat és lehetővé teszi a biometrikus adatokkal való kereséseket;
  - egy biztonságos kommunikációs infrastruktúra a közös BMS, a központi SIS és a CIR között.
- (3) Az eu-LISA kifejleszti a közös BMS-t, és gondoskodik annak műszaki irányításáról.

### 13. cikk

#### **Biometrikus sablonok tárolása a közös biometrikus megfeleltetési szolgáltatásban**

- (1) A közös BMS tárolja a biometrikus sablonokat, amelyeket az alábbi biometrikus adatokból nyer:
- az (EU) 2018/1862 rendelet 20. cikke (3) bekezdésének w) és y) pontjában említett adatok, a tenyérnyomatokra vonatkozó adatok kivételével;
  - az (EU) 2019/816 rendelet 5. cikke (1) bekezdésének b) pontjában és (2) bekezdésében említett adatok.

A biometrikus sablonokat a közös BMS logikailag különválasztva tárolja azon információs rendszerek szerint, amelyekből az adatok származnak.

(2) A közös BMS az (1) bekezdésben említett valamennyi adatszoport vonatkozásában minden biometrikus sablonban hivatkozást tartalmaz azokra az uniós információs rendszerekre, amelyekben a megfelelő biometrikus adatokat tárolják, és ezen uniós információs rendszerek konkrét bejegyzéseire.

(3) A biometrikus sablonokat csak azt követően lehet bevinni a közös BMS-be, hogy a közös BMS elvégezte a valamelyik uniós információs rendszerhez hozzáadott biometrikus adatok automatizált minőség-ellenőrzését annak biztosítása céljából, hogy az adatminőségi minimumkövetelmények teljesüljenek.

(4) Az (1) bekezdésben említett adatok tárolásának meg kell felelnie a 37. cikk (2) bekezdésében említett minőségi követelményeknek.

(5) A Bizottság végrehajtási jogi aktus révén meghatározza a közös BMS teljesítményének nyomon követésére vonatkozó teljesítmény-követelményeket és gyakorlati szabályokat annak biztosítása érdekében, hogy a biometrikus keresések hatékonysága megfeleljen az olyan időtartam szempontjából érzékeny eljárásoknak, mint például a határforgalom-ellenőrzések és a személyazonosítások. Ezeket a végrehajtási jogi aktusokat a 70. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

### 14. cikk

#### **Biometrikus adatok keresése a közös biometrikus megfeleltetési szolgáltatással**

A CIR-ben és a SIS-ben tárolt biometrikus adatok keresése céljából a CIR és a SIS a közös BMS-ben tárolt biometrikus sablonokat használja. Biometrikus adatokkal történő lekérdezés az e rendeletben, illetve a 767/2008/EK, az (EU) 2017/2226, az (EU) 2018/1860, az (EU) 2018/1861, az (EU) 2018/1862 és az (EU) 2019/816 rendeletben előírt célokból végezhető.

### 15. cikk

#### **Adatmegőrzés a közös biometrikus megfeleltetési szolgáltatás keretében**

A 13. cikk (1) és (2) bekezdésében említett adatokat kizárólag addig lehet tárolni a közös BMS rendszerben, amíg a megfelelő biometrikus adatokat a CIR vagy a SIS tárolja. Ezeket az adatokat automatikusan törölni kell a közös BMS-ből.



## 16. cikk

**Naplóvezetés**

(1) Az (EU) 2018/1862 rendelet 12. és 18. cikkének, valamint az (EU) 2019/816 rendelet 29. cikkének sérelme nélkül, az eu-LISA a közös BMS keretében végzett valamennyi adatkezelési műveletről naplót vezet. A napló az alábbiakat tartalmazza:

- a) a lekérdezést kezdeményező tagállam vagy uniós ügynökség;
- b) a biometrikus sablonok létrehozásával és tárolásával kapcsolatos előzmények;
- c) azon uniós információs rendszerek, amelyekben a közös BMS-ben tárolt biometrikus sablonokkal lekérdezést végeztek;
- d) a lekérdezés napja és időpontja;
- e) a lekérdezés kezdeményezéséhez használt biometrikus adatok típusa;
- f) a lekérdezés eredményei, valamint az eredmény elérésének napja és időpontja.

(2) Minden tagállam naplót vezet a közös BMS használatára megfelelő felhatalmazással rendelkező hatóságai által és e hatóságok megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről. Minden uniós ügynökség naplót vezet a megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről.

(3) Az (1) és a (2) bekezdésben említett naplókat kizárólag az adatvédelmi ellenőrzés érdekében – ideértve a lekérdezés elfogadhatóságának és az adatkezelés jogszerűségének ellenőrzését –, valamint az adatbiztonságnak és az adatok sértetlenségének garantálása céljából lehet felhasználni. E naplókat megfelelő intézkedésekkel kell védeni a jogosulatlan hozzáféréstől, és létrehozásuk után egy évvel törölni kell. Ha azonban egy már megkezdett ellenőrzési eljárásához szükség van rájuk, akkor törlésükre akkor kell sort keríteni, amikor már nem szükségesek az ellenőrzési eljárásához.

## IV. FEJEZET

**Közös személyazonosítóadat-tár**

## 17. cikk

**Közös személyazonosítóadat-tár**

(1) Létrejön az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban vagy az ECRIS-TCN-ben nyilvántartott valamennyi személy vonatkozásában egyéni aktát létrehozó, a 18. cikk szerinti adatokat tartalmazó közös személyazonosítóadat-tár (CIR), az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban és az ECRIS-TCN-ben nyilvántartott személyek 20. cikkel összhangban történő helyes azonosításának megkönnyítése és segítése, a 21. cikkel összhangban a MID működésének támogatása, valamint a kijelölt hatóságok és az Europol EES-hez, VIS-hez, ETIAS-hoz és Eurodachoz való hozzáféréseinek megkönnyítése és észszerűsítése céljából, amikor ez terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez vagy nyomozásához szükséges a 22. cikkel összhangban.

(2) A CIR a következőkből áll:

- a) egy központi infrastruktúra, amely a 18. cikkben említett adatok tárolásához szükséges mértékben az EES, a VIS, az ETIAS, az Eurodac és az ECRIS-TCN központi rendszereinek helyébe lép;
- b) a CIR és az uniós és nemzeti jog alapján a CIR használatára jogosult tagállamok és uniós ügynökségek közötti biztonságos kommunikációs csatorna;
- c) egy biztonságos kommunikációs infrastruktúra a CIR és az EES, a VIS, az ETIAS, az Eurodac és az ECRIS-TCN között, valamint az ESP, a közös BMS és a MID központi infrastruktúráival.

(3) Az eu-LISA kifejleszti a CIR-t, és gondoskodik annak műszaki irányításáról.

(4) Ha a CIR meghibásodása miatt műszakilag lehetetlen lekérdezést végezni a CIR-ben személyazonosítás céljából a 20. cikk szerint, a többszörös személyazonosság észlelése céljából a 21. cikk szerint vagy terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából a 22. cikk szerint, az eu-LISA automatikusan értesíti erről a CIR-felhasználókat.

(5) Az eu-LISA a tagállamokkal együttműködésben a CIR vonatkozásában a 38. cikkben említett UMF-n alapuló interfészvezérlési dokumentációt alkalmaz.

## 18. cikk

**A közös személyazonosítóadat-tár adatai**

(1) A CIR a következő adatokat logikailag különválasztva tárolja azon információs rendszerek szerint, amelyekből az adatok származnak: az (EU) 2019/816 rendelet 5. cikke (1) bekezdésének b) pontjában és (2) bekezdésében említett adatok, valamint 5. cikke (1) bekezdésének a) pontjában felsorolt következő adatok: vezetéknév (családi név), utónevek (keresztnevek), születési idő, születési hely (város és ország), állampolgárság vagy állampolgárságok, nem, adott esetben korábbi nevek, amennyiben rendelkezésre állnak, álnevek vagy felvett nevek, valamint – amennyiben rendelkezésre állnak – az úti okmányokra vonatkozó információk.

(2) A CIR az (1) bekezdésben említett minden adatcsoport esetében hivatkozást tartalmaz azon uniós információs rendszerekre, amelyekhez az adatok tartoznak.

(3) A CIR-hez hozzáférő hatóságok az uniós információs rendszereket szabályozó jogi eszközökben említett és a nemzeti jog, valamint az e rendelet szerinti hozzáférési jogosultságaikkal összhangban járnak el a hozzáférés során a 20., a 21. és a 22. cikkben említett célokból.

(4) A CIR az (1) bekezdésben említett minden adatcsoport tekintetében hivatkozást tartalmaz az uniós információs rendszerek azon konkrét bejegyzésére, amelyhez az adatok tartoznak.

(5) Az (1) bekezdésben említett adatok tárolásának meg kell felelnie a 37. cikk (2) bekezdésében foglalt minőségi követelményeknek.

## 19. cikk

**Adatok hozzáadása, módosítása és törlése a közös személyazonosítóadat-tárban**

(1) Adatoknak az Eurodacban vagy az ECRIS-TCN-ben történő hozzáadása, módosítása vagy törlése esetén a 18. cikkben említett, a CIR egyéni aktájában tárolt adatokat ennek megfelelően automatikusan ki kell egészíteni, módosítani, vagy törölni kell.

(2) Amennyiben a MID-ben a 32. vagy a 33. cikk szerinti fehér vagy vörös kapcsolatot hoznak létre a CIR-t alkotó két vagy több uniós információs rendszer adatai között, a CIR új egyéni akta létrehozása helyett hozzáadja az új adatokat az összekapcsolt adatok egyéni aktájához.

## 20. cikk

**Hozzáférés a közös személyazonosítóadat-tárhoz személyazonosítás céljából**

(1) A CIR lekérdezését a rendőri hatóság csak az alábbi körülmények között, a (2) és az (5) bekezdésnek megfelelően hajthatja végre:

- a) amennyiben a rendőri hatóság úti okmány vagy az adott személy személyazonosságát hitelt érdemlően igazoló más dokumentum hiányában nem tud azonosítani egy személyt;
- b) amennyiben kétség merül fel a személy által rendelkezésre bocsátott személyazonosító adatokat illetően;
- c) amennyiben kétség merül fel a személy által rendelkezésre bocsátott úti okmány vagy más hitelt érdemlő dokumentum eredetiségét illetően;
- d) amennyiben kétség merül fel az úti okmány vagy más hitelt érdemlő dokumentum birtokosának személyazonosságát illetően; vagy
- e) ha a személy nem tud vagy nem akar együttműködni.

Ilyen lekérdezések 12 év alatti kiskorúak esetében nem végezhetők, kivéve, ha ezt a gyermek mindenek felett álló érdeke megkívánja.

(2) Amennyiben felmerül az (1) bekezdésben felsorolt körülmények egyike és a rendőri hatóságot az (5) bekezdésben említett nemzeti jogalkotási intézkedések arra felhatalmazták, az kizárólag valamely személy azonosítása céljából jogosult a CIR lekérdezésére az illető személy személyazonosságának ellenőrzése során közvetlenül a helyszínen nyert biometrikus adatokkal, amennyiben az eljárást az adott személy jelenlétében kezdeményezték.

(3) Amennyiben a lekérdezés azt jelzi, hogy a CIR tárol az adott személyre vonatkozó adatokat, a rendőri hatóság betekintés céljából hozzáféréssel rendelkezik a 18. cikk (1) bekezdésében említett adatokhoz.

Amennyiben a személy biometrikus adatai nem használhatók, vagy ha az ilyen adatokkal történő lekérdezés sikertelen, a lekérdezést a személy személyazonosító adataival és az útiokmány-adatokkal együttesen, vagy az adott személy által szolgáltatott személyazonosító adatokkal kell elvégezni.

(4) Amennyiben a rendőri hatóságot a (6) bekezdésben említett nemzeti jogalkotási intézkedések felhatalmazzák arra, az adott rendőri hatóság természeti katasztrófa, baleset vagy terrortámadás esetén és kizárólag a személyazonosságukat igazolni nem tudó ismeretlen személyek vagy az azonosítatlan emberi maradványok azonosítása céljából e személyek biometrikus adataival lekérdezheti a CIR-t.

(5) Azok a tagállamok, amelyek élni kívánnak a (2) bekezdésben biztosított lehetőséggel, nemzeti jogalkotási intézkedéseket fogadnak el. Ennek során a tagállamok figyelembe veszik, hogy el kell kerülni a harmadik országok állampolgáraival szembeni mindennemű megkülönböztetést. E jogalkotási intézkedésekben meg kell határozni, hogy a 2. cikk (1) bekezdésének b) és c) pontjában szereplő célkitűzések körén belül melyek a személyazonosítás pontos céljai. A jogalkotási intézkedésekben ki kell jelölni az illetékes rendőri hatóságokat, és meg kell állapítani az ilyen ellenőrzésekre irányadó eljárásokat, feltételeket és kritériumokat.

(6) Azok a tagállamok, amelyek élni kívánnak a (4) bekezdésben foglalt lehetőséggel, nemzeti jogalkotási intézkedéseket fogadnak el, amelyben meghatározzák az eljárásokat, a feltételeket és a kritériumokat.

#### 21. cikk

### **Hozzáférés a közös személyazonosítóadat-tárhoz a többszörös személyazonosság észlelése céljából**

(1) Amennyiben a CIR lekérdezése a 28. cikk (4) bekezdése szerinti sárga kapcsolatot eredményez, a különböző személyazonosságoknak a 29. cikk szerinti manuális ellenőrzéséért felelős hatóság – kizárólag ezen ellenőrzés céljából – hozzáféréssel rendelkezik a sárga kapcsolattal összekapcsolt, CIR-ben tárolt, a 18. cikk (1) és (2) bekezdésében említett adatokhoz.

(2) Amennyiben a CIR lekérdezése a 32. cikk szerinti vörös kapcsolatot eredményez, a 26. cikk (2) bekezdésében említett hatóságok – kizárólag a személyazonossággal való visszaélés elleni küzdelem céljából – hozzáféréssel rendelkeznek a vörös kapcsolattal összekapcsolt, CIR-ben tárolt, a 18. cikk (1) és (2) bekezdésében említett adatokhoz.

#### 22. cikk

### **A közös személyazonosítóadat-tár lekérdezése terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy kivizsgálása céljából**

(1) Konkrét esetekben, amennyiben alapos okkal feltételezhető, hogy az uniós információs rendszerekbe való betekintés hozzájárul a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzéséhez, felderítéséhez vagy nyomozásához, különösen ha fennáll annak a gyanúja, hogy egy terrorista bűncselekmény vagy egyéb súlyos bűncselekmény elkövetésével gyanúsított személy, az ilyen bűncselekmények elkövetője vagy áldozata olyan személy, akinek adatait az Eurodacban tárolják, a kijelölt hatóságok és az Europol betekintheznek a CIR-be azon információ megszerzése érdekében, hogy egy adott személyre vonatkozó adatok szerepelnek-e az Eurodacban.

(2) Amennyiben a lekérdezésre válaszként a CIR azt jelzi, hogy az Eurodacban szerepelnek az adott személyre vonatkozó adatok, a CIR a kijelölt hatóságoknak és az Europolnak a 18. cikk (2) bekezdésében említett hivatkozás formájában ad választ, amely megjelöli, hogy az Eurodac egyező adatokat tartalmaz. A CIR olyan módon ad választ, amely nem veszélyeztetheti az adatbiztonságot.

A választ, amely szerint az adott személyre vonatkozóan szerepelnek adatok az Eurodacban, csak arra a célra lehet felhasználni, hogy hozzáférés iránti kérelmet nyújtsanak be az ilyen hozzáférésre vonatkozó megfelelő jogi eszközökben meghatározott feltételekkel és eljárások révén.

Egyezés vagy többszörös egyezés esetén a kijelölt hatóság vagy az Europol teljes körű hozzáférésre vonatkozó kérelmet nyújt be legalább egy olyan információs rendszerhez, amelyből a lekérdezésre adott válasz egyezést jelez.

Ha kivételesen nem nyújtanak be ilyen teljes körű hozzáférésre irányuló kérelmet, a kijelölt hatóságok a kérelem benyújtásának hiányára vonatkozó indokolást visszakereshető módon rögzítik a nemzeti aktában. Az Europol rögzíti az indokolást a megfelelő aktában.

(3) A terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából az Eurodac-ban tárolt adatokhoz való teljes körű hozzáférés továbbra is az ilyen hozzáférést szabályozó megfelelő jogi eszközökben meghatározott feltételek és eljárások hatálya alá tartozik.

## 23. cikk

**Adatmegőrzés a közös személyazonosítóadat-tárban**

(1) A 18. cikk (1), (2) és (4) bekezdésében említett adatokat az (EU) 2019/816 rendelet adatmegőrzésre vonatkozó rendelkezéseivel összhangban automatikusan törölni kell a CIR-ből.

(2) Az egyéni aktát a CIR-ben csak addig kell, amíg a megfelelő adatokat legalább azon uniós információs rendszerek egyike tárolja, amelyek adatait a CIR tartalmazza. A kapcsolat létrehozása nem befolyásolja az összekapcsolt adatok egyes elemeinek megőrzési időszakát.

## 24. cikk

**Naplóvezetés**

(1) Az (EU) 2019/816 rendelet 29. cikkének sérelme nélkül, az eu-LISA e cikk (2), (3) és (4) bekezdésével összhangban a CIR-ben végzett valamennyi adatkezelési műveletről naplót vezet.

(2) Az eu-LISA a CIR-ben végzett, 20. cikk szerinti minden adatkezelési műveletről naplót vezet. A napló az alábbiakat tartalmazza:

- a) a lekérdezést kezdeményező tagállam vagy uniós ügynökség;
- b) a CIR-ben lekérdezést végző felhasználó hozzáféréseinek célja;
- c) a lekérdezés napja és időpontja;
- d) a lekérdezés kezdeményezéséhez használt adatok típusa;
- e) a lekérdezés eredményei.

(3) Az eu-LISA a CIR-ben végzett, 21. cikk szerinti minden adatkezelési műveletről naplót vezet. A napló az alábbiakat tartalmazza:

- a) a lekérdezést kezdeményező tagállam vagy uniós ügynökség;
- b) a CIR-ben lekérdezést végző felhasználó hozzáféréseinek célja;
- c) a lekérdezés napja és időpontja;
- d) amennyiben kapcsolat jön létre, a lekérdezés kezdeményezéséhez használt adatok és a lekérdezés eredményei azon uniós információs rendszer megjelölésével, amelyből az adatokat kapták.

(4) Az eu-LISA a CIR-ben végzett, 22. cikk szerinti minden adatkezelési műveletről naplót vezet. A napló az alábbiakat tartalmazza:

- a) a lekérdezés napja és időpontja;
- b) a lekérdezés kezdeményezéséhez használt adatok típusa;
- c) a lekérdezés eredményei;
- d) a CIR-ben lekérdezést végző tagállam vagy uniós ügynökség.

Az ilyen hozzáférés nyomán keletkezett naplókat rendszeresen – hat hónapot meg nem haladó időközönként – ellenőrzi az illetékes felügyeleti hatóság az (EU) 2016/680 rendelet 41. cikkével összhangban, vagy az európai adatvédelmi biztos az (EU) 2016/794 rendelet 43. cikkével összhangban annak vizsgálata céljából, hogy az e rendelet 22. cikkének (1) és (2) bekezdésében meghatározott eljárásokat követték-e, és teljesültek-e az ott rögzített feltételek.

(5) Minden tagállam naplót vezet a CIR használatára a 20., a 21. és a 22. cikk alapján megfelelő felhatalmazással rendelkező hatóságai által és e hatóságok megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről. Minden uniós ügynökség naplót vezet a 21. és a 22. cikk alapján megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről.

Ezenkívül a CIR-hez való, 22. cikk szerinti valamennyi hozzáféréssel kapcsolatban minden tagállam naplójában rögzíti a következő adatokat:

- a) a nemzeti ügyiratszám;
- b) a hozzáférés célja;
- c) a nemzeti szabályokkal összhangban a lekérdezést végrehajtó tisztviselő és a lekérdezést elrendelő tisztviselő egyedi felhasználói azonosítója.

(6) Az (EU) 2016/794 rendelettel összhangban, a CIR-hez való, e rendelet 22. cikke szerinti valamennyi hozzáféréssel kapcsolatban az Europol naplójában rögzíti a lekérdezést végrehajtó tisztviselő és a lekérdezést elrendelő tisztviselő egyedi felhasználói azonosítóját.

(7) A (2)–(6) bekezdésben említett naplókat kizárólag az adatvédelmi ellenőrzés érdekében – ideértve a lekérdezés elfogadhatóságának és az adatkezelés jogszerűségének ellenőrzését –, valamint az adatbiztonságnak és az adatok sértetlensége biztosításának céljára lehet felhasználni. E naplókat megfelelő intézkedésekkel kell védeni a jogosulatlan hozzáféréstől, és létrehozásuk után egy évvel törölni kell. Ha azonban egy már megkezdett ellenőrzési eljáráshoz szükség van rájuk, akkor törlésükre akkor kell sort keríteni, amikor már nem szükségesek az ellenőrzési eljáráshoz.

(8) Az eu-LISA az egyéni aktákban megőrzi a tárolt adatok előzményeivel kapcsolatos naplókat. Az eu-LISA az adatok törlése után automatikusan törli ezeket a naplókat.

## V. FEJEZET

### A többszörös személyazonosságot észlelő rendszer

#### 25. cikk

### A többszörös személyazonosságot észlelő rendszer

(1) Létrejön a többszörös személyazonosságot észlelő rendszer (MID), amely létrehozza és tárolja a 34. cikkben említett, személyazonosságot megerősítő dossziékat, tartalmazza az uniós információs rendszerekben – köztük a CIR-ben és a SIS-ben – található adatok közötti kapcsolatokat, és lehetővé teszi a személyazonosság-ellenőrzés megkönnyítése és egyidejűleg a személyazonossággal való visszaélés elleni küzdelem érdekében a többszörös személyazonosságok észlelését; a MID létrehozásának célja a CIR működésének, valamint az EES, a VIS, az ETIAS, az Eurodac, a SIS és az ECRIS-TCN céljainak támogatása.

(2) A MID a következőkből áll:

- a) a kapcsolatokat és az uniós információs rendszerekre való hivatkozásokat tároló központi infrastruktúra;
- b) egy biztonságos kommunikációs infrastruktúra, amely a többszörös személyazonosságot felismerő rendszert összekapcsolja a SIS-szel, valamint az ESP és a CIR központi infrastruktúráival.

(3) Az eu-LISA kifejleszti a MID-et, és gondoskodik annak műszaki irányításáról.

#### 26. cikk

### Hozzáférés a többszörös személyazonosságot észlelő rendszerhez

(1) A különböző személyazonosságok 29. cikkben említett manuális ellenőrzése céljából a MID-ben tárolt, a 34. cikkben említett adatokhoz az alábbiaknak kell hozzáférést adni:

- a) a figyelmeztető jelzést az (EU) 2018/1862 rendelettel összhangban létrehozó vagy frissítő tagállam SIRENE-irodája;
- b) az ítélethozatal szerinti tagállam központi hatóságai, amikor azok az (EU) 2019/816 rendelet 5. vagy 9. cikkével összhangban adatokat visznek be vagy módosítanak az ECRIS-TCN-ben.

(2) A CIR-ben vagy a SIS-ben szereplő legalább egy uniós információs rendszerhez hozzáféréssel rendelkező tagállami hatóságok és uniós ügynökségek hozzáférést kapnak a 34. cikk a) és b) pontjában említett valamennyi, a 32. cikk szerinti vörös kapcsolatra vonatkozó adathoz.

(3) A tagállami hatóságok és az uniós ügynökségek hozzáférést kapnak a 33. cikk szerinti fehér kapcsolatokhoz, amennyiben hozzáféréssel rendelkeznek ahhoz a két uniós információs rendszerhez, amelyek tartalmazzák azokat az adatokat, amelyek között a fehér kapcsolat létrejött.

(4) A tagállami hatóságok és uniós ügynökségek hozzáférést kapnak a 31. cikk szerinti zöld kapcsolatokhoz, amennyiben hozzáféréssel rendelkeznek ahhoz a két uniós információs rendszerhez, amelyek tartalmazzák azokat az adatokat, amelyek között a zöld kapcsolat létrejött, és amennyiben az említett információs rendszerek lekérdezése egyezést eredményezett az összekapcsolt két adatscsoport között.

## 27. cikk

**A többszörös személyazonosság észlelése**

(1) A többszörös személyazonosság észlelése céljából keresést kell kezdeményezni a CIR-ben és a SIS-ben, ha:

- a) a SIS-ben az (EU) 2018/1862 rendelet VI–X. fejezetével összhangban egy személyre vonatkozó figyelmeztető jelzést hoznak létre vagy frissítenek;
- b) az ECRIS-TCN-ben az (EU) 2019/816 rendelet 5. vagy 9. cikkével összhangban adatrekordot rögzítenek vagy frissítenek;

(2) Amennyiben az (1) bekezdésben említett valamely uniós információs rendszerben található adatok biometrikus adatokat tartalmaznak, a CIR és a központi SIS a közös BMS-t használja a többszörös személyazonosság észlelése céljából. A közös BMS összehasonlítja a bármely új biometrikus adatokból nyert biometrikus sablonokat a közös BMS-ben már szereplő biometrikus sablonokkal annak ellenőrzése érdekében, hogy ugyanazon személy adatai már szerepelnek-e a CIR-ben vagy a központi SIS-ben.

(3) A (2) bekezdésben említett folyamaton túlmenően a CIR és a központi SIS az ESP-t használja a központi SIS-ben, illetve a CIR-ben tárolt adatok lekérdezésére a következő adatok felhasználásával:

- a) vezetéknevek, utónevek, születési nevek, korábban használt nevek és álnevek, születési hely, születési idő, nem és állampolgárságok az (EU) 2018/1862 rendelet 20. cikkének (3) bekezdésében említettek szerint;
- b) vezetéknev (családi név), utónevek (kereszt), születési idő, születési hely (város és ország), állampolgárság vagy állampolgárságok és nem az (EU) 2019/816 rendelet 5. cikke (1) bekezdésének a) pontjában említettek szerint.

(4) A (2) és a (3) bekezdésben említett folyamaton túlmenően a CIR és a központi SIS az ESP-t használja a központi SIS-ben, illetve a CIR-ben tárolt adatok keresésére az útiokmány-adatok felhasználásával.

(5) A többszörös személyazonosság észlelésére irányuló vizsgálat csak valamely uniós információs rendszerben rendelkezésre álló adatoknak más uniós információs rendszerekben rendelkezésre álló adatokkal való összehasonlítása céljából kezdeményezhető.

## 28. cikk

**A többszörös azonosság észlelésére irányuló vizsgálat eredményei**

(1) Amennyiben a 27. cikk (2), (3) és (4) bekezdése szerinti lekérdezések nem eredményeznek egyezést, a 27. cikk (1) bekezdésében szereplő eljárások az azokat szabályozó jogi eszközöknek megfelelően folytatódnak.

(2) Amennyiben a 27. cikk (2), (3) és (4) bekezdése szerinti lekérdezés egy vagy több egyezést eredményez, a CIR, és ha releváns, a SIS kapcsolatot hoz létre a lekérdezés kezdeményezéséhez használt adatok és a velük egyezést mutató adatok között.

Amennyiben a lekérdezés többszörös egyezést eredményez, az egymással egyezést mutató összes adat között kapcsolat jön létre. Ha az adatokat előzőleg már összekapcsolták, a meglévő kapcsolatot ki kell terjeszteni a lekérdezés kezdeményezéséhez használt adatokra.

(3) Amennyiben a 27. cikk (2), (3) és (4) bekezdése szerinti lekérdezés egy vagy több egyezést eredményez, és az összekapcsolt fájlokban szereplő személyazonosító adatok azonosak vagy hasonlóak, a 33. cikknek megfelelően fehér kapcsolat jön létre.

(4) Amennyiben a 27. cikk (2), (3) és (4) bekezdése szerinti lekérdezés egy vagy több egyezést eredményez, és az összekapcsolt fájlokban szereplő személyazonosító adatok nem tekinthetők hasonló adatoknak, a 30. cikknek megfelelően sárga kapcsolat jön létre, és a 29. cikkben említett eljárást kell alkalmazni.

(5) A Bizottság a 69. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogad el annak megállapítására irányuló eljárások meghatározására vonatkozóan, hogy a személyazonosító adatok mely esetekben tekintendők azonos vagy hasonló adatoknak.

(6) A kapcsolatokat a 34. cikkben említett, személyazonosságot megerősítő dossziében kell tárolni.

(7) A Bizottság az eu-LISA-val együttműködve végrehajtási jogi aktusok útján megállapítja a különböző uniós információs rendszerekből származó adatok közötti kapcsolatok létrehozására vonatkozó technikai szabályokat. Ezeket a végrehajtási jogi aktusokat a 70. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

## 29. cikk

**A különböző személyazonosságok manuális ellenőrzése és a felelős hatóságok**

(1) A (2) bekezdés sérelme nélkül, a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság a következő:

- a) a tagállam SIRENE-irodája azon egyezések vonatkozásában, amelyek a SIS figyelmeztető jelzésnek az (EU) 2018/1862 rendelet szerinti létrehozása vagy frissítése során következtek be;
- b) az ítélethozatal szerinti tagállam központi hatóságai, az (EU) 2019/816 rendelet 5. vagy 9. cikkével összhangban adatoknak az ECRIS-TCN-be történő bevitelkor vagy azok módosításakor bekövetkezett egyezések vonatkozásában.

A MID a személyazonosságot megerősítő dossziében megjelöli a különböző személyazonosságok manuális ellenőrzéséért felelős hatóságot.

(2) A személyazonosságot megerősítő dossziében szereplő, különböző személyazonosságok manuális ellenőrzéséért felelős hatóság a figyelmeztető jelzést kibocsátó tagállam SIRENE-irodája, amennyiben kapcsolatot hoznak létre az alábbi adatokkal:

- a) átadási vagy kiadási letartóztatás céljából körözött személyekre vonatkozó figyelmeztető jelzésben szereplő adatok, az (EU) 2018/1862 rendelet 26. cikkének megfelelően;
- b) eltűnt vagy különleges bánásmódot igénylő személyekre vonatkozó figyelmeztető jelzésben szereplő adatok, az (EU) 2018/1862 rendelet 32. cikkének megfelelően;
- c) bírósági eljárásban való közreműködés céljából keresett személyekre vonatkozó figyelmeztető jelzésben szereplő adatok, az (EU) 2018/1862 rendelet 34. cikkének megfelelően;
- d) rejtett ellenőrzés, kikérdezés vagy célzott ellenőrzés céljából keresett személyekre vonatkozó figyelmeztető jelzésben szereplő adatok, az (EU) 2018/1862 rendelet 36. cikkének megfelelően.

(3) A különböző személyazonosságok manuális ellenőrzéséért felelős hatóság hozzáféréssel rendelkezik a releváns, személyazonosságot megerősítő dossziében szereplő összekapcsolt adatokhoz, valamint a CIR-ben és – adott esetben – a SIS-ben összekapcsolt személyazonosító adatokhoz. A hatóság késedelem nélkül megvizsgálja a különböző személyazonosságokat. A vizsgálat végeztével a 31., a 32. és a 33. cikkkel összhangban frissíti a kapcsolatot, és haladéktalanul hozzáadja a személyazonosságot megerősítő dossziéhez.

(4) Ha egynél több kapcsolat jön létre, a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság mindegyiket külön-külön értékeli.

(5) Ha az egyezést jelző adatokat már összekapcsolták, a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság figyelembe veszi a meglévő kapcsolatokat, amikor új kapcsolatokat létrehozását értékeli.

## 30. cikk

**Sárga kapcsolat**

(1) Ha különböző személyazonosságok manuális ellenőrzésére még nem került sor, a két vagy több uniós információs rendszerben szereplő adatok közötti kapcsolatot a következő esetek bármelyikében sárga kapcsolatként kell besorolni:

- a) az összekapcsolt adatok azonos biometrikus adatokat, de hasonló vagy eltérő személyazonosító adatokat tartalmaznak;
- b) az összekapcsolt adatok eltérő személyazonosító adatokat, de azonos útiokmány-adatokat tartalmaznak, és legalább az uniós információs rendszerek egyike nem tartalmaz az érintett személyre vonatkozó biometrikus adatokat;
- c) az összekapcsolt adatok azonos személyazonosító adatokat, de eltérő biometrikus adatokat tartalmaznak;
- d) az összekapcsolt adatok hasonló vagy eltérő személyazonosító adatokat azonos útiokmány-adatokat, de eltérő biometrikus adatokat tartalmaznak.

(2) Amennyiben egy kapcsolatot az (1) bekezdéssel összhangban sárga kapcsolatként soroltak be, a 29. cikkben megállapított eljárást kell alkalmazni.

## 31. cikk

**Zöld kapcsolat**

- (1) A két vagy több uniós információs rendszerből származó adatok közötti kapcsolatot zöldnek kell minősíteni, ha:
- a) az összekapcsolt adatok eltérő biometrikus adatokat, de azonos személyazonosító adatokat tartalmaznak, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy az összekapcsolt adatok két különböző személyt jelölnek;
  - b) az összekapcsolt adatok eltérő biometrikus adatokat, hasonló vagy eltérő személyazonosító adatokat és azonos útiokmány-adatokat tartalmaznak, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy az összekapcsolt adatok két különböző személyt jelölnek;
  - c) az összekapcsolt adatok eltérő személyazonosító adatokat, de azonos útiokmány-adatokat tartalmaznak, és az uniós információs rendszerek közül legalább az egyik nem tartalmazza az érintett személyre vonatkozó biometrikus adatokat, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy az összekapcsolt adatok két különböző személyt jelölnek.
- (2) A CIR vagy a SIS lekérdezésekor, ha az uniós információs rendszerek közül kettő vagy több rendszerben szereplő adatok között zöld kapcsolat áll fenn, a MID jelzi, hogy az összekapcsolt adatok között szereplő személyazonosító adatok nem ugyanarra a személyre vonatkoznak.
- (3) Ha egy tagállami hatóságnak arra utaló bizonyítéka van, hogy a MID-ben hibásan rögzítették a zöld kapcsolatot, vagy az nem naprakész, illetve hogy az adatokat a MID-ben vagy az uniós információs rendszerekben e rendelet megsértve kezelték, a hatóság ellenőrzi CIR-ben és a SIS-ben tárolt vonatkozó adatokat, és szükség esetén haladéktalanul helyesbíti vagy törli a kapcsolatot a MID-ből. Az említett tagállami hatóság haladéktalanul tájékoztatja a különböző személyazonosságok manuális ellenőrzéséért felelős tagállamot.

## 32. cikk

**Vörös kapcsolat**

- (1) A két vagy több uniós információs rendszerben szereplő adatok közötti kapcsolatot a következő esetek bármelyikében vörös kapcsolatként kell besorolni:
- a) az összekapcsolt adatok azonos biometrikus adatokat, de hasonló vagy eltérő személyazonosító adatokat tartalmaznak, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy az összekapcsolt adatok – nem indokolt módon – ugyanazt a személyt jelölik;
  - b) az összekapcsolt adatok azonos, hasonló vagy eltérő személyazonosító adatokat, azonos útiokmány-adatokat, de eltérő biometrikus adatokat tartalmaznak, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy ezek az adatok két különböző személyt jelölnek, akik közül legalább az egyik nem indokolt módon ugyanazt az úti okmányt használja;
  - c) az összekapcsolt adatok azonos személyazonosító adatokat, de eltérő biometrikus adatokat tartalmaznak, és az úti okmány-adatok eltérőek vagy nem állnak rendelkezésre, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy ezek az adatok nem indokolt módon két különböző személyt jelölnek;
  - d) az összekapcsolt adatok eltérő személyazonosító adatokat, de azonos útiokmány-adatokat tartalmaznak, az uniós információs rendszerek közül legalább az egyik nem tartalmaz az érintett személyre vonatkozó biometrikus adatokat, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy ezek az adatok nem indokolt módon ugyanazt a személyt jelölik.
- (2) A CIR vagy a SIS lekérdezésekor, és ha az uniós információs rendszerek közül kettő vagy több rendszerben szereplő adatok között vörös kapcsolat áll fenn, a MID megjelöli a 34. cikkben említett adatokat. A vörös kapcsolat nyomon követése az uniós és a nemzeti joggal összhangban történik, oly módon, hogy az érintett személyt terhelő jogkövetkezmények kizárólag az adott személyre vonatkozó adatokon alapulhatnak. Kizárólag a vörös kapcsolat meglétéből nem származhat semmilyen, az érintett személyt terhelő jogkövetkezmény.
- (3) Ha az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban vagy az ECRIS-TCN-ben szereplő adatok között vörös kapcsolat jön létre, a CIR-ben tárolt egyéni aktát a 19. cikk (2) bekezdésében foglaltak szerint frissíteni kell.



(4) A SIS-be bevitt figyelmeztető jelzések kezelésére vonatkozó, az (EU) 2018/1860, az (EU) 2018/1861 és az (EU) 2018/1862 rendeletben foglalt rendelkezések sérelme nélkül, valamint a biztonság és a közrend védelme, a bűncselekmények megelőzése, és a nemzeti nyomozások veszélyeztetésének megakadályozása érdekében szükséges korlátozások sérelme nélkül, vörös kapcsolat létrehozása esetén a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság tájékoztatja az érintett személyt arról, hogy több jogellenes személyazonosító adat létezik, és a személlyel közli az e rendelet 34. cikkének c) pontjában említett egységes azonosító számot, az e rendelet 34. cikkének d) pontjában említett, különböző személyazonosságok manuális ellenőrzéséért felelős hatóságra való hivatkozást és az e rendelet 49. cikkével összhangban létrehozott webportál internetes címét.

(5) A (4) bekezdésben említett információkat szabványos formanyomtatványon keresztül a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság írásban közli. A Bizottság végrehajtási jogi aktusok révén határozza meg az említett formanyomtatvány tartalmát és formáját. Ezeket a végrehajtási jogi aktusokat a 70. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(6) Vörös kapcsolat létrehozása esetén a MID automatikusan értesítést küld az összekapcsolt adatokért felelős hatóságoknak.

(7) Ha egy, a CIR-hez vagy a SIS-hez hozzáféréssel rendelkező tagállami hatóságnak vagy uniós ügynökségnek arra utaló bizonyítéka van, hogy a MID-ben hibásan rögzítették a vörös kapcsolatot, vagy hogy az adatokat a MID-ben, a CIR-ben vagy a SIS-ben e rendeletet megsértve kezelték, az említett hatóság vagy ügynökség ellenőrzi a CIR-ben és a SIS-ben tárolt vonatkozó adatokat és:

- a) amennyiben a kapcsolat a 29. cikk (2) bekezdésében említett SIS figyelmeztető jelzések egyikéhez kapcsolódik, haladéktalanul tájékoztatja a SIS figyelmeztető jelzést kibocsátó tagállam illetékes SIRENE-irodáját;
- b) minden más esetben haladéktalanul helyesbíti vagy törli a MID-ből a kapcsolatot.

Amennyiben a SIRENE-irodával az első albekezdés a) pontja alapján felveszik a kapcsolatot, az iroda ellenőrzi a tagállam hatósága vagy az uniós ügynökség által benyújtott bizonyítékot, és adott esetben haladéktalanul helyesbíti vagy törli a kapcsolatot a MID-ből.

A bizonyítékot megszerző tagállami hatóság haladéktalanul tájékoztatja a különböző személyazonosságok manuális ellenőrzéséért felelős tagállami hatóságot a vörös kapcsolat esetleges releváns helyesbítéséről vagy törléséről.

### 33. cikk

#### Fehér kapcsolat

(1) A két vagy több uniós információs rendszerben szereplő adatok közötti kapcsolatot a következő esetek bármelyikében fehér kapcsolatként kell besorolni:

- a) az összekapcsolt adatok azonos biometrikus adatokat és azonos vagy hasonló személyazonosító adatokat tartalmaznak;
- b) az összekapcsolt adatok azonos vagy hasonló személyazonosító adatokat, azonos útiokmány-adatokat tartalmaznak, és legalább az uniós információs rendszerek egyike nem tartalmaz az érintett személyre vonatkozó biometrikus adatokat;
- c) az összekapcsolt adatok azonos biometrikus adatokat, azonos útiokmány-adatokat, és hasonló személyazonosító adatokat tartalmaznak;
- d) az összekapcsolt adatok azonos biometrikus adatokat, de hasonló vagy eltérő személyazonosító adatokat tartalmaznak, és a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság arra a megállapításra jutott, hogy az összekapcsolt adatok– indokolt módon– ugyanazt a személyt jelölik;

(2) A CIR vagy a SIS lekérdezésekor, ha az uniós információs rendszerek közül két vagy több rendszerben szereplő adatok között fehér kapcsolat áll fenn, a MID jelzi, hogy az összekapcsolt adatok között szereplő személyazonosító adatok ugyanannak a személynek felelnek meg. A lekérdezett uniós információs rendszerek olyan választ adnak, amely a személyre vonatkozó valamennyi összekapcsolt adatot feltünteti, amennyiben azok relevánsak, és így egyezést eredményez a fehér kapcsolat által összekapcsolt adatok között, amennyiben a lekérdezést kezdeményező hatóság az uniós vagy a nemzeti jog alapján hozzáféréssel rendelkezik az összekapcsolt adatokhoz.

(3) Ha az EES-ben, a VIS-ben, az ETIAS-ban, az Eurodacban vagy az ECRIS-TCN-ben szereplő adatok között fehér kapcsolatot hoznak létre, a CIR-ben tárolt egyéni aktát a 19. cikk (2) bekezdésében foglaltak szerint frissíteni kell.

(4) A SIS-be bevitt figyelmeztető jelzések kezelésére vonatkozó, az (EU) 2018/1860, az (EU) 2018/1861 és az (EU) 2018/1862 rendeletekben foglalt rendelkezések sérelme nélkül, valamint a biztonság és a közrend védelme, a bűncselekmények megelőzése, és a nemzeti nyomozások veszélyeztetésének megakadályozása érdekében szükséges korlátozások sérelme nélkül, ha a különböző személyazonosságok manuális ellenőrzését követően fehér kapcsolatot hoznak létre, a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság tájékoztatja az érintett személyt arról, hogy több hasonló vagy különböző személyazonosító adat áll fenn, és a személlyel közli az e rendelet 34. cikkének c) pontjában említett egységes azonosító számot, az e rendelet 34. cikkének d) pontjában említett, különböző személyazonosságok manuális ellenőrzéséért felelős hatóságra való hivatkozást és az e rendelet 49. cikkével összhangban létrehozott webportál internetes címét.

(5) Ha egy tagállami hatóságnak arra utaló bizonyítéka van, hogy a MID-ben hibásan rögzítették a fehér kapcsolatot, vagy hogy a fehér kapcsolat nem naprakész, vagy hogy az adatokat a MID-ben vagy az uniós információs rendszerekben e rendeletet megsértve kezelték, a hatóság ellenőrzi CIR-ben és a SIS-ben tárolt vonatkozó adatokat, és szükség esetén haladéktalanul helyesbíti vagy törli a kapcsolatot a MID-ből. Az említett tagállami hatóság haladéktalanul tájékoztatja a különböző személyazonosságok manuális ellenőrzéséért felelős tagállamot.

(6) A (4) bekezdésben említett információkat szabványos formanyomtatványon keresztül a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság írásban közli. A Bizottság végrehajtási jogi aktusok révén meghatározza az említett formanyomtatvány tartalmát és formáját. Ezeket a végrehajtási jogi aktusokat a 70. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

#### 34. cikk

### A személyazonosságot megerősítő dosszié

A személyazonosságot megerősítő dosszié a következő adatokat tartalmazza:

- a) a 30–33. cikkben szereplő kapcsolatok,
- b) hivatkozás azokra az uniós információs rendszerekre, amelyekben az összekapcsolt adatok szerepelnek;
- c) egységes azonosító szám, amely lehetővé teszi az összekapcsolt adatok lehívását a megfelelő uniós információs rendszerekből;
- d) a különböző személyazonosságok manuális ellenőrzéséért felelős hatóság;
- e) a kapcsolat létrehozásának vagy bármely frissítésének időpontja.

#### 35. cikk

### Adatmegőrzés a többszörös személyazonosságot észlelő rendszerben

A személyazonosságot megerősítő dossziékat és az azokban szereplő adatokat – beleértve a kapcsolatokat is – csak addig lehet tárolni a MID-ben, amíg az összekapcsolt adatok szerepelnek két vagy több uniós információs rendszerben. Ezeket az adatokat automatikusan törölni kell a MID-ből.

#### 36. cikk

### Naplóvezetés

(1) Az eu-LISA-nak a MID-ben végzett összes adatkezelési műveletről naplót kell vezetnie. A napló az alábbiakat tartalmazza:

- a) a lekérdezést kezdeményező tagállamot;
- b) a felhasználó hozzáféréseinek célját;
- c) a lekérdezés napját és időpontját;
- d) a lekérdezés kezdeményezéséhez használt adatok típusát;
- e) az összekapcsolt adatokra való utalást;
- f) a személyazonosságot megerősítő dosszié előzményeit.

(2) Minden tagállam naplót vezet a MID használatára megfelelő felhatalmazással rendelkező hatóságai által és e hatóságok megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről. Minden uniós ügynökség naplót vezet a megfelelő felhatalmazással rendelkező személyi állománya által végzett lekérdezésekről,

(3) Az (1) és a (2) bekezdésben említett naplókat kizárólag az adatvédelmi ellenőrzés érdekében – ideértve a lekérdezés elfogadhatóságának és az adatkezelés jogszerűségének ellenőrzését –, valamint az adatbiztonság és az adatok sérthetatlensége biztosításának céljára lehet felhasználni. E naplókat megfelelő intézkedésekkel kell védeni a jogosulatlan hozzáféréstől, és létrehozásuk után egy évvel törölni kell. Ha azonban egy már megkezdett ellenőrzési eljáráshoz szükség van rájuk, akkor törlésükre akkor kell sort keríteni, amikor már nem szükségesek az ellenőrzési eljáráshoz.

## VI FEJEZET

### Az interoperabilitást támogató intézkedések

#### 37. cikk

#### Adatminőség

(1) A tagállamoknak a rendszerbe bevitt adatok minőségével kapcsolatos felelősségének sérelme nélkül az eu-LISA az adatminőség ellenőrzésére irányuló automatizált mechanizmusokat és eljárásokat dolgoz ki a SIS-ben, az Eurodacban, az ECRIS-TCN-ben, a közös BMS-ben és a CIR-ben tárolt adatokra vonatkozóan.

(2) Az eu-LISA mechanizmusokat hajt végre a közös BMS pontosságának értékelésére, valamint közös adatminőségi mutatókat és minőségi minimumkövetelményeket a SIS-ben, az Eurodacban, az ECRIS-TCN-ben, a közös BMS-ben és a CIR-ben szereplő adatok tárolására vonatkozóan.

Kizárólag a minőségi minimumkövetelményeknek megfelelő adatok vihetők be a SIS-be, az Eurodacba, az ECRIS-TCN-be, a közös BMS-be, a CIR-be és a MID-be.

(3) Az eu-LISA a tagállamok részére rendszeresen jelentést készít az adatminőség ellenőrzésére irányuló automatizált mechanizmusokról és eljárásokról, valamint a közös adatminőségi mutatókról. Az eu-LISA a Bizottság részére is rendszeresen jelentést készít a felmerült problémákról és az érintett tagállamokról. Az eu-LISA ezt a jelentést kérelemre eljuttatja az Európai Parlamentnek és a Tanácsnak is. Az e bekezdés értelmében készült jelentések nem tartalmazhatnak személyes adatokat.

(4) Az adatminőség ellenőrzésére irányuló automatizált mechanizmusok és eljárások részleteit, valamint a SIS-ben, az Eurodacban, az ECRIS-TCN-ben, a közös BMS-ben és a CIR-ben szereplő adatok tárolására vonatkozó közös adatminőségi mutatók és minőségi minimumkövetelmények részleteit végrehajtási jogi aktusokban kell meghatározni. Ezeket a végrehajtási jogi aktusokat a 70. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(5) A Bizottság az adatminőség ellenőrzésére irányuló automatizált mechanizmusok és eljárások, valamint a közös adatminőségi követelmények és az adatminőségi minimumkövetelmények megállapítása után egy évvel, majd azt követően évente értékeli az adatminőség tagállamok általi végrehajtását, és szükség esetén ajánlásokat tesz. A tagállamok cselekvési tervet nyújtanak be a Bizottságnak az értékelő jelentésben esetlegesen feltárt hiányosságok – és különösen az uniós információs rendszerekben szereplő téves adatokból származó adatminőségi problémák – orvoslására. A tagállamok rendszeresen jelentést tesznek a Bizottságnak a cselekvési terv tekintetében elért minden előrehaladásról a cselekvési terv maradéktalan végrehajtásáig.

A Bizottság továbbítja az értékelő jelentést az Európai Parlamentnek, a Tanácsnak, az európai adatvédelmi biztosnak, az Európai Adatvédelmi Testületnek és az Európai Unió Alapjogi Ügynökségének, amelyet a 168/2007/EK tanácsi rendelet <sup>(37)</sup> hozott létre.

#### 38. cikk

#### Egységes üzenetformátum

(1) Létrejön az egységes üzenetformátum (UMF) szabvány. Az UMF a bel- és igazságügy területén működő információs rendszerek, hatóságok vagy szervezetek közötti, határokon átnyúló információcseré bizonyos tartalmi elemeire vonatkozó szabványokat határoz meg.

<sup>(37)</sup> A Tanács 168/2007/EK rendelete (2007. február 15.) az Európai Unió Alapjogi Ügynökségének létrehozásáról (HL L 53., 2007.2.22., 1. o.).

(2) Az UMF szabványt kell használni az Eurodac, az ECRIS-TCN, az ESP, a CIR, a MID, és adott esetben a bel- és igazságügy területén működő bármely új információcseré-modellnek és információs rendszernek az eu-LISA vagy más uniós ügynökség által történő kidolgozása során.

(3) A Bizottság végrehajtási jogi aktust fogad el az e cikk (1) bekezdésében szereplő UMF szabvány meghatározása és kidolgozása céljából. Ezeket a végrehajtási jogi aktusokat a 70. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

### 39. cikk

#### A jelentések és statisztikák központi adattára

(1) A SIS-t, az Eurodacot és az ECRIS-TCN-t szabályozó jogi eszközökkel összhangban e rendszerek célkitűzéseinek támogatása, valamint a rendszerek közötti statisztikai adatok és elemzési jelentések szakpolitikai, működési és adatminőségi célokból történő biztosítása érdekében létrejön a jelentések és statisztikák központi adattára (CRRS).

(2) A CRRS-t, amely az (EU) 2018/1862 rendelet 74. cikkében és az (EU) 2019/816 rendelet 32. cikkében említett adatokat és statisztikákat uniós információs rendszerek szerint logikailag különválasztva tartalmazza, az eu-LISA hozza létre, vezeti be és üzemelteti technikai helyszínein. A CRRS-hez és ellenőrzött és biztonságos módon, egyedi felhasználói profilokkal, kizárólag jelentések és statisztikák készítése céljából lehet hozzáférést biztosítani az (EU) 2018/1862 rendelet 74. cikkében és az (EU) 2019/816 rendelet 32. cikkében említett hatóságok számára.

(3) Az eu-LISA anonimizálja az adatokat, és az ilyen anonimizált adatokat rögzíti a CRRS-ben. Az adatok anonimizálása automatizált módon történik.

A CRRS-ben szereplő adatok nem tehetik lehetővé az egyének azonosítását.

(4) A CRRS a következő elemekből áll:

- a) az adatok anonimizálásához szükséges eszközök;
- b) az anonim adatok adattárából álló központi infrastruktúra;
- c) egy biztonságos kommunikációs infrastruktúra a CRRS-nek a SIS-szel, az Eurodac-kal és az ECRIS-TCN-nel, valamint a közös BMS-szel, a CIR-rel és a MID központi infrastruktúráival való összekapcsolása céljából.

(5) A Bizottság a 69. cikknek megfelelően felhatalmazáson alapuló jogi aktust fogad el a CRRS működésére irányuló részletes szabályok megállapítására vonatkozóan, beleértve az e cikk (2) és (3) bekezdésében említett személyes adatok kezelésére vonatkozó különleges biztosítékokat, és az adattárra vonatkozó biztonsági szabályokat.

## VII. FEJEZET

### Adatvédelem

#### 40. cikk

#### Az adatkezelő

(1) A személyes adatoknak a közös BMS keretében történő kezelése tekintetében a tagállamok azon hatóságai, amelyek az Eurodac, a SIS és az ECRIS-TCN vonatkozásában adatkezelőnek minősülnek, az (EU) 2016/679 rendelet 4. cikkének 7. pontja vagy az (EU) 2016/680 irányelv 3. cikkének 8. pontja szerinti adatkezelőnek tekintendők az e rendelet 13. cikkében említett olyan adatokból nyert biometrikus sablonok tekintetében is, amelyeket ők visznek be az alapul szolgáló rendszerekbe, valamint felelősek a biometrikus sablonok közös BMS keretében történő kezeléséért.

(2) A személyes adatoknak CIR-ben történő kezelése tekintetében a tagállamok azon hatóságai, amelyek az Eurodac és az ECRIS-TCN vonatkozásában adatkezelőnek minősülnek, az (EU) 2016/679 rendelet 4. cikkének 7. pontja vagy az (EU) 2016/680 irányelv 3. cikkének 8. pontja szerinti adatkezelőnek tekintendők az e rendelet 18. cikkében említett olyan adatok tekintetében, amelyeket ők visznek be az alapul szolgáló rendszerekbe, valamint felelősek az említett személyes adatok CIR-ben történő kezeléséért.

(3) Az adatok MID keretében történő kezelése tekintetében:

- a) a személyes adatok ETIAS központi egysége általi feldolgozása tekintetében az Európai Határ- és Partvédelmi Ügynökség tekintendő az (EU) 2018/1725 rendelet 3. cikkének 8. pontja szerinti adatkezelőnek;
- b) a személyazonosságot megerősítő dossziéhoz adatokat hozzáadó vagy abban adatokat módosító tagállami hatóságok tekintendők az (EU) 2016/679 rendelet 4. cikkének 7. pontja vagy az (EU) 2016/680 irányelv 3. cikkének 8. pontja szerinti adatkezelőnek, és felelősek a személyes adatok MID-ben történő kezeléséért.

(4) Az adatvédelem – többek között a lekérdezés elfogadhatóságának és az adatkezelés jogszerűségének – ellenőrzése céljából az adatkezelők a 44. cikkben említetteknek megfelelően önellenőrzés céljából hozzáféréssel rendelkeznek a 10., a 16., a 24. és a 36. cikkben említett naplókhoz.

#### 41. cikk

### Az adatfeldolgozó

A közös BMS-ben, a CIR-ben és a MID-ben tárolt személyes adatok kezelése tekintetében az eu-LISA minősül az (EU) 2018/1725 rendelet 3. cikke 12. pontjának a) alpontja szerinti adatfeldolgozónak.

#### 42. cikk

### Az adatkezelés biztonsága

(1) Az eu-LISA, az ETIAS központi egysége, az Europol és a tagállami hatóságok biztosítják a személyes adatok e rendelet alapján történő kezelésének biztonságát. Az eu-LISA, az ETIAS központi egysége, az Europol és a tagállami hatóságok együttműködnek a biztonsággal kapcsolatos feladatok ellátása során.

(2) Az (EU) 2018/1725 rendelet 33. cikkének sérelme nélkül, az eu-LISA megteszi az interoperabilitási elemek és a hozzájuk kapcsolódó kommunikációs infrastruktúra biztonságának garantálásához szükséges intézkedéseket.

(3) Az eu-LISA különösen elfogadja a szükséges intézkedéseket, többek között egy biztonsági tervet, egy üzletmenet-folytonossági és katasztrófa-elhárítási tervet annak érdekében, hogy:

- a) fizikai adatvédelmet valósítson meg, többek között a kritikus infrastruktúra védelmére irányuló vészhelyzeti tervek kidolgozása által;
- b) megtagadja a jogosulatlan személyek hozzáférését az adatkezelő eszközökhöz és berendezésekhez;
- c) megakadályozza az adathordozók jogosulatlan olvasását, másolását, módosítását vagy eltávolítását;
- d) megakadályozza az adatok jogosulatlan bevitelét és a rögzített személyes adatok jogosulatlan ellenőrzését, módosítását vagy törlését;
- e) megakadályozza az adatok jogosulatlan kezelését, valamint jogosulatlan másolását, módosítását vagy törlését;
- f) megakadályozza az automatizált adatkezelő rendszerek jogosulatlan személyek általi, adatátviteli berendezés útján történő használatát;
- g) biztosítsa, hogy az interoperabilitási elemekhez való hozzáférésre jogosult személyek csak a hozzáférési jogosultságuk körébe tartozó adatokhoz férjenek hozzá, mégpedig kizárólag egyéni felhasználói azonosítókkal és titkos hozzáférési módszerekkel;
- h) biztosítsa, hogy ellenőrizhető és megállapítható legyen, hogy az adatátviteli berendezések használatával mely szerverekhez lehet személyes adatokat továbbítani;
- i) biztosítsa, hogy ellenőrizhető és megállapítható legyen, hogy ki, mikor, mely adatokat és milyen célból kezelt az interoperabilitási elemekben;
- j) megakadályozza a személyes adatoknak az interoperabilitási elemekbe vagy azokból történő továbbítása vagy adathordozón történő szállítása során a személyes adatok jogosulatlan olvasását, másolását, módosítását vagy törlését, különösen a megfelelő titkosítási technikák révén;
- k) biztosítsa, hogy üzemzavar esetén helyreállítható legyen a telepített rendszerek normál működése;
- l) garantálja a megbízhatóságot azzal, hogy biztosítja, hogy az interoperabilitási elemek működése során fellépő hibákat minden esetben megfelelően bejelentik;
- m) figyelemmel kíséri az e bekezdésben említett biztonsági intézkedések eredményességét, és megtegye a belső ellenőrzéssel kapcsolatban szükséges szervezeti intézkedéseket az e rendeletnek való megfelelés biztosítása érdekében, továbbá az új technológiai fejlesztések fényében értékeli az említett biztonsági intézkedéseket.

(4) A tagállamok, az Europol és az ETIAS központi egysége a (3) bekezdésben említettekkel egyenértékű intézkedéseket hoznak a személyes adatok azon hatóságok általi kezelése tekintetében, amelyek hozzáférésre jogosultak bármely interoperabilitási elemhez.

## 43. cikk

**Biztonsági incidensek**

(1) Biztonsági incidensnek kell tekinteni bármely olyan eseményt, amely kihatással van vagy lehet az interoperabilitási elemek biztonságára és kárt vagy veszteséget okozhat a bennük tárolt adatokban, különösen akkor, ha az adatokhoz jogosulatlan hozzáférés történt, vagy az adatok rendelkezésre állása, sértetlensége, illetve bizalmas jellege kárt szenvedett vagy szenvedhetett.

(2) A biztonsági incidenseket gyors, hatékony és megfelelő reagálással kell kezelni.

(3) A személyes adatok megsértésének az (EU) 2016/679 rendelet 33. cikke, az (EU) 2016/680 irányelv 30. cikke vagy mindkettő szerinti bejelentésének és közlésének sérelme nélkül a tagállamok a Bizottságot, az eu-LISA-t, az illetékes felügyeleti hatóságokat és az európai adatvédelmi biztost haladéktalanul tájékoztatják valamennyi biztonsági incidensről.

Az (EU) 2018/1725 rendelet 34. és 35. cikkének és az (EU) 2016/794 rendelet 34. cikkének sérelme nélkül az ETIAS központi egysége és az Europol haladéktalanul tájékoztatja a Bizottságot az eu-LISA-t és az európai adatvédelmi biztost valamennyi biztonsági incidensről.

Az interoperabilitási elemek központi infrastruktúráját érintő biztonsági incidens esetén az eu-LISA haladéktalanul tájékoztatja a Bizottságot és az európai adatvédelmi biztost.

(4) A tagállamok, az ETIAS központi egysége, valamint az Europol számára haladéktalanul információkat kell szolgáltatni, és az eu-LISA által biztosított incidens-kezelési tervnek megfelelően be kell számolni azokról a biztonsági incidensekről, amelyek hatással vannak vagy hatással lehetnek az interoperabilitási elemek működésére, vagy az adatok rendelkezésre állására, sértetlenségére, illetve bizalmas jellegére.

(5) Az érintett tagállamok, az ETIAS központi egysége, az Europol és az eu-LISA a biztonsági incidensek bekövetkezése esetén együttműködnek. A Bizottság végrehajtási jogi aktusok útján meghatározza ezen együttműködési eljárás részleteit. Ezeket a végrehajtási jogi aktusokat a 70. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

## 44. cikk

**Önellenzés**

A tagállamok és a releváns uniós ügynökségek biztosítják, hogy az interoperabilitási elemekhez való hozzáférésre jogosult valamennyi hatóság megtegye az e rendeletnek való megfelelése nyomon követéséhez szükséges intézkedéseket, és szükség esetén együttműködjön a felügyeleti hatósággal.

A 40. cikk szerinti adatkezelők megteszik a szükséges intézkedéseket az adatkezelés e rendelet szerinti megfelelésének figyelemmel kísérésére, többek a 10., a 16., a 24. és a 36. cikkben említett naplók gyakori ellenőrzése révén, és szükség esetén együttműködnek a felügyeleti hatóságokkal és az európai adatvédelmi biztossal.

## 45. cikk

**Szankciók**

A tagállamok biztosítják, hogy az adatokkal való visszaélésre és az adatok e rendeletbe ütköző kezelésére és megosztására a nemzeti joggal összhangban büntetőszankciók vonatkozzanak. Az előírt szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük.

## 46. cikk

**Felelősség**

(1) A kártérítéshez való jog, valamint az adatkezelőnek vagy adatfeldolgozónak az (EU) 2016/679 rendelet, az (EU) 2016/680 irányelv és az (EU) 2018/1725 rendelet értelmében fennálló felelősségének sérelme nélkül:

a) minden olyan személy vagy tagállam, aki, illetve amely jogellenes személyesadat-kezelési műveletből vagy bármilyen egyéb, e rendelettel összeegyeztethetetlen tagállami intézkedésből adódóan vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adott tagállamtól kártérítésre jogosult;

- b) minden olyan személy vagy tagállam, aki, illetve amely az Europol, az Európai Határ- és Partvédelmi Ügynökség vagy az eu-LISA e rendelettel összeegyeztethetetlen intézkedéséből adódóan vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért kártérítésre jogosult az adott ügynökségtől.

Az érintett tagállam, az Europol, az Európai Határ- és Partvédelmi Ügynökség vagy az eu-LISA teljes mértékben vagy részben mentesül az első albekezdés szerinti felelőssége alól, ha bizonyítja, hogy a kárt előidéző eseményért nem felelős.

(2) Ha egy tagállam az e rendelet szerinti kötelezettségeinek elmulasztásával kárt okoz az interoperabilitási elemekben, az okozott kárért e tagállamot terheli a felelősség, kivéve és amennyiben az eu-LISA vagy az e rendelet hatálya alá tartozó valamely másik tagállam elmulasztotta meghozni a kár megelőzéséhez vagy hatásának minimalizálásához szükséges észszerű intézkedéseket.

(3) A tagállammal szembeni, az (1) és a (2) bekezdésben említett kártérítési igényekre az alperes tagállam nemzeti joga az irányadó. Az adatkezelővel vagy az eu-LISA-val szembeni, az (1) és a (2) bekezdésben említett kártérítési igényekre a Szerződésekben előírt feltételek vonatkoznak.

#### 47. cikk

### A tájékoztatáshoz való jog

(1) A közös BMS-ben, a CIR-ben vagy a MID-ben tárolandó személyes adatokat gyűjtő hatóság azon személyek rendelkezésére bocsátja az (EU) 2016/679 rendelet 13. és 14. cikkében, az (EU) 2016/680 irányelv 12. és 13. cikkében és az (EU) 2018/1725 rendelet 15. és 16. cikkében előírt információkat, akiknek az adatait gyűjtik. A hatóság az információkat az ilyen adatok gyűjtésének időpontjában közli.

(2) Minden információt – világos és közérthető nyelven – hozzáférhetővé kell tenni egy olyan nyelvi változatban, amelyet az érintett személy megért, vagy amelyről észszerűen feltételezhető, hogy megérti. Ez azt is magában foglalja, hogy a kiskorú érintetteknek a tájékoztatást az életkoruknak megfelelő módon kell megadni.

(3) Az alkalmazandó uniós adatvédelmi szabályokban foglalt, a tájékoztatáshoz való jogra vonatkozó szabályok alkalmazandók az ECRIS-TCN-ben rögzített és az e rendelet alkalmazásában kezelt személyes adatokra.

#### 48. cikk

### A MID-ben tárolt személyes adatokhoz kapcsolódó hozzáférési, helyesbítési és törlési jog, valamint az adatok kezelésének korlátozása

(1) Az (EU) 2016/679 rendelet 15–18. cikke, az (EU) 2018/1725 rendelet 17–20. cikke, valamint az (EU) 2016/680 irányelv 14., 15. és 16. cikke értelmében fennálló jogai gyakorlása érdekében bármely személynek jogában áll bármely tagállam illetékes hatóságához fordulni, amely kivizsgálja és megválaszolja a kérelmet.

(2) Az a tagállam, amely a kérelmet megvizsgálja, indokolatlan késedelem nélkül, de legkésőbb a kérelem kézhezvételétől számított 45 napon belül válaszol. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további 15 nappal meghosszabbítható. Az a tagállam, amely a kérelmet megvizsgálja, a kérelem kézhezvételétől számított 45 napon belül tájékoztatja az érintettet a határidő meghosszabbításáról, megjelölve a késedelem okait. A tagállamok dönthetnek úgy, hogy a válaszokat a központi hivatalok adják meg.

(3) Ha a személyes adatok helyesbítése vagy törlése iránti kérelmet a különböző személyazonosságok manuális ellenőrzéséért felelős tagállamtól eltérő tagállamhoz intézik, az a tagállam, amelyhez a kérelmet benyújtották, hét napon belül felveszi a kapcsolatot a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam hatóságával. A különböző személyazonosságok manuális ellenőrzéséért felelős tagállam indokolatlan késedelem nélkül, de legkésőbb az ilyen megkereséstől számított 30 napon belül ellenőrzi az adatok pontosságát és az adatkezelés jogszerűségét. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további 15 nappal meghosszabbítható. A különböző személyazonosságok manuális ellenőrzéséért felelős tagállam tájékoztatja a vele kapcsolatba lépett tagállamot az ilyen meghosszabbításról és a késedelem okáról. Az a tagállam, amely kapcsolatba lépett a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam hatóságával, tájékoztatja az érintett személyt a további eljárásról.

(4) Ha a személyes adatok helyesbítése vagy törlése iránti kérelmet egy olyan tagállamhoz nyújtják be, amelyben az ETIAS központi egysége volt felelős a különböző személyazonosságok manuális ellenőrzéséért, a tagállam, amelyhez a kérelmet benyújtották, hét napon belül felveszi a kapcsolatot az ETIAS központi egységével, és kéri véleményét. Az ETIAS központi egysége indokolatlan késedelem nélkül, de legkésőbb az ilyen megkereséstől számított 30 napon belül véleményt nyilvánít. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további 15 nappal meghosszabbítható. Az érintett személyt a további eljárásról az ETIAS központi egységével kapcsolatba lépett tagállam

(5) Amennyiben a vizsgálatot követően megállapítást nyer, hogy a MID-ben tárolt adatok pontatlanok, vagy jogellenesen kerültek rögzítésre, a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam, vagy ha a nincs a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam, vagy ha az ETIAS központi egysége volt a felelős a különböző személyazonosságok manuális ellenőrzéséért, az a tagállam, amelyhez a kérelmet benyújtották, indokolatlan késedelem nélkül helyesbíti vagy törli ezeket az adatokat. Az érintett személyt írásban tájékoztatni kell arról, hogy adatait helyesbítették vagy törölték.

(6) Amennyiben a MID-ben tárolt adatokat valamely tagállam azok megőrzésének ideje alatt módosítja, az említett tagállam elvégzi a 27. cikkben, és adott esetben a 29. cikkben meghatározott adatkezelést annak megállapítása céljából, hogy a módosított adatokat össze kell-e kapcsolni. Amennyiben az adatkezelés nem jelez egyezést, az említett tagállam törli az adatokat a személyazonosságot megerősítő dossziéból. Amennyiben az automatizált adatfeldolgozás egy vagy több egyezést jelez, az említett tagállam e rendelet vonatkozó rendelkezéseivel összhangban létrehozza vagy frissíti a releváns kapcsolatot.

(7) Ha a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam, illetve adott esetben az a tagállam, amelyhez a kérelmet benyújtották, nem ért egyet azzal, hogy a MID-ben tárolt adatok pontatlanok vagy jogellenesen kerültek rögzítésre, e tagállam haladéktalanul közigazgatási határozatot hoz, amely írásbeli magyarázatot nyújt az érintett személynek arról, hogy e tagállam miért nem kívánja helyesbíteni vagy törölni a rá vonatkozó adatokat.

(8) A (7) bekezdésben említett határozat tájékoztatással is kell, hogy szolgáljon az érintett személy részére, ismertetve annak lehetőségét, hogy a személyes adatokhoz való hozzáférés, az adatok helyesbítése, törlése vagy kezelésének korlátozása iránti kérelem tárgyában hozott határozat ellen kifogást nyújthat be, és adott esetben arról, hogy hogyan nyújthat be keresetet vagy panaszt az illetékes hatóságokhoz vagy bíróságokhoz, továbbá ismertetve az esetleges segítségnyújtás lehetőségét, beleértve a felügyeleti hatóságok általi segítségnyújtást is.

(9) A személyes adatokhoz való hozzáférés, az adatok helyesbítése, törlése vagy kezelésének korlátozása iránti kérelmeknek tartalmazniuk kell az érintett személy személyazonosításához szükséges információkat. Ezek az információk kizárólag az e cikkben említett jogok gyakorlásának lehetővé tételére használhatók fel, és ezt követően haladéktalanul törlésre kerülnek.

(10) A különböző személyazonosságok manuális ellenőrzéséért felelős tagállamnak vagy adott esetben annak a tagállamnak, amelyhez a kérelmet benyújtották, írásos bejegyzést kell vezetnie arról, hogy kérelmet nyújtottak be a személyes adatokhoz való hozzáférés, az helyesbítése, törlése vagy kezelésének korlátozása iránt, valamint arról, hogy hogyan kezelték a kérelmet, és haladéktalanul a hatóságok rendelkezésére kell bocsátania ezt a bejegyzést.

(11) Ez a cikk nem érinti az ebben a cikkben meghatározott jogokra vonatkozó, az (EU) 2016/679 rendelet és az (EU) 2016/680 irányelv szerinti korlátozásokat és megszorító feltételeket.

#### 49. cikk

#### Webportál

(1) A személyes adatokhoz való hozzáféréshez, az adatok helyesbítéséhez, törléséhez vagy kezelésének korlátozásához való jog gyakorlásának megkönnyítése céljából webportál jön létre.

(2) A webportál tájékoztatást nyújt a 47. és a 48. cikkben említett jogokról és eljárásokról, valamint tartalmaz egy felhasználói felületet, amely lehetővé teszi azon személyek számára, akiknek adatait a MID-ben kezelik, és akiket a 32. cikk (4) bekezdésének megfelelően tájékoztattak a vörös kapcsolat meglétéről, hogy megkapják a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam illetékes hatóságának kapcsolattartási adatait.

(3) A különböző személyazonosságok manuális ellenőrzéséért felelős tagállam illetékes hatósága kapcsolattartási adatainak megszerzése érdekében annak a személynek, akinek adatait a MID-ben kezelik, be kell vinnie a rendszerbe a 34. cikk d) pontjában említett különböző személyazonosságok manuális ellenőrzéséért felelős hatóságra vonatkozó hivatkozást. A webportál felhasználja ezt a hivatkozást a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam illetékes hatósága kapcsolattartási adatainak lekérésére. A webportál tartalmaz egy elektronikus levélmintát is, amely megkönnyíti a portál-felhasználó és a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam illetékes hatósága közötti kommunikációt. Az ilyen elektronikus levél tartalmazza a 34. cikk c) pontjában említett egységes azonosító számot annak érdekében, hogy a különböző személyazonosságok manuális ellenőrzéséért felelős tagállam illetékes hatósága azonosítani tudja az érintett adatokat.



(4) A tagállamok tájékoztatják az eu-LISA-t minden olyan hatóság kapcsolattartási adatairól, amely hatáskörrel rendelkezik a 47. és a 48. cikkben említett bármely kérelem vizsgálatára és megválaszolására, és rendszeresen áttekinti, hogy ezek az adatok naprakészek-e.

(5) Az eu-LISA kifejleszti a webportált, és gondoskodik annak műszaki irányításáról.

(6) A Bizottság a 69. cikkkel összhangban felhatalmazáson alapuló jogi aktust fogad el, amelyben részletes szabályokat határoz meg a webportál működtetésére vonatkozóan, beleértve a felhasználói felületet, azon nyelveket, amelyeken a webportált elérhetővé kell tenni, valamint az elektronikus levélmintát.

#### 50. cikk

### **Személyes adatok közlése harmadik országokkal, nemzetközi szervezetekkel és magánfelekkel**

A 767/2008/EK rendelet 31. cikkének, az (EU) 2016/794 rendelet 25. és 26. cikkének, az (EU) 2017/2226 rendelet 41. cikkének, az (EU) 2018/1240 rendelet 65. cikkének, valamint az Interpol-adatbázisok ESP-n keresztüli, e rendelet 9. cikkének (5) bekezdésével összhangban történő, olyan lekérdezésének sérelme nélkül, amely megfelel az (EU) 2018/1725 rendelet V. fejezetében és az (EU) 2016/679 rendelet V. fejezetében foglalt rendelkezéseknek, az interoperabilitási elemekben tárolt, kezelt vagy azokon keresztül elért személyes adatok nem továbbíthatók és nem tehetők elérhetővé harmadik országok, nemzetközi szervezetek vagy magánfelek számára.

#### 51. cikk

### **A felügyeleti hatóságok által gyakorolt felügyelet**

(1) Minden tagállam biztosítja, hogy a felügyeleti hatóságok független módon figyelemmel kísérik, hogy az érintett tagállam jogszerűen kezeli-e e rendelet alapján a személyes adatokat, beleértve az adatok interoperabilitási elemekbe és onnan történő továbbítását is.

(2) Minden tagállam biztosítja, hogy az (EU) 2016/680 irányelv alapján elfogadott nemzeti törvényi, rendeleti és közigazgatási rendelkezések alkalmazása adott esetben kiterjedjen a rendőri hatóságok és a kijelölt hatóságok interoperabilitási elemekhez való hozzáféréseire is, az olyan személyek jogaival összefüggésben is, akiknek az adataihoz ilyen módon fértek hozzá.

(3) A felügyeleti hatóságok biztosítják a felelős nemzeti hatóságok által az e rendelet értelmében végzett személyesadat-kezelési műveleteknek a vonatkozó nemzetközi ellenőrzési standardoknak megfelelő, legalább négyévente történő ellenőrzését.

Az említett felügyeleti hatóságok évente közzéteszik a személyes adatok helyesbítésére, törlésére vagy kezelésének korlátozására irányuló kérelmek számát, a kérelmek nyomán hozott intézkedéseket, valamint az érintett személyek kérelme nyomán végzett helyesbítések, törlések és az adatkezelés korlátozásainak számát.

(4) A tagállamok biztosítják, hogy felügyeleti hatóságaik rendelkezzenek az e rendelet alapján rájuk ruházott feladatok ellátásához szükséges erőforrásokkal és szakértelemmel.

(5) A tagállamok az (EU) 2016/679 rendelet 51. cikkének (1) bekezdésében említett felügyeleti hatóság rendelkezésére bocsátják a kért információkat, különösen az e rendelet szerinti felelősségi körüknek megfelelően folytatott tevékenységekre vonatkozó információkat. A tagállamok biztosítják az (EU) 2016/679 rendelet 51. cikkének (1) bekezdésében említett felügyeleti hatóságok számára az e rendelet 10., 16., 24. és 36. cikkében említett naplóihoz való hozzáférést, az e rendelet 22. cikkének (2) bekezdésében említett indokolásukhoz való hozzáférést, valamint mindenkor lehetővé teszik számukra az interoperabilitási célokra használt létesítményeikbe történő bejutást.

#### 52. cikk

### **Az európai adatvédelmi biztos általi ellenőrzések**

Az európai adatvédelmi biztos gondoskodik arról, hogy az eu-LISA, az ETIAS központi egysége és az Europol által e rendelet alkalmazásában végzett személyesadat-kezelési műveleteket a vonatkozó nemzetközi ellenőrzési standardok alapján legalább négyévente ellenőrizzék. Az ellenőrzésről készült jelentést meg kell küldeni az Európai Parlament, a Tanács, az eu-LISA, a Bizottság, a tagállamok és az érintett uniós ügynökség számára. Az eu-LISA, az ETIAS központi egysége és az Europol a jelentések elfogadása előtt lehetőséget kap észrevételeinek megtételére.

Az eu-LISA, az ETIAS központi egysége és az Europol az európai adatvédelmi biztos rendelkezésére bocsátja a kért információkat, hozzáférést biztosít az európai adatvédelmi biztos számára minden általa igényelt dokumentumhoz és a 10., a 16., a 24. és a 36. cikkben említett naplóihoz, valamint mindenkor lehetővé teszi az európai adatvédelmi biztos számára az eu-LISA összes létesítményébe történő bejutást.

## 53. cikk

**A felügyeleti hatóságok és az európai adatvédelmi biztos közötti együttműködés**

(1) A felügyeleti hatóságok és az európai adatvédelmi biztos – hatáskörük keretein belül eljárva – tevékenyen együttműködnek egymással felelősségi körük keretein belül, és biztosítják az interoperabilitási elemek használatának és az e rendelet egyéb rendelkezései alkalmazásának összehangolt felügyeletét, különösen akkor, ha az európai adatvédelmi biztos vagy valamely felügyeleti hatóság jelentős eltéréseket talál a tagállamok gyakorlatai között, vagy az interoperabilitási elemek kommunikációs csatornáin zajló, potenciálisan jogellenes adattovábbítást észlel.

(2) Az e cikk (1) bekezdésében említett esetekben az (EU) 2018/1725 rendelet 62. cikkével összhangban összehangolt felügyeletet kell biztosítani.

(3) Az Európai Adatvédelmi Testület 2021. június 12-ig, és azt követően két évente az e cikk szerinti tevékenységeire vonatkozóan együttes jelentést küld az Európai Parlamentnek, a Tanácsnak, a Bizottságnak, az Europolnak, az Európai Határ- és Partvédelmi Ügynökségnek és az eu-LISA-nak. A jelentésben valamennyi tagállamra vonatkozóan szerepelnie kell egy, az adott tagállam felügyeleti hatósága által összeállított fejezetnek.

## VIII. FEJEZET

**Feladatkörök**

## 54. cikk

**Az eu-LISA feladatai a tervezési és fejlesztési szakaszban**

(1) Az eu-LISA biztosítja az interoperabilitási elemeknek e rendelettel összhangban történő működtetését.

(2) Az interoperabilitási elemek elhelyezését az eu-LISA biztosítja a technikai helyszínein, valamint biztosítja az e rendeletben meghatározott funkciókat a biztonságra, a hozzáférhetőségre, a minőségre és a teljesítményre vonatkozóan az 55. cikk (1) bekezdésében meghatározott feltételekkel összhangban.

(3) Az eu-LISA felelős az interoperabilitási elemek fejlesztéséért, valamint az EES, a VIS, az ETIAS, a SIS az Eurodac, valamint az ECRIS-TCN és az ESP, a közös BMS, a CIR, a MID és a CRRS központi rendszerei közötti interoperabilitás megteremtéséhez szükséges kiigazításokért.

A 62. cikk sérelme nélkül az eu-LISA nem férhet hozzá az ESP-n, a közös BMS-en, a CIR-en vagy a MID-en keresztül kezelt személyes adatokhoz.

Az eu-LISA meghatározza az interoperabilitási elemek – ideértve azok kommunikációs infrastruktúráját is – fizikai felépítését, valamint a központi infrastruktúra és a biztonságos kommunikációs infrastruktúra tekintetében a műszaki előírásokat és azok továbbfejlesztését is, amelyeket a Bizottság kedvező véleményétől függően az igazgatótanács fogad el. Az eu-LISA továbbá minden olyan kiigazítást végrehajt a SIS-ben, az Eurodacban vagy az ECRIS-TCN-ben, amelyre az interoperabilitás megteremtéséhez, valamint az e rendeletben foglaltaknak megfelelően szükség van.

Az eu-LISA e rendelet hatálybalépését, valamint a 8. cikk (2) bekezdésében, a 9. cikk (7) bekezdésében, a 28. cikk (5) és (7) bekezdésében, a 37. cikk (4) bekezdésében, a 38. cikk (3) bekezdésében, a 39. cikk (5) bekezdésében, a 43. cikk (5) bekezdésében és a 74. cikk (10) bekezdésében előírt intézkedéseknek a Bizottság általi elfogadását követően a lehető leghamarabb kifejleszti és végrehajtja az interoperabilitási elemeket.

A fejlesztésnek a műszaki előírások kidolgozását és végrehajtását, a tesztelést és az átfogó projektmenedzsmentet és -koordinációt kell magában foglalnia.

(4) A kialakítás és fejlesztés szakaszában létre kell hozni egy legfeljebb 10 tagból álló programirányítási tanácsot. A programirányítási tanács az eu-LISA igazgatótanácsa által saját tagjai vagy póttagjai közül kinevezett hét tagból, a 71. cikkben említett, az interoperabilitással foglalkozó tanácsadó csoport elnökéből, az eu-LISA-t képviselő, az ügyvezető igazgató által kinevezett tagból, valamint a Bizottság által kinevezett tagból áll. Az eu-LISA igazgatótanácsa kizárólag azon tagállamokból nevez ki tagokat, amelyekre nézve az uniós jog értelmében teljes mértékben kötelezők valamennyi uniós információs rendszer tekintetében a rendszerek fejlesztését, létrehozását, működtetését és használatát szabályozó jogi eszközök, és amelyek részt fognak venni az interoperabilitási elemekben.

(5) A programirányítási tanács rendszeresen és negyedévente legalább három alkalommal ülésezik. A programirányítási tanács biztosítja az interoperabilitási elemek kialakítási és fejlesztési szakaszának megfelelő irányítását.

A programirányítási tanács minden hónapban írásban beszámol az eu-LISA igazgatótanácsának a projekt előrehaladásáról. A programirányítási tanács nem rendelkezik döntéshozatali hatáskörrel, és az eu-LISA igazgatótanácsának tagjait nem képviselheti.

(6) Az eu-LISA igazgatótanácsa meghatározza a programirányítási tanács eljárási szabályzatát, amely különösen a következőkről rendelkezik:

- a) az elnökség;
- b) az ülések helyszíne;
- c) az ülések előkészítése;
- d) a szakértők részvétele az üléseken;
- e) az igazgatótanácsban részt nem vevő tagállamok teljes körű tájékoztatását biztosító kommunikációs tervek.

Az elnöki tisztelet egy olyan tagállamnak kell betöltenie, amelyre nézve az uniós jog értelmében teljes mértékben kötelezőek valamennyi uniós információs rendszer tekintetében a rendszerek fejlesztését, létrehozását, működtetését és használatát szabályozó jogi eszközök, és amely rész fog venni az interoperabilitási elemekben.

A programirányítási tanács tagjainak valamennyi utazási és ellátási költségét az eu-LISA fedezi, és az eu-LISA eljárási szabályzatának 10. cikkét értelemszerűen alkalmazni kell. A programirányítási tanács titkárságát az eu-LISA biztosítja.

A 71. cikkben említett, interoperabilitással foglalkozó tanácsadó csoport rendszeresen ülésezik mindaddig, amíg az interoperabilitási elemek meg nem kezdik a működést. A tanácsadó csoport minden ülés után beszámol a programirányítási tanácsnak. A tanácsadó csoport biztosítja a programirányítási tanács tevékenységét támogató műszaki szakértelmet, valamint nyomon követi a tagállami előkészületek alakulását.

#### 55. cikk

### **Az eu-LISA feladatköre az üzemeltetés megkezdését követően**

(1) Műtán valamennyi interoperabilitási elem működésbe lépett, az eu-LISA felelős az interoperabilitási elemek központi infrastruktúrájának műszaki irányításáért, ideértve az interoperabilitási elemek karbantartását és technológiai fejlesztését is. Az eu-LISA – költség-haszon elemzés alapján – a tagállamokkal együttműködve biztosítja, hogy a legjobb rendelkezésre álló technológiát alkalmazzák. Az eu-LISA felelős a 6., a 12., a 17., a 25. és a 39. cikkben említett kommunikációs infrastruktúra műszaki irányításáért is.

Az interoperabilitási elemek műszaki irányítása magában foglal minden olyan feladatot és műszaki megoldást, amely a hét minden napján, napi 24 órában, e rendelettel összhangban az interoperabilitási elemek működtetéséhez és a tagállamok és az uniós ügynökségek számára megszakításmentes szolgáltatások nyújtásához szükséges, ideértve azokat a karbantartási munkákat és technikai fejlesztéseket, amelyek az elemek megfelelő műszaki minőségű, a műszaki előírásoknak eleget tévő működéséhez szükségesek, mindenekelőtt a központi infrastruktúrákban történő lekérdezések válaszüzeje tekintetében.

Az interoperabilitási elemek mindegyikét oly módon kell fejleszteni és kezelni, hogy biztosított legyen a gyors, zökkenőmentes, hatékony és ellenőrzött hozzáférés ezen elemekhez és a MID-ben, a közös BMS-ben és a CIR-ben tárolt adatokhoz, valamint a tagállami hatóságok és az uniós ügynökségek operatív igényeinek megfelelő válaszüzeje.

(2) Az Európai Unió tisztviselőire alkalmazandó személyzeti szabályzat 17. cikkének sérelme nélkül, az eu-LISA megfelelő szakmai titoktartási vagy azzal egyenértékű titoktartási szabályokat alkalmaz személyi állományának minden olyan tagjára, aki munkája során az interoperabilitási elemekben tárolt adatokat kell, hogy kezeljen. Ez a kötelezettség ezen személyi állomány hivatali vagy munkaviszonyának megszűnését, vagy tevékenysége megszűntét követően is fennáll.

Az 62. cikk sérelme nélkül, az eu-LISA nem férhet hozzá az ESP-n, a közös BMS-n, a CIR-en és a MID-en keresztül kezelt személyes adatokhoz.

(3) Az eu-LISA az adatminőség ellenőrzésére irányuló mechanizmust és eljárásokat dolgoz ki és üzemeltet a közös BMS-ben és a CIR-ben a 37. cikknek megfelelően tárolt adatokra vonatkozóan.

(4) Az eu-LISA ellátja továbbá az interoperabilitási elemek technikai használatára vonatkozó képzéssel kapcsolatos feladatokat.

## 56. cikk

**A tagállamok feladatai**

(1) Az egyes tagállamok felelősek:

- a) az ESP és a CIR kommunikációs infrastruktúrájához való kapcsolódásért;
- b) a meglévő nemzeti rendszereknek és infrastruktúráknak az ESP-vel, a CIR-rel és a MID-del történő integrálásáért;
- c) a meglévő nemzeti infrastruktúrájuk szervezéséért, irányításáért, működtetéséért és karbantartásáért, valamint annak az interoperabilitási elemekkel való összekapcsolásáért;
- d) az illetékes nemzeti hatóságok megfelelő felhatalmazással rendelkező személyi állománya számára az e rendelettel összhangban az ESP-hez, a CIR-hez és a MID-hez biztosított hozzáférés irányításáért és részletes szabályozásáért, valamint a személyi állomány e tagjairól és azok profiljáról összeállítandó lista elkészítéséért és rendszeres frissítéséért;
- e) a CIR-hez személyazonosítás céljából történő hozzáférést lehetővé tévő, a 20. cikk (5) és (6) bekezdésében említett jogalkotási intézkedések elfogadásáért;
- f) a különböző személyazonosságok manuális ellenőrzéséért, a 29. cikkben említettek szerint;
- g) az uniós jogban meghatározott adatminőségi követelményeknek való megfelelésért;
- h) az egyes uniós információs rendszerek szabályainak való maradéktalan megfelelésért a személyes adatok biztonságának és sértetlenségének biztosítása érdekében;
- i) a Bizottságnak a 37. cikk (5) bekezdésében említett, az adatminőségre vonatkozó értékelő jelentésében feltárt hiányosságok orvoslásáért.

(2) Valamennyi tagállam összekapcsolja kijelölt hatóságait a CIR-rel.

## 57. cikk

**Az Europol feladatai**

(1) Az Europol biztosítja az Europol-adatok ESP-n keresztül történő lekérdezéseinek kezelését. Az Europol az alap védelmi szintű adatok vonatkozásában megfelelően kiigazítja az Europol-rendszerek lekérdezése (QUEST) elnevezésű interfészt.

(2) Az Europol felelős a megfelelő felhatalmazással rendelkező személyi állománya számára az ESP és a CIR e rendelet szerinti használatának és az azokhoz történő hozzáférésnek az irányításáért és a vonatkozó feltételek biztosításáért, valamint az említett személyi állományt és tagjai profilját tartalmazó lista elkészítéséért és rendszeres aktualizálásáért.

## 58. cikk

**Az ETIAS központi egységének feladatai**

Az ETIAS központi egysége felelős:

- a) a különböző személyazonosságok manuális ellenőrzéséért a 29. cikkkel összhangban;
- b) az EES-ben, a VIS-ben, az Eurodacban és a SIS-ben tárolt adatok körében a többszörös személyazonosság észlelését célzó, a 65. cikkben említett ellenőrzés elvégzéséért.

**IX. FEJEZET****Egyéb uniós eszközök módosításai**

## 59. cikk

**Az (EU) 2018/1726 rendelet módosításai**

Az (EU) 2018/1726 rendelet a következőképpen módosul:

1. A 12. cikk helyébe a következő szöveg lép:

„12. cikk

**Adatminőség**

(1) Az ügynökség üzemeltetési felelősségi körébe tartozó rendszerekbe bevitt adatokkal kapcsolatos tagállami felelősségek sérelme nélkül az ügynökség, szorosan bevonva tanácsadó csoportját, az ügynökség üzemeltetési felelősségi körébe tartozó valamennyi rendszer tekintetében az adatminőség ellenőrzésére irányuló, automatizált mechanizmusokat és az adatminőségre vonatkozó közös mutatókat, valamint az adatok tárolására vonatkozó minőségi minimumkövetelményeket alakít ki, az említett rendszereket szabályozó jogi eszközök vonatkozó rendelkezéseivel, valamint az (EU) 2019/817 (\*) és az (EU) 2019/818 (\*\*) európai parlamenti és tanácsi rendelet 37. cikkével összhangban.

(2) Az ügynökség az (EU) 2019/817 rendelet és az (EU) 2019/818 rendelet 39. cikkével összhangban létrehozza a jelentések és statisztikák kizárólag anonimizált adatokat tartalmazó központi adattárát, az ügynökség által kezelt nagyméretű IT-rendszerek fejlesztését, létrehozását, működtetését és használatát szabályozó jogi eszközök különös rendelkezéseire is figyelemmel.

(\*) Az Európai Parlament és a Tanács (EU) 2019/817 rendelete (2019. május 20.) az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a határok és a vízumügy területén, továbbá a 767/2008/EK, az (EU) 2016/399, az (EU) 2017/2226, az (EU) 2018/1240, az (EU) 2018/1726 és az (EU) 2018/1861 európai parlamenti és tanácsi rendelet, valamint a 2004/512/EK és a 2008/633/IB tanácsi határozat módosításáról (HL L 135., 2019.5.22., 27. o.).

(\*\*) Az Európai Parlament és a Tanács (EU) 2019/818 rendelete (2019. május 20.) az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a rendőrségi és igazságügyi együttműködés, a menekültügy és a migráció területén, valamint az (EU) 2018/1726, az (EU) 2018/1862 és az (EU) 2019/816 rendelet módosításáról. (HL L 135., 2019.5.22., 85. o.).”

2. A 19. cikk (1) bekezdése a következőképpen módosul:

a) a bekezdés a következő ponttal egészül ki:

„eea) elfogadja az interoperabilitási elemek fejlesztésének helyzetéről szóló jelentéseket az (EU) 2019/817 rendelet 78. cikkének (2) bekezdése és az (EU) 2019/818 rendelet 74. cikkének (2) bekezdése alapján.”

b) az ff) pont helyébe a következő szöveg lép:

„ff) elfogadja a SIS II műszaki működéséről szóló jelentéseket az (EU) 2018/1861 európai parlamenti és tanácsi rendelet (\*) 60. cikkének (7) bekezdése és az (EU) 2018/1862 európai parlamenti és tanácsi rendelet (\*\*) 74. cikkének (8) bekezdése szerint, a VIS műszaki működéséről szóló jelentéseket a 767/2008/EK rendelet 50. cikkének (3) bekezdése és a 2008/633/IB határozat 17. cikkének (3) bekezdése szerint, az EES műszaki működéséről szóló jelentéseket az (EU) 2017/2226 rendelet 72. cikkének (4) bekezdése szerint, az ETIAS műszaki működéséről szóló jelentéseket az (EU) 2018/1240 rendelet 92. cikkének (4) bekezdése szerint, az ECRIS-TCN és az ECRIS referenciaalkalmazás műszaki működéséről szóló jelentéseket az (EU) 2019/816 európai parlamenti és tanácsi rendelet (\*\*\*) 36. cikkének (8) bekezdése szerint, valamint az interoperabilitási elemek műszaki működéséről szóló jelentéseket az (EU) 2019/817 rendelet 78. cikkének (3) bekezdése és az (EU) 2019/818 rendelet 74. cikkének (3) bekezdése szerint;

(\*) Az Európai Parlament és a Tanács (EU) 2018/1861 rendelete (2018. november 28.) a határforgalom-ellenőrzés terén a Schengeni Információs Rendszer (SIS) létrehozásáról, működéséről és használatáról, a Schengeni Megállapodás végrehajtásáról szóló egyezmény módosításáról, valamint az 1987/2006/EK rendelet módosításáról és hatályon kívül helyezéséről (HL L 312., 2018.12.7., 14. o.).

(\*\*) Az Európai Parlament és a Tanács (EU) 2018/1862 rendelete (2018. november 28.) a rendőrségi együttműködés és a büntetőügyekben folytatott igazságügyi együttműködés terén a Schengeni Információs Rendszer (SIS) létrehozásáról, működéséről és használatáról, a 2007/533/IB tanácsi határozat módosításáról és hatályon kívül helyezéséről, valamint az 1986/2006/EK európai parlamenti és tanácsi rendelet és a 2010/261/EU bizottsági határozat hatályon kívül helyezéséről (HL L 312., 2018.12.7., 56. o.).

(\*\*\*) Az Európai Parlament és a Tanács (EU) 2019/816 rendelete (2019. április 17.) az Európai Bűnügyi Nyilvántartási Információs Rendszer kiegészítése érdekében a harmadik országbeli állampolgárokkal és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval rendelkező tagállamok azonosítására szolgáló központosított rendszer (ECRIS-TCN) létrehozásáról, valamint az (EU) 2018/1726 rendelet módosításáról (HL L 135., 2019.5.22., 1. o.);”

c) a hh) pont helyébe a következő szöveg lép:

„hh) hivatalos észrevételeket fogad el az európai adatvédelmi biztosnak az (EU) 2018/1861 rendelet 56. cikkének (2) bekezdése, a 767/2008/EK rendelet 42. cikkének (2) bekezdése, a 603/2013/EU rendelet 31. cikkének (2) bekezdése, valamint az (EU) 2017/2226 rendelet 56. cikkének (2) bekezdése, az (EU) 2018/1240 rendelet 67. cikke, továbbá az (EU) 2019/816 rendelet 29. cikkének (2) bekezdése, az (EU) 2019/817 rendelet és az (EU) 2019/818 rendelet 52. cikke szerinti vizsgálatokról szóló jelentéseivel kapcsolatban, valamint biztosítja e vizsgálatok megfelelő nyomon követését;”

d) az mm) pont helyébe a következő szöveg lép:

„mm) biztosítja az (EU) 2018/1861 rendelet 41. cikkének (8) bekezdése és az (EU) 2018/1862 rendelet 56. cikkének (7) bekezdése értelmében a SIS-ben tárolt adatok közvetlen keresésére jogosult illetékes hatóságok jegyzékének, valamint a (EU) 2018/1861 rendelet 7. cikkének (3) bekezdése, illetve az (EU) 2018/1862 rendelet 7. cikkének (3) bekezdése alapján a SIS (N.SIS) nemzeti rendszerek és a SIRENE-irodák jegyzékének, továbbá az (EU) 2017/2226 rendelet 65. cikkének (2) bekezdése szerinti illetékes hatóságok listájának, az (EU) 2018/1240 rendelet 87. cikkének (2) bekezdése szerinti illetékes hatóságok listájának, az (EU) 2019/816 rendelet 34. cikkének (2) bekezdése szerinti központi hatóságok listájának, valamint az (EU) 2019/817 rendelet 71. cikkének (1) bekezdése és az (EU) 2019/818 rendelet 67. cikkének (1) bekezdése szerinti hatóságok jegyzékének évenkénti közzétételét;”.

3. A 22. cikk (4) bekezdése helyébe a következő szöveg lép:

„(4) Az Europol és az Eurojust megfigyelőként részt vehet az igazgatótanács ülésein, amikor a SIS II-t érintő, a 2007/533/IB határozat alkalmazásával kapcsolatos kérdés van napirenden.

Az Európai Határ- és Partvédelmi Ügynökség megfigyelőként részt vehet az igazgatótanács ülésein, amikor a SIS-t érintő, az (EU) 2016/1624 rendelet alkalmazásával kapcsolatos kérdés van napirenden.

Az Europol megfigyelőként részt vehet az igazgatótanács azon ülésein is, amikor a VIS-t érintő, a 2008/633/IB határozat alkalmazásával kapcsolatos vagy az Eurodacot érintő, a 603/2013/EU rendelet alkalmazásával kapcsolatos kérdés van napirenden.

Az Europol megfigyelőként részt vehet az igazgatótanács azon ülésein, amikor az EES-t érintő, az (EU) 2017/2226 rendelet alkalmazásával kapcsolatos vagy az ETIAS-t érintő, az (EU) 2018/1240 rendelet alkalmazásával kapcsolatos kérdés van napirenden.

Az Európai Határ- és Partvédelmi Ügynökség megfigyelőként részt vehet az igazgatótanács ülésein, amikor az ETIAS-t érintő, az (EU) 2018/1240 rendelet alkalmazásával kapcsolatos kérdés van napirenden.

Az Eurojust, az Europol és az Európai Ügyészség megfigyelőként részt vehet az igazgatótanács ülésein, amikor az (EU) 2019/816 rendelettel kapcsolatos kérdés van napirenden.

Az Europol, Eurojust és az Európai Határ- és Partvédelmi Ügynökség megfigyelőként részt vehet az igazgatótanács ülésein, amikor az (EU) 2019/817 rendelettel, valamint az (EU) 2019/818 rendelettel kapcsolatos kérdés van napirenden.

Az igazgatótanács az üléseire megfigyelőként meghívhat bárkit, akinek véleménye érdeklődésre tarthat számot.”

4. A 24. cikk (3) bekezdésének p) pontja helyébe a következő szöveg lép:

„p) a tisztviselők személyzeti szabályzata 17. cikkének sérelme nélkül, megállapítja a titoktartási követelményeket annak érdekében, hogy megfeleljenek az 1987/2006/EK rendelet 17. cikkének, a 2007/533/IB határozat 17. cikkének, a 767/2008/EK rendelet 26. cikke (9) bekezdésének, továbbá a 603/2013/EU rendelet 4. cikke (4) bekezdésének; az (EU) 2017/2226 rendelet 37. cikke (4) bekezdésének, az (EU) 2018/1240 rendelet 74. cikke (2) bekezdésének, az (EU) 2019/816 rendelet 11. cikke (16) bekezdésének, valamint az (EU) 2019/817 rendelet és az (EU) 2019/818 rendelet 55. cikke (2) bekezdésének;”.

5. A 27. cikk a következőképpen módosul:

a) Az (1) bekezdés a következő ea) ponttal egészül ki:

„da) az interoperabilitással foglalkozó tanácsadó csoport;”

b) a (3) bekezdés helyébe a következő szöveg lép:

„(3) Az Europol, az Eurojust, valamint az Európai Határ- és Partvédelmi Ügynökség egyaránt kinevezhet egy-egy képviselőt a SIS II tanácsadó csoportba.

Az Europol képviselőt nevezhet ki továbbá a VIS, az Eurodac és az EES-ETIAS tanácsadó csoportba.

Az Európai Határ- és Partvédelmi Ügynökség kinevezhet továbbá egy képviselőt az EES-ETIAS tanácsadó csoportba.

Az Eurojust, az Europol és az Európai Ügyészség szintén kinevezhet egy-egy képviselőt az ECRIS-TCN-nel foglalkozó tanácsadó csoportba.

Az Europol, az Eurojust, valamint az Európai Határ- és Partvédelmi Ügynökség kinevezhet egy-egy képviselőt az interoperabilitással foglalkozó tanácsadó csoportba.”

## 60. cikk

**Az (EU) 2018/1862 rendelet módosításai**

Az (EU) 2018/1862 rendelet a következőképpen módosul:

1. A 3. cikk a következő pontokkal egészül ki:

- „18. »ESP«: az (EU) 2019/818 európai parlamenti és tanácsi rendelet (\*) 6. cikkének (1) bekezdésével létrehozott európai keresőportál;”;
- 19. »közös BMS«: az (EU) 2019/818 rendelet 12. cikkének (1) bekezdésével létrehozott közös biometrikus megfeleltetési szolgáltatás;
- 20. »CIR«: az (EU) 2019/818 rendelet 17. cikkének (1) bekezdésével létrehozott közös személyazonosítóadat-tár;
- 21. »MID«: az (EU) 2019/818 rendelet 25. cikkének (1) bekezdésével létrehozott, többszörös személyazonosságot észlelő rendszer;

(\*) Az Európai Parlament és a Tanács (EU) 2019/818 rendelete (2019. május 20.) az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a rendőrségi és igazságügyi együttműködés, a menekültügy és a migráció területén, valamint az (EU) 2018/1726, az (EU) 2018/1862 és az (EU) 2019/816 rendelet módosításáról (HL L 135., 2019. 5.22., 85. o.)”

2. A 4. cikk a következőképpen módosul:

a) az (1) bekezdés b) és c) pontja helyébe a következő szöveg lép:

- „b) az egyes tagállamok nemzeti rendszere (a továbbiakban: N.SIS), amely a SIS központi rendszerrel kommunikáló nemzeti adatrendszerekből áll, ideértve legalább egy nemzeti vagy közös tartalék N.SIS-hez;
- c) a CS-SIS, a tartalék CS-SIS és az NI-SIS közötti kommunikációs infrastruktúra (a továbbiakban: kommunikációs infrastruktúra), amely a SIS-adatok, valamint a 7. cikk (2) bekezdésében említett SIRENE-irodák közötti adatcsere céljára rendelt kódolt virtuális hálózatot képez; és
- d) egy biztonságos kommunikációs infrastruktúra a CS-SIS, illetve az ESP, a közös BMS és a MID központi infrastruktúrái között.”;

b) a szöveg a következő bekezdésekkel egészül ki:

„(8) Az (1)–(5) bekezdés sérelme nélkül a személyekre és személyazonosító okmányokra vonatkozó SIS-adatok az ESP útján is kereshetők.

(9) Az (1)–(5) bekezdés sérelme nélkül a személyekre és személyazonosító okmányokra vonatkozó SIS-adatok az (1) bekezdés d) pontjában említett biztonságos kommunikációs infrastruktúrán keresztül is továbbíthatók. Ezeket az adattovábbításokat olyan mértékre kell korlátozni, amilyen mértékben az adatok szükségesek az (EU) 2019/818 rendeletben említett célokhoz.”

3. A 7. cikk a következő bekezdéssel egészül ki:

„(2a) A SIRENE-irodák biztosítják továbbá a különböző személyazonosságok manuális ellenőrzését az (EU) 2019/818 rendelet 29. cikkével összhangban. A SIRENE-irodák az e feladat elvégzéséhez szükséges mértékben hozzáféréssel rendelkeznek a CIR-ben és a MID-ben tárolt adatokhoz az (EU) 2019/818 rendelet 21. és 26. cikkében meghatározott célokra.”

4. A 12. cikk (1) bekezdése a következő albekezdéssel egészül ki:

„A tagállamok gondoskodnak arról, hogy az ESP-n keresztül a személyes adatokhoz való minden hozzáférést szintén naplózzák a lekérdezés jogszerűségének ellenőrzése, az adatkezelés jogszerűségének ellenőrzése, az önellenőrzés, továbbá az adatok sértetlensége és biztonsága érdekében.”

5. A 44. cikk (1) bekezdése a következő ponttal egészül ki:

„f) a különböző személyazonosságok ellenőrzése és a személyazonossággal való visszaélés elleni küzdelem az (EU) 2019/818 rendelet V. fejezetének megfelelően.”

6. A 74. cikk (7) bekezdése helyébe a következő szöveg lép:

„(7) A 15. cikk (4) bekezdésének és e cikk (3), (4) és (6) bekezdésének alkalmazása céljából az eu-LISA-nak a 15. cikk (4) bekezdésében és az e cikk (3) bekezdésében említett adatokat oly módon kell tárolnia, amely nem teszi lehetővé egyének személyazonosságának megállapítását az (EU) 2019/818 rendelet 39. cikkében említett jelentések és statisztikák központi adattárában.

Az eu-LISA lehetőséget nyújt a Bizottságnak és az e cikk (6) bekezdésben említett szerveknek arra, hogy személyre szabott jelentéseket és statisztikákat kérjenek le. Kérelemre az eu-LISA az (EU) 2019/818 rendelet 39. cikkével összhangban jelentéstételi és statisztikai célból hozzáférést biztosít a tagállamok, a Bizottság, az Europol és az Európai Határ- és Partvédelmi Ügynökség számára a központi adattárhoz.”

#### 61. cikk

### Az (EU) 2019/816 rendelet módosításai

Az (EU) 2019/816 rendelet a következőképpen módosul:

1. Az 1. cikk a következő ponttal egészül ki:

„c) megállapítja azokat a feltételeket, amelyek mellett az ECRIS-TCN hozzájárul az ECRIS-TCN-ben az (EU) 2019/818 európai parlamenti és tanácsi rendelet (\*) 20. cikke alkalmazásában és az abban foglalt feltételek mellett nyilvántartott személyek helyes azonosításának megkönnyítéséhez és elősegítéséhez, azáltal, hogy a CIR-ben személyazonosító adatokat, útiokmány adatokat és biometrikus adatokat tárol.

(\*) Az Európai Parlament és a Tanács (EU) 2019/818 rendelete (2019. május 20.) az uniós információs rendszerek közötti interoperabilitás kereteinek megállapításáról a rendőrségi és igazságügyi együttműködés, a menekültügy és a migráció területén, valamint az (EU) 2018/1726, az (EU) 2018/1862 és az (EU) 2019/816 rendelet módosításáról (HL L 135., 2019.5.22., 85. o.)”

2. A 2. cikk helyébe a következő szöveg lép:

„2. cikk

#### Hatály

Ez a rendelet a tagállamokban hozott ítéletek hatálya alá tartozó harmadik országbeli állampolgárok személyazonosító adatainak az ítélethozatal szerinti tagállamok azonosítása céljából történő kezelésére alkalmazandó. Az 5. cikk (1) bekezdése b) pontjának ii. alpontja kivételével e rendelet harmadik országbeli állampolgárokra vonatkozó rendelkezéseit azokra az uniós polgárokra is alkalmazni kell, akik valamely harmadik ország állampolgárságával is rendelkeznek és a tagállamokban hozott ítéletek hatálya alá tartoznak. Ez a rendelet megkönnyíti és támogatja a személyek helyes azonosítását e rendelettel és az (EU) 2019/818 rendelettel összhangban.”;

3. A 3. cikk a következőképpen módosul:

a) a 8. pontot el kell hagyni;

b) a cikk a következő pontokkal egészül ki:

„19. „CIR”: az (EU) 2019/818 rendelet 17. cikkének (1) bekezdésével létrehozott közös személyazonosítóadat-tár;

20. „ECRIS-TCN-adatok”: az 5. cikkel összhangban a központi rendszerben és a CIR-ben tárolt összes adat;

21. „ESP”: az (EU) 2019/818 rendelet 6. cikkének (1) bekezdésével létrehozott európai keresőportál.”

4. A 4. cikk (1) bekezdése a következőképpen módosul:

a) az a) pont helyébe a következő szöveg lép:

„a) központi rendszer;”

b) a bekezdés a következő ponttal egészül ki:

„aa) CIR;”

c) a szöveg a következő ponttal egészül ki:

„e) kommunikációs infrastruktúra a központi rendszer, valamint az ESP és a CIR központi infrastruktúrái között.”

5. Az 5. cikk a következőképpen módosul:

a) az (1) bekezdés bevezető része helyébe a következő szöveg lép:

„(1) Az ítélethozatal szerinti tagállam központi hatósága minden elítélt harmadik országbeli állampolgár esetében adatrekordot hoz létre az ECRIS-TCN-ben. Az adatrekordnak a következőket kell tartalmaznia:”;



b) a cikk a következő bekezdéssel egészül ki:

„(1a) A CIR tartalmazza az (1) bekezdés b) pontjában említett adatokat, valamint az (1) bekezdés a) pontjában szereplő következő adatokat: vezetéknev (családi név), utónevek (keresztnevek), születési idő, születési hely (város és ország), állampolgárság vagy állampolgárságok, nem, adott esetben korábbi nevek, amennyiben rendelkezésre állnak, álnevek vagy felvett nevek, amennyiben rendelkezésre állnak, a személy úti okmányainak típusa és száma, valamint a kiállító hatóság neve. A CIR tartalmazhatja a (3) bekezdésben említett adatokat. A fennmaradó ECRIS-TCN-adatokat a központi rendszerben kell tárolni.”

6. A 8. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) Minden adatrekordot addig kell tárolni a központi rendszerben és a CIR-ben, amíg az érintett személlyel kapcsolatos ítéletekre vonatkozó adatokat a bünyügyi nyilvántartásokban tárolják.”;

b) a (2) bekezdés helyébe a következő szöveg lép:

„(2) Az (1) bekezdésben említett megőrzési időtartam lejártakor az ítélethozatal szerinti tagállam központi hatóságának törölnie kell a központi rendszerből és a CIR-ből az adatrekordot, beleértve az ujjnyomatadatokat és az arcképmásokat is. A törlést lehetőség szerint automatikusan, de minden esetben legkésőbb egy hónappal a megőrzési időtartam lejártát követően el kell végezni.”

7. A 9. cikk a következőképpen módosul:

a) az (1) bekezdésben az „az ECRIS-TCN-be” szövegrész helyébe az „a központi rendszerbe és a CIR-be” szövegrész lép;

b) a (2), a (3) és a (4) bekezdésben a „központi rendszerben” szövegrész helyébe a „központi rendszerben és a CIR-ben” szövegrész, a „központi rendszeren” szövegrész helyébe pedig a „központi rendszeren és a CIR-en” szövegrész lép.

8. A 10. cikk (1) bekezdésének j) pontját el kell hagyni.

9. A 12. cikk (2) bekezdésében a „központi rendszerben” szövegrész helyébe a „központi rendszerben és a CIR-ben” szövegrész lép.

10. A 13. cikk (2) bekezdésében a „központi rendszer” szövegrész helyébe a „központi rendszer és a CIR” szövegrész lép.

11. A 23. cikk (2) bekezdésében a „központi rendszerbe” szövegrész helyébe a „központi rendszerbe és a CIR-be” szövegrész lép.”

12. A 24. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) A központi rendszerbe és a CIR-be feltöltött adatok kizárólag a harmadik országbeli állampolgárokra vonatkozó bünyügyi nyilvántartási információval rendelkező tagállamok azonosítása céljából kezelhetők. A CIR-be feltöltött adatokat is az (EU) 2019/818 rendelettel összhangban kell kezelni az ECRIS-TCN-ben nyilvántartásba vett személyek e rendelettel összhangban történő helyes azonosításának megkönnyítése és elősegítése céljából.”;

b) a cikk a következő bekezdéssel egészül ki:

„(3) A (2) bekezdés sérelme nélkül a CIR-ben tárolt adatokba való betekintés céljából való hozzáférést továbbá az egyes tagállamok nemzeti hatóságainak megfelelően felhatalmazott személyzete, valamint az (EU) 2019/818 rendelet 20. és 21. cikkében megállapított célok tekintetében illetékes uniós ügynökségek megfelelően felhatalmazott személyzete számára kell fenntartani. E hozzáférést olyan mértékre kell korlátozni, amilyen mértékben az adatok szükségesek az említett célokkal összhangban álló feladataik elvégzéséhez, és e hozzáférésnek a kizűzött célok szempontjából szükségesnek és arányosnak kell lennie.”

13. A 32. cikk (2) bekezdése helyébe a következő szöveg lép:

„(2) E cikk (1) bekezdésének alkalmazásában az eu-LISA az említett bekezdésben említett adatokat az (EU) 2019/818 rendelet 39. cikkében említett, a jelentések és statisztikák központi adattárában tárolja.”

14. A 33. cikk (1) bekezdésében a „központi rendszer,” szövegrész helyébe a „központi rendszer, a CIR és” szövegrész lép.

15. A 41. cikk (2) bekezdése helyébe a következő szöveg lép:

„(2) Az adatfeltöltésnek a 35. cikk (1) bekezdésével összhangban meghatározott kezdő időpontja előtt hozott ítéletek esetében a központi hatóságoknak az alábbiak szerint kell létrehozniuk a központi rendszerben és a CIR-ben az egyéni adatrekordokat:

- a) az alfanumerikus adatokat a 35. cikk (2) bekezdésében említett időtartam végéig kell feltölteni a központi rendszerbe és a CIR-be;
- b) az ujjnyomatadatokat a működés 35. cikk (4) bekezdésével összhangban történő megkezdését követő két éven belül kell feltölteni a központi rendszerbe és a CIR-be.”

## X. FEJEZET

### Záró rendelkezések

#### 62. cikk

#### Jelentéstétel és statisztikák

(1) A tagállamok illetékes hatóságainak, a Bizottságnak és az eu-LISA-nak a megfelelő felhatalmazással rendelkező személyi állománya kizárólag jelentések és statisztikák összeállítása céljából betekintés céljából hozzáféréssel rendelkezik az ESP-felhasználói profilonkénti lekérdezések számához.

Az adatok alapján nem válhat lehetővé az egyének azonosítása.

(2) A tagállamok illetékes hatóságainak, a Bizottságnak és az eu-LISA-nak a megfelelő felhatalmazással rendelkező személyi állománya kizárólag jelentések és statisztikák összeállítása céljából betekintés céljából hozzáféréssel rendelkezik a CIR-rel kapcsolatos következő adatokhoz:

- a) a 20., a 21. és a 22. cikk szerinti célokból folytatott lekérdezések száma;
- b) a személy állampolgársága, neme és születési éve;
- c) az úti okmány típusa és a kiállító ország három betűből álló kódja;
- d) a biometrikus adatokkal és azok nélkül végzett keresések száma.

Az adatok alapján nem válhat lehetővé az egyének azonosítása.

(3) A tagállamok illetékes hatóságainak, a Bizottságnak és az eu-LISA-nak a megfelelő felhatalmazással rendelkező személyi állománya kizárólag jelentések és statisztikák összeállítása céljából betekintés céljából hozzáféréssel rendelkezik a MID-del kapcsolatos következő adatokhoz:

- a) a biometrikus adatokkal és azok nélkül végzett keresések száma;
- b) a kapcsolatok száma valamennyi kapcsolat-típus esetében és az összekapcsolt adatokat tartalmazó uniós információs rendszerek;
- c) az az időszak, amelyen keresztül a sárga és vörös kapcsolat a rendszerben maradt.

Az adatok alapján nem válhat lehetővé az egyének azonosítása.

(4) Az Európai Határ- és Partvédelmi Ügynökség megfelelő felhatalmazással rendelkező személyi állománya betekintéscéljából hozzáférhet az e cikk (1), (2) és (3) bekezdésében szereplő adatokhoz az (EU) 2016/1624 európai parlamenti és tanácsi rendelet <sup>(38)</sup> 11. és 13. cikkében említett kockázatelemzések és sebezhetőségi értékelések elvégzése céljából.

(5) Az Europol megfelelően felhatalmazott személyi állománya betekintés céljából hozzáférhet az e cikk (2) és (3) bekezdésében említett adatokhoz az (EU) 2016/794 rendelet 18. cikke (2) bekezdésének b) és c) pontjában említett stratégiai, tematikus és operatív elemzések elvégzése céljából.

(6) Az (1), a (2) és a (3) bekezdés alkalmazásában az említett bekezdésekben említett adatokat az eu-LISA a CRRS-ben tárolja. A CRRS-ben szereplő adatok alapján nem válhat lehetővé az egyének azonosítása, ugyanakkor az adatok az (1), a (2) és a (3) bekezdésben felsorolt hatóságok számára lehetővé teszik, hogy személyre szabott jelentéseket és statisztikákat kérjenek le a határforgalom-ellenőrzés hatékonyságának fokozása, a vízumkérelmek kezelésének megkönnyítése, valamint a tényeken alapuló uniós migrációs és biztonsági szakpolitikák kialakításának elősegítése érdekében.

(7) Kérés esetén a Bizottság az Európai Unió Alapjogi Ügynökségének rendelkezésére bocsátja a releváns információkat e rendelet alapvető jogokra gyakorolt hatásának értékelése céljából.

<sup>(38)</sup> Az Európai Parlament és a Tanács (EU) 2016/1624 rendelete (2016. szeptember 14.) az Európai Határ- és Parti Őrségről és az (EU) 2016/399 európai parlamenti és tanácsi rendelet módosításáról, valamint a 863/2007/EK európai parlamenti és tanácsi rendelet, a 2007/2004/EK tanácsi rendelet és a 2005/267/EK tanácsi határozat hatályon kívül helyezéséről (HL L 251., 2016.9.16., 1. o.).

## 63. cikk

**Az európai keresőportál használatára vonatkozó átmeneti időszak**

(1) Az ESP működésbe lépésétől számított két éven keresztül a 7. cikk (2) és (4) bekezdésében foglalt kötelezettségek nem alkalmazandók, és az ESP használata nem kötelező.

(2) A Bizottság felhatalmazást kap arra, hogy a 69. cikknek megfelelően felhatalmazáson alapuló jogi aktust fogadjon el, amelyben módosítja e rendeletet az e cikk (1) bekezdésében említett időszak egyszeri, legfeljebb 1 évvel történő meghosszabbítása révén, amennyiben az ESP végrehajtásának értékelése azt mutatja, hogy e meghosszabbítás különösen szükséges annak fényében, hogy az ESP működtetésének megkezdése milyen hatással járna a határforgalom-ellenőrzés megszervezésére és időtartamára.

## 64. cikk

**A közös személyazonosítóadat-tárhoz terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából történő hozzáférésre vonatkozó rendelkezésekre alkalmazandó átmeneti időszak**

A 22. cikket a CIR működése megkezdésének a 68. cikk (3) bekezdésében említett időpontjától kell alkalmazni.

## 65. cikk

**Átmeneti időszak a többszörös személyazonosság észlelése vonatkozásában**

(1) Azon időpontot követően egy éven át, amikor az eu-LISA a 68. cikk (4) bekezdésének b) pontjában említettek szerint bejelentette, hogy sikeresen lezárult a MID tesztelése, a MID működésének megkezdése előtt az ETIAS központi egysége felelős a többszörös személyazonosság észlelésére irányuló vizsgálat elvégzéséért az EES-ben, a VIS-ben, az Eurodacban és a SIS-ben tárolt adatok felhasználásával. A többszörös személyazonosság észlelésére irányuló vizsgálatokat kizárólag biometrikus adatok felhasználásával lehet elvégezni.

(2) Amennyiben a lekérdezés egy vagy több egyezést jelez, és az összekapcsolt fájlokban szereplő személyazonosító adatok azonosak vagy hasonlóak, a 33. cikknek megfelelően fehér kapcsolatot kell létrehozni.

Amennyiben a lekérdezés egy vagy több egyezést jelez és az összekapcsolt fájlokban szereplő személyazonosító adatok nem tekinthetők hasonlóaknak, a 30. cikknek megfelelően sárga kapcsolatot kell létrehozni, és a 29. cikk szerinti eljárást kell alkalmazni.

Amennyiben több egyezés is szerepel, az egyezést kiváltó valamennyi adatelem között kapcsolatot kell létrehozni.

(3) Sárga kapcsolat létrehozása esetén a MID az ETIAS központi egysége számára hozzáférést biztosít a különböző uniós információs rendszerekben található személyazonosító adatokhoz.

(4) A SIS-ben szereplő figyelmeztető jelzéssel történő kapcsolat létrehozása esetén – kivéve az (EU) 2018/1860 rendelet 3. cikkében, illetve az (EU) 2018/1861 rendelet 24. és 25. cikkében, vagy az (EU) 2018/1862 rendelet 38. cikkében szereplő figyelmeztető jelzéseket – a MID a figyelmeztető jelzést létrehozó tagállam SIRENE-irodája számára hozzáférést biztosít a különböző információs rendszerekben található személyazonosító adatokhoz.

(5) Az ETIAS központi egysége vagy az e cikk (4) bekezdésében említett esetekben a figyelmeztető jelzést létrehozó tagállam SIRENE-irodája hozzáféréssel rendelkezik a személyazonosság-megerősítő dossziében szereplő adatokhoz, értékeli a különböző személyazonosságokat, a 31., a 32. és a 33. cikkel összhangban frissíti a kapcsolatot, és azt hozzáadja a személyazonosság-megerősítő dossziéhoz.

(6) Az ETIAS központi egysége csak akkor értesíti a Bizottságot a 67. cikk (3) bekezdésének megfelelően, ha az összes sárga kapcsolatot manuálisan ellenőrizték és besorolásukat zöld, fehér vagy vörös kapcsolattá frissítették.

(7) A tagállamok szükség esetén segítséget nyújtanak az ETIAS központi egysége számára az e cikk szerinti többszörös személyazonosság észlelésére irányuló vizsgálat végrehajtásában.

(8) A Bizottság felhatalmazást kap arra, hogy a 69. cikknek megfelelően felhatalmazáson alapuló jogi aktust fogadjon el e rendelet módosítására az e cikk (1) bekezdésben említett időszak hat hónappal történő meghosszabbítása révén, amely két alkalommal alkalmanként hat hónappal meghosszabbítható. A meghosszabbítás csak azt követően adható meg, hogy felmérték a többszörös személyazonosság észlelésére irányuló vizsgálat lezárultához szükséges becsült időt, amely azt mutatja, hogy az (1) bekezdésben említett határidő lejárt vagy a folyamatban lévő meghosszabbítás lejárt előtt a többszörös személyazonosság észlelésére irányuló vizsgálat nem zárulhat le az ETIAS központi egységétől független okokból, és nem alkalmazhatók korrekciós intézkedések. Az értékelést legkésőbb az említett határidő lejárt vagy a folyamatban lévő meghosszabbítás lejárt előtt három hónappal kell elvégezni.

## 66. cikk

**Költségek**

(1) Az ESP, a közös BMS, a CIR és a MID létrehozásával és működtetésével kapcsolatban felmerült költségeket az Unió általános költségvetéséből kell fedezni.

(2) A meglévő nemzeti határinfrastruktúrák integrációja, azoknak az egységes nemzeti interfészekhez való kapcsolódása, valamint az egységes nemzeti interfészek elhelyezésével kapcsolatban felmerülő költségeket az Unió általános költségvetéséből kell fedezni.

Ez alól kivételt képeznek az alábbi költségek:

- a) a tagállamok projektirányítási irodái (találkozók, kiküldetések, irodák);
- b) a nemzeti IT-rendszerek elhelyezése (helyszín, végrehajtás, villamos energia, hűtés);
- c) a nemzeti IT-rendszerek üzemeltetése (üzemeltetői és támogatási szerződések);
- d) a nemzeti kommunikációs hálózatok tervezése, fejlesztése, bevezetése, üzemeltetése és karbantartása;

(3) Az Európai Unió általános költségvetésének más forrásaiból e célból nyújtott további finanszírozás sérelme nélkül 32 077 000 EUR összeg igénybevételére kerül sor az 515/2014/EU rendelet 5. cikke (5) bekezdésének b) pontja szerinti 791 000 000 EUR összegű keretből az e rendelet végrehajtásával kapcsolatos, az e cikk (1) és (2) bekezdésében előírt végrehajtási költségek fedezésére.

(4) A (3) bekezdésben említett keretből az eu-LISA számára 22 861 000 EUR-t, az Europol számára 9 072 000 EUR-t és az Európai Unió Bűnüldözési Képzési Ügynöksége (CEPOL) számára 144 000 EUR-t kell elkülöníteni azért, hogy ezek az ügynökségek az e rendelet szerinti feladataik ellátásában támogatáshoz jussanak. E finanszírozást közvetett irányítás keretében kell végrehajtani.

(5) A kijelölt hatóságoknál felmerülő költségeket az e hatóságokat kijelölő tagállamoknak kell viselniük. Az egyes tagállamok viselik a kijelölt hatóságok CIR-hez való kapcsolódásának költségeit.

Az Europolnál felmerülő költségeket, beleértve a CIR-hez való kapcsolódást is, az Europol viseli.

## 67. cikk

**Értesítések**

(1) A tagállamok értesítik az eu-LISA-t a 7., a 20., a 21. és a 26. cikkben említett azon hatóságokról, amelyek használati jogosultsággal vagy hozzáféréssel rendelkeznek az ESP-hez, a CIR-hez, illetve a MID-hez.

E hatóságok összesített jegyzékét közzé kell tenni az *Európai Unió Hivatalos Lapjában* az egyes interoperabilitási elemeknek a 68. cikk szerinti működésbe lépését követő három hónapon belül. A jegyzék módosulása esetén az eu-LISA évente frissített összesített jegyzéket tesz közzé.

(2) Az eu-LISA értesíti a Bizottságot a 68. cikk (1) bekezdésének b) pontjában, (2) bekezdésének b) pontjában, (3) bekezdésének b) pontjában, (4) bekezdésének (b) pontjában, (5) bekezdésének b) pontjában és (6) bekezdésének b) pontjában említett teszt sikeres befejezéséről.

(3) Az ETIAS központi egysége értesíti a Bizottságot a 65. cikkben említett átmeneti időszak sikeres befejezéséről.

(4) A Bizottság egy folyamatosan frissített nyilvános honlapon a tagállamok és a nyilvánosság rendelkezésére bocsátja az (1) bekezdés szerint bejelentett információkat.

## 68. cikk

**A működés megkezdése**

(1) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusban meghatározza azt az időpontot, amikor az ESP megkezdheti működését:

- a) elfogadták a 8. cikk (2), a 9. cikk (7) és a 43. cikk (5) bekezdésében szereplő intézkedéseket;

- b) az eu-LISA bejelentette, hogy sikeresen lezárult az ESP átfogó tesztelése, amelyet az eu-LISA az ESP használatára jogosult tagállami hatóságokkal és uniós ügynökségekkel együttműködve hajtott végre;
- c) Az eu-LISA érvényesítette a 8. cikk (1) bekezdésében említett adatok összegyűjtésére és továbbítására vonatkozó technikai és jogi előírásokat, és azokról értesítette a Bizottságot.

Az ESP csak azt követően kérdezheti le az Interpol-adatbázisokat, hogy a technikai intézkedések lehetővé teszik a 9. cikk (5) bekezdésének való megfelelést. Ha a 9. cikk (5) bekezdésének való megfelelés nem teljesíthető, akkor az ESP nem végez lekérdezést az Interpol-adatbázisokban, de ez nem késleltetheti az ESP működésének megkezdését.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

(2) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusban meghatározza azt az időpontot, amikor a közös BMS megkezdzi működését:

- a) elfogadták a 13. cikk (5) bekezdésében és a 43. cikk (5) bekezdésében említett intézkedéseket;
- b) az eu-LISA bejelentette, hogy sikeresen lezárult a közös BMS átfogó tesztelése, amelyet az eu-LISA a tagállamok hatóságaival együttműködve hajtott végre;
- c) az eu-LISA érvényesítette a 13. cikkben említett adatok összegyűjtésére és továbbítására vonatkozó technikai és jogi előírásokat, és azokról értesítette a Bizottságot;
- d) az eu-LISA bejelentette az (5) bekezdés b) pontjában említett teszt sikeres befejezését.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

(3) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusban meghatározza azt az időpontot, amikor a CIR megkezdzi működését:

- a) elfogadták a 43. cikk (5) bekezdésében és a 74. cikk (10) bekezdésében említett intézkedéseket;
- b) az eu-LISA bejelentette, hogy sikeresen lezárult a CIR átfogó tesztelése, amelyet az eu-LISA a tagállamok hatóságaival együttműködve hajtott végre;
- c) az eu-LISA érvényesítette a 18. cikkben említett adatok összegyűjtésére és továbbítására vonatkozó technikai és jogi előírásokat, és azokról értesítette a Bizottságot;
- d) az eu-LISA bejelentette az (5) bekezdés b) pontjában említett teszt sikeres befejezését.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

(4) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusban meghatározza azt az időpontot, amikor a MID megkezdzi működését:

- a) elfogadták a 28. cikk (5) és (7) bekezdésében, a 32. cikk (5) bekezdésében, a 33. cikk (6) bekezdésében, a 43. cikk (5) bekezdésében és a 49. cikk (6) bekezdésében említett intézkedéseket;
- b) az eu-LISA bejelentette, hogy sikeresen lezárult a MID átfogó tesztelése, amelyet az eu-LISA a tagállamok hatóságaival és az ETIAS központi egységével együttműködve hajtott végre;
- c) az eu-LISA érvényesítette a 34. cikkben említett adatok összegyűjtésére és továbbítására vonatkozó technikai és jogi előírásokat, és azokról értesítette a Bizottságot;
- d) az ETIAS központi egysége értesítette a Bizottságot a 67. cikk (3) bekezdésében foglaltaknak megfelelően;
- e) az eu-LISA bejelentette, hogy sikeresen lezárultak az (1) bekezdés b) pontjában, a (2) bekezdés b) pontjában, a (3) bekezdés b) pontjában és az (5) bekezdés b) pontjában említett tesztek.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

(5) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusokban meghatározza azt az időpontot, amelytől kezdődően az adatminőség ellenőrzésére irányuló automatizált mechanizmusokat és eljárásokat, a közös adatminőségi mutatókat és az adatminőségi minimumkövetelményeket alkalmazni kell:

- a) elfogadták a 37. cikk (4) bekezdésében említett intézkedéseket;

- b) az eu-LISA bejelentette, hogy sikeresen lezárult az adatminőség ellenőrzésére irányuló automatizált mechanizmusok és eljárások, a közös adatminőségi mutatók és az adatminőségi minimumkövetelmények átfogó tesztelése, amelyet az eu-LISA a tagállamok hatóságaival együttműködve hajtott végre.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

- (6) A Bizottság az alábbi feltételek teljesülését követően végrehajtási jogi aktusban meghatározza azt az időpontot, amikor a CRRS megkezdzi működését:

- a) elfogadták a 39. cikk (5) bekezdésében és a 43. cikk (5) bekezdésében említett intézkedéseket;
- b) az eu-LISA bejelentette, hogy sikeresen lezárult a CRRS átfogó tesztelése, amelyet az eu-LISA a tagállamok hatóságaival együttműködve hajtott végre;
- c) az eu-LISA érvényesítette a 39. cikkben említett adatok összegyűjtésére és továbbítására vonatkozó technikai és jogi előírásokat, és azokról értesítette a Bizottságot.

A Bizottság meghatározza az első albekezdésben említett időpontot, amelynek a végrehajtási jogi aktus elfogadásának napjától számított 30 napon belülre kell esnie.

- (7) A Bizottság tájékoztatja az Európai Parlamentet és a Tanácsot az (1) bekezdés b) pontjának, az (1) bekezdés b) pontjának, a (2) bekezdés b) pontjának, a (3) bekezdés b) pontjának, a (4) bekezdés b) pontjának, az (5) bekezdés b) pontjának és a (6) bekezdés b) pontjának megfelelően végzett tesztek eredményéről.

- (8) A tagállamok, az ETIAS központi egysége és az Europol az (1), a (2), a (3), illetve a (4) bekezdéssel összhangban a Bizottság által meghatározott időponttól megkezdik az egyes interoperabilitási elemek alkalmazását.

#### 69. cikk

### A felhatalmazás gyakorlása

- (1) A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozóan a Bizottság részére adott felhatalmazás feltételeit ez a cikk határozza meg.

(2) A Bizottságnak a 28. cikk (5) bekezdésében, a 39. cikk (5) bekezdésében, a 49. cikk (6) bekezdésében, a 63. cikk (2) bekezdésében és a 65. cikk (8) bekezdésében említett, felhatalmazáson alapuló jogi aktusok elfogadására vonatkozó felhatalmazása ötéves időtartamra szól 2019. június 11-től kezdődő hatállyal. A Bizottság legkésőbb kilenc hónappal az ötéves időtartam letelte előtt jelentést készít a felhatalmazásról. A felhatalmazás hallgatólagosan meghosszabbodik a korábbival megegyező időtartamra, amennyiben az Európai Parlament vagy a Tanács nem ellenzi a meghosszabbítást legkésőbb három hónappal minden egyes időtartam letelte előtt.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 28. cikk (5) bekezdésében, a 39. cikk (5) bekezdésében, a 49. cikk (6) bekezdésében, a 63. cikk (2) bekezdésében és a 65. cikk (8) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon, vagy a benne megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(4) A felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban foglalt elveknek megfelelően konzultál az egyes tagállamok által kijelölt szakértőkkel.

(5) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

(6) A 28. cikk (5) bekezdése, a 39. cikk (5) bekezdése, a 49. cikk (6) bekezdése, a 63. cikk (2) bekezdése és a 65. cikk (8) bekezdése értelmében elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő két hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve, ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam két hónappal meghosszabbodik.

#### 70. cikk

### Bizottsági eljárás

- (1) A Bizottság munkáját egy bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.

(2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikkét kell alkalmazni.

Ha a bizottság nem nyilvánít véleményt, a Bizottság nem fogadhatja el a végrehajtási jogi aktus tervezetét, és a 182/2011/EU rendelet 5. cikke (4) bekezdésének harmadik albekezdése alkalmazandó.

## 71. cikk

**Tanácsadó csoport**

Az eu-LISA tanácsadó csoportot hoz létre. Az interoperabilitási elemek kialakításának és fejlesztésének szakaszában az 54. cikk (4), (5) és (6) bekezdésének rendelkezéseit kell alkalmazni.

## 72. cikk

**Képzés**

Az eu-LISA az (EU) 2018/1726 rendeletnek megfelelően ellátja az interoperabilitási elemek technikai használatára vonatkozó képzés nyújtásával kapcsolatos feladatokat.

A tagállamok hatóságai és az uniós ügynökségek az interoperabilitási elemek használatával történő adatkezelésre felhatalmazott személyi állományuk számára megfelelő képzési programot biztosítanak az adatbiztonságról, az adatminőségről, az adatvédelmi szabályokról, az adatkezelési eljárásokról és a tájékoztatási kötelezettségről a 32. cikk (4) bekezdése, a 33. cikk (4) bekezdése és a 47. cikk szerint.

Szükség esetén uniós szintű közös képzéseket kell szervezni az említett témákról a tagállamok hatóságai és az uniós ügynökségek interoperabilitási elemek használatával történő adatkezelésre felhatalmazott személyi állománya közötti együttműködés fokozása és a bevált gyakorlatok megosztása céljából. Különös figyelmet kell fordítani a többszörös személyazonosság észlelésére irányuló eljárásra, többek között a különböző személyazonosságok manuális ellenőrzésére és az ezzel járó, az alapvető jogokkal kapcsolatos biztosítékok garantálása iránti igényre.

## 73. cikk

**Gyakorlati kézikönyv**

A Bizottság a tagállamokkal, az eu-LISA-val és más érintett uniós ügynökségekkel szorosan együttműködve rendelkezésre bocsátja az interoperabilitási elemek bevezetésével és igazgatásával kapcsolatos gyakorlati kézikönyvet. A gyakorlati kézikönyv technikai és üzemeltetési iránymutatásokat és ajánlásokat foglal magában, illetve példákkal szolgál a bevált gyakorlatokra. A Bizottság a gyakorlati kézikönyvet ajánlás formájában fogadja el.

## 74. cikk

**Nyomon követés és értékelés**

(1) Az eu-LISA biztosítja azoknak az eljárásoknak a kialakítását, amelyekkel nyomon követhető egyrészt a tervezéssel és a költségekkel kapcsolatos célok fényében az interoperabilitási elemek fejlesztése és egységes nemzeti interfészhez való kapcsolódása, másrészt pedig a technikai eredményekkel, a költséghatékonysággal, a biztonsággal és a szolgáltatás minőségével kapcsolatos célok fényében az interoperabilitási elemek működése.

(2) Az eu-LISA 2019. december 12-ig, majd azt követően hat havonta az interoperabilitási elemek fejlesztési szakasza során jelentést készít az Európai Parlamentnek és a Tanácsnak arról, hogy hol tart az interoperabilitási elemek fejlesztése és egységes nemzeti interfészhez való kapcsolódása. A fejlesztés befejeztével jelentést kell benyújtani az Európai Parlamentnek és a Tanácsnak, amely részletesen bemutatja a célok – különösen a tervezéssel és a költségekkel kapcsolatos célok – megvalósítását és az esetleges eltérések indokait.

(3) Az eu-LISA az egyes interoperabilitási elemek működésének 68. cikk szerinti megkezdését követően négy évvel, majd azt követően négyévente jelentést nyújt be az Európai Parlamentnek, a Tanácsnak és a Bizottságnak az interoperabilitási elemek műszaki működéséről, beleértve azok biztonságosságát is.

(4) Ezenkívül az eu-LISA minden egyes jelentése után egy évvel a Bizottság átfogó értékelést készít az interoperabilitási elemekről, beleértve a következőket:

- a) e rendelet alkalmazásának értékelése;
- b) e rendelet elért eredményeinek a célkitűzések fényében történő vizsgálata, valamint az alapvető jogokra gyakorolt hatás vizsgálata, ideértve különösen az interoperabilitási elemek megkülönböztetésmentességhez való jogra gyakorolt hatásának értékelését;
- c) a webportál működésének értékelése, beleértve a webportál használatára és a megoldott kérelmek számára vonatkozó adatokat;
- d) az interoperabilitási elemek alapjául szolgáló megfontolások változatlan helytállóságának értékelése;

- e) az interoperabilitási elemek biztonságosságának értékelése;
- f) a CIR személyazonosítás céljából történő használatának értékelése;
- g) a CIR terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából történő használatának értékelése;
- h) a rendszer működéséből fakadó következmények értékelése, beleértve a határátkelőhelyeken a forgalom áramlására gyakorolt aránytalan hatásokat, valamint az Unió általános költségvetésére hatást gyakorló következményeket;
- i) az Interpol-adatbázisokban az ESP-n keresztül végzett keresések értékelése, beleértve az Interpol-adatbázisok lekérdezéséből eredő egyezések számára és a felmerült problémákra vonatkozó adatokat.

Az e bekezdés első albekezdése szerinti átfogó értékelések szükség esetén ajánlásokat tartalmaznak. A Bizottság továbbítja az értékelésről szóló jelentést az Európai Parlamentnek, a Tanácsnak, az európai adatvédelmi biztosnak és az Európai Unió Alapjogi Ügynökségének.

(5) A Bizottság 2020. június 12-ig, majd ezt követően mindaddig, amíg a Bizottság el nem fogadta a 68. cikkben említett végrehajtási jogi aktusokat, minden évben jelentést nyújt be az Európai Parlamentnek és a Tanácsnak az e rendelet teljes körű alkalmazására vonatkozó előkészületek aktuális állásáról. Ennek a jelentésnek részletes információkat kell tartalmaznia a felmerült költségekről, valamint minden olyan kockázatról, amely hatással lehet az összköltségre.

(6) A Bizottság két évvel a MID működésének a 68. cikk (4) bekezdése szerinti megkezdése után megvizsgálja a MID hatását a megkülönböztetésmentességhez való jogra. Az első jelentést követően a MID megkülönböztetésmentességhez való jogra gyakorolt hatásának vizsgálata az e cikk (4) bekezdésének b) pontjában említett vizsgálat részét képezi.

(7) A tagállamok és az Europol az eu-LISA és a Bizottság rendelkezésére bocsátják a (3)–(6) bekezdésben említett jelentések elkészítéséhez szükséges információkat. Ez a tájékoztatás nem veszélyeztetheti a kijelölt hatóságok munkamódszereit, és nem tartalmazhat a kijelölt hatóságok információforrásait, személyi állományának tagjait, illetve nyomozásait felfedő információt.

(8) Az eu-LISA a Bizottság rendelkezésére bocsátja a (4) bekezdésben említett átfogó értékelés elkészítéséhez szükséges információkat.

(9) Az érzékeny információk közzétételére irányadó nemzeti jogszabályok rendelkezéseinek tiszteletben tartása mellett, valamint a biztonság és a közrend védelme, a bűnmegelőzés, valamint a nemzeti nyomozások veszélyeztetésének megakadályozása érdekében szükséges korlátozások sérelme nélkül minden tagállam és az Europol éves jelentést készít a CIR-ben tárolt adatok terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából történő hozzáférés eredményességéről, amely jelentés információkat és statisztikákat tartalmaz az alábbiakról:

- a) a betekintés pontos célja, beleértve a terrorista bűncselekmények vagy egyéb súlyos bűncselekmények típusait;
- b) azon megalapozott gyanú alapos indokai, miszerint a gyanúsított, az elkövető vagy az áldozat a 603/2013/EU rendelet hatálya alá tartozik;
- c) a CIR-hez terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából történő hozzáférés iránti kérelmek száma;
- d) a sikeres személyazonosítást eredményező esetek száma és típusa;
- e) a sürgősségi eseteket megalapozó kivételek szükségessége és alkalmazása, beleértve azokat az eseteket, amikor a központi hozzáférési pont az utólagos ellenőrzés során nem találta indokoltnak a sürgősséget.

A tagállamok és az Europol által készített éves jelentéseket a következő év június 30-ig kell megküldeni a Bizottságnak.

(10) A tagállamok rendelkezésére kell bocsátani egy olyan műszaki megoldást, amely kezeli a felhasználók 22. cikkben említett hozzáférés iránti kérelmeit, és megkönnyíti az e cikk (7) és (9) bekezdése szerinti információknak az említett bekezdésekben említett jelentések és statisztikák összeállítására céljából történő összegyűjtését. A Bizottság végrehajtási jogi aktusokat fogad el a műszaki megoldások előírásaival kapcsolatban. Ezeket a végrehajtási jogi aktusokat a 70. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.



## 75. cikk

**Hatálybalépés és alkalmazhatóság**

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

E rendelet ESP-vel kapcsolatos rendelkezéseit a Bizottság által a 68. cikk (1) bekezdésével összhangban meghatározott időponttól kell alkalmazni.

E rendelet közös BMS-szel kapcsolatos rendelkezéseit a Bizottság által a 68. cikk (2) bekezdésével összhangban meghatározott időponttól kell alkalmazni.

E rendelet CIR-rel kapcsolatos rendelkezéseit a Bizottság által a 68. cikk (3) bekezdésével összhangban meghatározott időponttól kell alkalmazni.

E rendelet MID-del kapcsolatos rendelkezéseit a Bizottság által a 68. cikk (4) bekezdésével összhangban meghatározott időponttól kell alkalmazni.

E rendeletnek az adatminőség ellenőrzésére irányuló, automatizált mechanizmusokkal és eljárásokkal, az adatminőségre vonatkozó közös mutatókkal és az adatminőségi minimumkövetelményekkel kapcsolatos rendelkezéseit a Bizottság által a 68. cikk (5) bekezdésével összhangban meghatározott időponttól kell alkalmazni.

E rendelet CRRS-szel kapcsolatos rendelkezéseit a Bizottság által a 68. cikk (6) bekezdésével összhangban meghatározott időponttól kell alkalmazni.

A 6., a 12., a 17., a 25., a 38., a 42., az 54., az 56., az 58., a 66., a 67., a 69., a 70., a 71. és a 73. cikket, valamint a 74. cikk (1) bekezdését 2019. június 11-től kell alkalmazni.

E rendeletet az Eurodac tekintetében a 603/2013/EU rendelet átdolgozott változata alkalmazásának kezdőnapjától kell alkalmazni.

Ez a rendelet a Szerződéseknél megfelelően teljes egészében kötelező és közvetlenül alkalmazandó a tagállamokban.

Kelt Brüsszelben, 2019. május 20-án.

az Európai Parlament részéről

az elnök

A. TAJANI

a Tanács részéről

az elnök

G. CIAMBA

---





ISSN 1977-0731 (elektronikus kiadás)  
ISSN 1725-5090 (nyomtatott kiadás)



**Az Európai Unió Kiadóhivatala**  
2985 Luxembourg  
LUXEMBURG

**HU**