TERVEZET!

2022. évi …. törvény

a Délkelet-európai Rendőri Együttműködési Egyezmény Felei között létrejött, a DNS-adatok, a daktiloszkópiai adatok és a gépjármű-nyilvántartási adatok automatizált cseréjéről szóló Megállapodás kihirdetéséről

1. §

Az Országgyűlés e törvénnyel felhatalmazást ad a Délkelet-európai Rendőri Együttműködési Egyezmény Felei között létrejött, a DNS-adatok, a daktiloszkópiai adatok és a gépjármű-nyilvántartási adatok automatizált cseréjéről szóló Megállapodás (a továbbiakban: Megállapodás) kötelező hatályának elismerésére.

2. §

Az Országgyűlés a Megállapodást e törvénnyel kihirdeti.

3. §

(1) A Megállapodás hivatalos magyar nyelvű fordítását az *1. melléklet* tartalmazza.
(2) A Megállapodás hiteles angol nyelvű szövegét a *2. melléklet* tartalmazza.

4. §

(1) Ez a törvény – a (2) bekezdésben foglalt kivétellel – a kihirdetését követő napon lép hatályba.
(2) A 2. §, a 3. §, valamint az *1. melléklet* és a *2. melléklet* a Megállapodás 26. cikkében meghatározott időpontban lép hatályba.
(3) A Megállapodás, a 2. §, 3. §, valamint az *1. melléklet* és a *2. melléklet* hatálybalépésének naptári napját a külpolitikáért felelős miniszter – annak ismertté válását követően – a Magyar Közlönyben haladéktalanul közzétett közleményével állapítja meg.

5. §

Az e törvény végrehajtásához szükséges intézkedésekről a rendészetért felelős miniszter gondoskodik.

1. melléklet a 2022. évi ... törvényhez

MEGÁLLAPODÁS
A DÉLKELET-EURÓPAI RENDŐRI EGYÜTTMŰKÖDÉSI EGYEZMÉNY FELEI KÖZÖTT LÉTREJÖTT,
A DNS-ADATOK, A DAKTILOSZKÓPIAI ADATOK ÉS A GÉPJÁRMŰ-NYILVÁNTARTÁSI ADATOK AUTOMATIZÁLT CSERÉJÉRŐL

Jelen Megállapodás Felei,

a Délkelet-Európai Rendőri Együttműködési Egyezmény alapján (a továbbiakban: PCC SEE),

azzal az óhajjal, hogy megerősítsék a határokon átnyúló együttműködést, különösen a terrorizmus, a határokon átnyúló bűnözés és az illegális migráció elleni küzdelemben, és törekedjenek a PCC SEE végrehajtására , különösen a DNS-profilok, daktiloszkópiai adatok és gépjármű-nyilvántartási adatok továbbítása és összehasonlítása terén,

tekintettel a PCC SEE Miniszteri Bizottság 11. ülésének (01/2014), a PCC SEE Miniszteri Bizottság 12. ülésének (05/2014) és a PCC SEE Miniszteri Bizottság 15. ülésének (01/2016) következtetéseire, kiemelve a DNS-adatok, a daktiloszkópiai adatok és a gépjármű-nyilvántartási adatok automatizált információcseréje fejlesztésének nagy szükségét a PCC SEE jogi keretei között,

elismerve az adatvédelem terén a PCC SEE keretében elért fejleményeket, miszerint minden Fél sikeresen teljesítette az adatvédelmi értékelést, következésképpen teljesítették a személyes adatok cseréjének feltételeit, figyelembe véve az Európai Parlament és a Tanács (EU) 2016. április 27-én kelt, 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 szóló 2016/680 irányelvét (a továbbiakban: 2016/680 (EU) irányelv), valamint az Európa Tanács vonatkozó Adatvédelmi Egyezményét és az Európa Tanács vonatkozó ajánlását a személyes adatok védelméről a rendőrségi ágazatban (a továbbiakban: az Európa Tanács vonatkozó Egyezménye és ajánlásai),

tekintettel a Belga Királyság, a Németországi Szövetségi Köztársaság, a Spanyol Királyság, a Francia Köztársaság, a Luxemburgi Nagyhercegség, a Holland Királyság és az Osztrák Köztársaság között a határon átnyúló együttműködés fokozásáról, különösen a terrorizmus, a határon átnyúló bűnözés és az illegális migráció elleni küzdelem terén 2005. május 27-én aláírt Szerződés (a továbbiakban: Prümi Szerződés), a Prümi Szerződés Végrehajtási Megállapodásainak, a Tanács 2008. június 23-án kelt, a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló 2008/615/IB Határozat (a továbbiakban: Prümi Határozat) és a Tanács 2008. június 23-án kelt, a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló 2008/615/IB határozat végrehajtásáról szóló 2008/616/IB Határozata (a továbbiakban: Prümi Végrehajtási Határozat) rendelkezéseire,

a következőkben állapodtak meg:

I. FEJEZET
Általános rendelkezések

1. cikk
Cél, hatály és fogalommeghatározások

(1) A Felek célja, hogy jelen Megállapodás által megerősítsék a határokon átnyúló rendőri együttműködésüket a közbiztonságot fenyegető veszélyek elleni küzdelemben, a bűncselekmények megelőzésében, felderítésében és nyomozásában a PCC SEE-ben lefektetettek szerint. E cél érdekében jelen Megállapodás a DNS-adatok, a daktiloszkópiai adatok és a gépjármű-nyilvántartási adatok, valamint egyezőség esetén a rendelkezésre álló további személyes és az ügyhöz kapcsolódó adatok automatizált cseréjére vonatkozóan tartalmaz szabályokat.

(2) A DNS-adatok, a daktiloszkópiai adatok és a gépjármű-nyilvántartási adatok továbbítása és összehasonlítása végrehajtásának támogatása érdekében a Felek meghatározzák:

(a) a DNS-profilok, daktiloszkópiai adatok és gépjármű-nyilvántartási adatok automatizált továbbítására vonatkozó feltételekkel és eljárással kapcsolatos rendelkezéseket;

(b) a DNS-adatok, a daktiloszkópiai adatok és a gépjármű-nyilvántartási adatok automatizált cseréjének végrehajtásához szükséges adminisztratív és technikai rendelkezéseket.

(3) Jelen Megállapodás alkalmazásában:

(a) „**keresés**” és „**összehasonlítás**”: valamely Fél által átadott DNS-adatok vagy daktiloszkópiai adatok és egy, több vagy valamennyi más Fél adatbázisában tárolt DNS-adatok vagy daktiloszkópiai adatok közötti egyezés megállapítására alkalmazott eljárások;
(b) “**automatizált keresés**”: egy, több vagy valamennyi Fél adatbázisába való betekintésre alkalmazott online hozzáférési eljárás;
(c) „**DNS-profil**”: az elemzett emberi DNS-minta nem kódoló részének azonosító jellemzőit – azaz a különböző DNS helyeken (lókuszokon) az adott molekuláris szerkezetet – megjelenítő betű- vagy számkód;
(d) „**DNS nem kódoló része**”: olyan kromoszóma régiók, amelyekről genetikai információ nem íródik át, azaz nem ismert, hogy a szervezet funkcionális jellemzőit hordoznák;
(e) „**DNS-adat**”: DNS-profil, hivatkozási szám és személyazonosító adat;
(f) „**DNS-referenciaadatok**”: DNS-profil és egy hivatkozási szám;
(g) „**referencia DNS-profil**”: ismert személy DNS-profilja;
(h) „**azonosítatlan DNS-profil**”: bűncselekmények nyomozása során gyűjtött nyomokból meghatározott, ismeretlen személyhez tartozó DNS-profil;
(i) „**megjegyzés**”: az egyik Fél által nemzeti adatbázisában a DNS-profil kapcsán tett bejegyzés, amely azt jelzi, hogy egy másik Fél által végzett keresés vagy összehasonlítás ezen DNS-profilra vonatkozóan már egyezést mutatott;
(j) „**daktiloszkópiai adatok**”: ujjnyomatok, látens ujjnyomok, tenyérnyomatok, látens tenyérnyomok, valamint ezek sablonjai (kódolt sajátossági pontok [minúciák]), ha azokat automatizált ujjlenyomat-azonosító rendszer (AFIS) adatbázisban tárolják és kezelik;
(k) „**gépjármű-nyilvántartási adatok**”: a 9. cikkben meghatározott adatok;
(l) „**személyes adat**”: az azonosított vagy azonosítható természetes személyre („adatalany”) vonatkozó bármely információ;

(m) „**személyes alapadat**”: név (családnév/nevek, utónév/nevek), születési idő, állampolgárság, nem, felvett név/nevek és születési idő/k, ujj- tenyérnyomat/DNS mintavétel dátuma, ujj- tenyérnyomat/DNS mintavétel oka, ujj- tenyérnyomat/DNS mintavétel helye és amennyiben elérhető a valós személyazonosítási státusz, lakcím, magasság, súly, útlevélszám, (arc)kép;

(n) „**egyedi eset**”: egyetlen nyomozási vagy ügyészségi ügyirat. Ha egy ilyen állomány egynél több DNS-profilt, daktiloszkópiai adatot tartalmaz, azok egyben, egy kérelemként továbbíthatók;

(o) „**személyes adatok kezelése**”: a személyes adatokkal automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége, úgymint adatok gyűjtése, rögzítése, rendszerezése, tárolása, átalakítása vagy megváltoztatása, szétválogatása, visszakeresése, az azokba való betekintés, adatok felhasználása, közlése átadás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, adatok összehangolása vagy összekapcsolása, zárolása, törlése vagy megsemmisítése. Jelen Megállapodás szerinti adatkezelés magában foglalja továbbá a találatok meglétéről szóló értesítést;

(p) „**automatizált keresési eljárás**”: egy másik Fél automatizált adatállományaihoz való közvetlen hozzáférés, amely eljárás során a válasz teljesen automatizált módon érkezik;

(q) „**eltűnt személyek**”: azon személyek, akiknek eltűnése feltehetően bűncselekmény elkövetésével, öngyilkossággal, balesettel vagy természeti katasztrófával van összefüggésben;

(r) „**egyezés/nem-egyezés**”: a (AFIS vagy DNS-egyezési) szakrendszeri ellenőrzés eredménye. Nem-egyezés esetén biztosan nincs találat. Egyezés esetén szakértői megerősítés szükséges, lehetséges, hogy az előzetesen a rendszer által egyezőnek vélt biometrikus adatok mégsem egyeznek, így a találat eredménye nem-egyezésre módosulhat;

(s) „**találat**”: szakértő által megerősített pozitív azonosítási eredmény. A szakértői vizsgálatot az igazságügyi minőségkezelési követelményeknek (pl.: akkreditációs sztenderdeknek) megfelelően kell lefolytatni;

(t) „**DNS-elemzési állományok**”: nemzeti DNS-adatbázisok és a kapcsolódó adminisztrációs alrendszerek, úgymint helyszíni nyomokat/ személyeket azonosító adatbázisok és laboratóriumi információs rendszerek, amelyek a DNS technológiával elemzett DNS-profilok bűnügyi és nyomozati megerősítésével kapcsolatos információkat tartalmazzák, és biztonságos kapcsolatot tesznek lehetővé az egyes esetekkel és a DNS-profilok személyes adataival;

(u) „**bűncselekmények**”: azon cselekmények, amelyek a Felek nemzeti jogszabályaival összhangban hivatalból üldözendők.

II. FEJEZET
ONLINE HOZZÁFÉRÉSI ÉS NYOMONKÖVETÉSI KÉRÉSEK

2. cikk
Nemzeti DNS-elemzési állományok létrehozása

(1) A Felek nemzeti DNS-elemzési állományokat nyitnak és vezetnek a bűncselekmények nyomozása, valamint az eltűnt személyek és az azonosítatlan emberi maradványok beazonosításának támogatása érdekében, a nemzeti jogszabályokkal összhangban. Az ezen állományokban tárolt adatok feldolgozását a jelen Megállapodásnak megfelelően, a PCC SEE és az adatkezelésre vonatkozó nemzeti szabályok rendelkezéseivel összhangban kell végrehajtani.

(2) Jelen Megállapodás végrehajtása érdekében a Felek biztosítják az (1) bekezdés első mondatában említett nemzeti DNS-elemzési állományokból származó referenciaadatok rendelkezésre állását. A referenciaadatok kizárólag a DNS nem kódoló szakaszai alapján létrehozott DNS-profilokat és egy hivatkozási számot tartalmaznak. A referenciaadatok nem tartalmazhatnak olyan adatokat, amelyek

alapján az adatalany közvetlenül azonosítható. A konkrét személyekhez nem kapcsolható referenciaadatok (azonosítatlan DNS-profilok) e minőségének felismerhetőnek kell lennie.

(3) Minden Fél tájékoztatja a letéteményest azokról a nemzeti DNS-elemzési állományokról, amelyekre a 2-4. és 7. cikk vonatkozik, valamint a 3. cikk (1) bekezdésében említett automatizált keresés feltételeiről.

3. cikk
DNS-profilok automatizált keresése

(1) Büntetőeljárások lefolytatása céljából, valamint az eltűnt személyek és azonosítatlan emberi maradványok azonosításában történő segítségnyújtás érdekében a Felek lehetővé teszik más Felek – a 8. cikkben említett – nemzeti kapcsolattartó pontjai számára a DNS-elemzési állományaikban lévő referenciaadatokhoz való hozzáférést, és felhatalmazzák őket a DNS-profilok összehasonlításával történő automatizált keresés végzésére. Keresést csak egyedi esetekben és a keresést végző Fél nemzeti jogszabályaival összhangban lehet folytatni.

(2) Amennyiben az automatizált keresés eredményeként valamely átadott DNS-profil egyezést mutat a fogadó Fél állományában rögzített DNS-profilokkal, a keresést végző Fél nemzeti kapcsolattartó pontja automatizált módon megkapja azokat a referenciaadatokat, amelyek alapján a találatot elérték. Egyezés hiányában a kapcsolattartó egy arról szóló automatizált értesítést kap.

4. cikk
DNS-profilok automatizált összehasonlítása

(1) Büntetőeljárások lefolytatása céljából, valamint az eltűnt személyek és azonosítatlan emberi maradványok azonosításában történő segítségnyújtás érdekében a Felek kölcsönös beleegyezés alapján és nemzeti kapcsolattartó pontjaikon keresztül összehasonlítják azonosítatlan DNS-profiljaikat az egyéb nemzeti DNS-elemzési állományok referenciaadatain alapuló valamennyi DNS-profillal. A profilokat automatizált módon kell átadni és összehasonlítani. Azonosítatlan DNS-profilokat összehasonlítás céljára kizárólag akkor kell átadni, amennyiben arról a megkereső Fél nemzeti jogszabályai rendelkeznek.

(2) Amennyiben valamely Fél az (1) bekezdésben említett összehasonlítás eredményeként úgy találja, hogy a részére átadott DNS-profilok bármelyike megegyezik valamely, a saját DNS elemzési állományában lévővel, haladéktalanul átadja a másik Fél kapcsolattartó pontjának azokat a referenciaadatokat, amelyek alapján az egyezést találták.

5. cikk
Daktiloszkópiai adatok

Jelen Megállapodás végrehajtása érdekében a Felek biztosítják a bűncselekmények megelőzése és kivizsgálása, valamint az eltűnt személyek és azonosítatlan emberi maradványok azonosításában történő segítségnyújtás céljából létrehozott nemzeti automatizált ujjnyomat-azonosító rendszer állományából származó referenciaadatok rendelkezésre állását. A referenciaadatok csak a daktiloszkópiai adatokat és egy hivatkozási számot tartalmaznak. A referenciaadatok nem tartalmazhatnak olyan adatokat, amelyek alapján az adatalany közvetlenül azonosítható. A konkrét személyekhez nem kapcsolható referenciaadatok (azonosítatlan daktiloszkópiai adatok) e

minőségének felismerhetőnek kell lennie.

6. cikk
Daktiloszkópiai adatok automatizált keresése

(1) Bűncselekmények megelőzése és vizsgálata, valamint az eltűnt személyek és azonosítatlan emberi maradványok azonosításában történő segítségnyújtás érdekében a Felek lehetővé teszik más Felek – 8. cikkben említett – nemzeti kapcsolattartó pontjai számára az általuk e célra létrehozott automatizált daktiloszkópiai azonosító rendszerben lévő referenciaadatokhoz való hozzáférést, és felhatalmazzák őket daktiloszkópiai adatok összehasonlításával történő automatizált keresés végzésére. Keresést csak egyedi esetekben és a keresést végző Fél nemzeti jogszabályaival összhangban lehet folytatni.

(2) Daktiloszkópiai adatoknak az állományt kezelő Fél kezelésében lévő referenciaadatokkal való megfelelésének megerősítését a fogadó Fél nemzeti kapcsolattartó pontja végzi az egyértelmű egyezéshez szükséges referenciaadatok automatizált átadása révén.

7. cikk
További személyes adatok és egyéb információk átadása

Amennyiben a 3. és a 4. cikkben említett eljárás DNS-adatok egyezését mutatja, vagy a 6. cikkben említett eljárás daktiloszkópiai adatok egyezését mutatja, a referenciaadatokkal kapcsolatos további rendelkezésre álló személyes adatok és egyéb információk átadására a megkeresett Fél nemzeti joga az irányadó, a jogsegélyre vonatkozó szabályokat is beleértve. A 8. cikk (2) bekezdése esetén az átadás a nemzeti kapcsolattartó ponton keresztül történik.

8. cikk
Nemzeti kapcsolattartó pontok

(1) A 3., 4. és 6. cikkben említett adatok átadása és a 7. cikkben említett rendelkezésre álló további személyes adatok, valamint a referenciaadathoz kapcsolódó egyéb információk későbbi átadása céljából minden egyes Fél nemzeti kapcsolattartó pontot jelöl ki. Ki kell jelölni a 3. és 4. cikkben a DNS-adatok vonatkozásában említett nemzeti kapcsolattartó pontot, a 6. cikkben a daktiloszkópiai adatok vonatkozásában említett nemzeti kapcsolattartó pontot, a 9. cikkben a gépjármű-nyilvántartási adatok vonatkozásában említett nemzeti kapcsolattartó pontot és a 7. cikkben a személyes adatok vonatkozásában említett nemzeti kapcsolattartó pontot.

(2) A 7. cikkben említett nemzeti kapcsolattartó pont átadja az ilyen további személyes adatokat a felelős kapcsolattartó pontot kijelölő fél nemzeti jogszabályaival összhangban. Jogsegély előterjesztésére szolgáló más elérhető csatorna használata nem szükséges, kivéve, ha a Felek nemzeti jogszabályai – a jogsegélyre vonatkozó szabályokat is beleértve – alapján arra mégis szükség van.

9. cikk
Gépjármű-nyilvántartási adatok automatizált keresése

(1) Bűncselekmények megelőzése és vizsgálata, valamint az eltűnt személyek és azonosítatlan emberi maradványok azonosításában történő segítségnyújtás, valamint a keresést végző Fél bíróságainak vagy ügyészségi hatóságainak a hatáskörébe tartozó egyéb jogsértések kezelése, továbbá a közbiztonság fenntartása érdekében a Felek lehetővé teszik más Felek nemzeti kapcsolattartó pontjai számára az alábbi nemzeti gépjármű-nyilvántartási adatokhoz való hozzáférést, és felhatalmazzák őket egyedi

esetekben automatizált keresés végzésére:

(a) tulajdonosokra vagy üzembentartókra vonatkozó adatok; és

(b) gépjárművekre vonatkozó adatok.

Keresés kizárólag teljes alvázszám vagy teljes rendszám alapján végezhető. Keresést csak a keresést végző Fél nemzeti jogszabályaival összhangban lehet folytatni.

(2) Az (1) bekezdésben említett adatok átadása céljából minden egyes Fél kijelöl egy beérkező kérelmekkel foglalkozó nemzeti kapcsolattartó pontot. A nemzeti kapcsolattartó pont hatáskörére az alkalmazandó nemzeti jog az irányadó. Az eljárásra vonatkozó technikai rendelkezések részleteit a gépjármű-nyilvántartási adatról szóló felhasználói kézikönyv tartalmazza.

III. FEJEZET
AZ ADATCSERE KERETRENDSZERRE VONATKOZÓ KÖZÖS RENDELKEZÉSEK

10. cikk
A DNS-adatok és daktiloszkópiai adatok cseréjére vonatkozó elvek

(1) A DNS- és daktiloszkópiai adatok cseréje során a Feleknek a meglévő szabványokat kell alkalmazniuk.

(2) A DNS-profilok és daktiloszkópiai adatok automatizált keresése és összehasonlítása esetén a továbbításra decentralizált struktúrában kerül sor.

(3) Megfelelő intézkedéseket kell hozni a más Felek részére történő adatküldés tárgyát képező adatok bizalmas jellegének és sértetlenségének biztosítása érdekében, beleértve azok kódolását is.

(4) A Felek megteszik a szükséges intézkedéseket a többi Fél számára hozzáférhetővé tett vagy összehasonlítás céljából átadott DNS-profilok és daktiloszkópiai adatok sértetlenségének szavatolása érdekében, valamint annak biztosítására, hogy ezen intézkedések megfeleljenek a nemzetközi szabványoknak.

11. cikk
Műszaki és eljárási előírások

(1) A Felek a DNS-profilok, a daktiloszkópiai adatok és a gépjármű-nyilvántartási adatok keresésével és összehasonlításával kapcsolatos valamennyi kérelem és válasz tekintetében betartják a közös technikai előírásokat.

(2) Ezeket a technikai előírásokat a Végrehajtási Megállapodás és a Felhasználói kézikönyvek tartalmazzák.

IV. FEJEZET
ADATVÉDELEM

12. cikk
Az adatvédelem szintje

Jelen Megállapodás keretében átadott személyes adatok tekintetében minden Fél biztosítja nemzeti jogszabályaiban a személyes adatok védelemének legalább a 2016/680 (EU) irányelvben, valamint az Európa Tanács vonatkozó Egyezményében és ajánlásaiban megfogalmazott elveknek és szabványoknak a megfelelő szintjét.

13. cikk
Cél

(1) Az átvevő Fél a személyes adatokat kizárólag az adatok átadásának jelen Megállapodáson alapuló célja érdekében dolgozhatja fel. Bármilyen más célból való felhasználás csak az állományt kezelő Fél előzetes engedélyével megengedett, és az kizárólag a fogadó Fél nemzeti jogának hatálya alá tartozik. Ilyen engedély abban az esetben adható, ha az egyéb célokat szolgáló adatkezelés az állományt kezelő Fél nemzeti joga szerint megengedett.

(2) A 3, 4. és 6. cikk értelmében átadott adatok kezelése a keresést vagy összehasonlítást végző Fél által kizárólag az alábbiak érdekében engedélyezett:

(a) az összehasonlított DNS-profilok egyezésének megállapítása;

(b) az összehasonlított daktiloszkópiai adatok egyezésének megállapítása;

(c) az adatok egyezése esetén jogsegély iránti rendőrségi vagy igazságügyi kérelem előkészítése és benyújtása a 7. és 8. cikkel összhangban kijelölt nemzeti kapcsolattartó ponton keresztül a nemzeti jogszabályoknak megfelelően;

(d) a 17. cikk szerinti jegyzőkönyvbe vétel.

(3) Az állományt kezelő Fél kizárólag akkor dolgozhatja fel a részére a 3., 4. és 6. cikknek megfelelően átadott adatokat, amennyiben az az összehasonlítás, a keresésre való automatizált válaszadás vagy a 17. cikk szerinti jegyzőkönyvbe vétel céljából szükséges. Az átadott adatokat azok összehasonlítását vagy a keresésre való automatizált válaszadást követően haladéktalanul törölni kell, amennyiben nincs szükség azok további, a második bekezdés b) és c) pontjában említett célokat szolgáló kezelésére.

(4) A 9. cikk értelmében átadott adatokat az állományt kezelő Fél kizárólag a keresési eljárásokra való automatizált válaszadás vagy a 17. cikkben meghatározott jegyzőkönyvbe vétel céljából használhatja fel. Az átadott adatokat a keresésre való automatizált válaszadást követően haladéktalanul törölni kell, amennyiben nincs szükség azok további, a 17. cikk szerinti jegyzőkönyvbe vétel célját szolgáló kezelésére. A válaszadás során a keresést végző Fél az eljárás eredményeként kapott adatokat kizárólag a keresési eljárás során meghatározott célra használhatja fel.

14. cikk
Hatáskörrel rendelkező hatóságok

Az átadott személyes adatok kizárólag a 13. cikkben említett célok elvégzéséért felelős, hatáskörrel rendelkező rendészeti hatóságok által dolgozhatók fel. Adatokat más szervek részére csak az átadó Fél előzetes engedélyével, és kizárólag az átvevő Fél nemzeti jogának megfelelően lehet átadni.

15. cikk
Az adatok pontossága, aktualitása és tárolási ideje

(1) A Feleknek biztosítaniuk kell a személyes adatok pontosságát és aktualitását. Ha a hivatali eljárás során vagy az adatalanytól származó értesítésből kiderül, hogy helytelen adatok vagy olyan adatok kerültek átadásra, amelyeket nem lett volna szabad átadni, erről haladéktalanul értesíteni kell az átvevő Felet vagy Feleket. Az érintett Fél vagy Felek kötelesek kijavítani vagy törölni az adatokat. Továbbá a helytelennek talált személyes adatokat is ki kell javítani. Ha az átvevő szerv okkal feltételezi, hogy az átadott adatok helytelenek, vagy azokat törölni kellene, akkor erről haladéktalanul tájékoztatja az átadó szervet.

(2) Azokat az adatokat, amelyek pontosságát az adatalany kétségbe vonja, valamint amelyek pontossága vagy pontatlansága nem állapítható meg, a Felek nemzeti jogszabályainak megfelelően az adatalany kérésére meg kell jelölni. Amennyiben létezik egy ilyen megjelölés, azt a Felek nemzeti jogszabályainak figyelembevételével kizárólag az adatalany engedélyével vagy az illetékes bíróság vagy a független adatvédelmi hatóság határozata alapján lehet eltávolítani.

(3) Azokat az átadott személyes adatokat, amelyeket nem lett volna szabad átadni vagy átvenni, törölni kell. A jogszerűen átadott és átvett adatokat törölni kell:

(a) ha az adatok nem vagy már nem szükségesek az átadás céljának szempontjából; amennyiben a személyes adatok kérés nélkül kerültek átadásra, az átvevő szervnek haladéktalanul ellenőriznie kell, hogy azok szükségesek-e az átadás céljának szempontjából;

(b) az átadó Fél nemzeti jogszabályaiban az adatok megőrzése tekintetében megállapított maximális időtartam lejáratát követően, amennyiben az átadó szerv az átvevő szervet az említett maximális időtartamról az adatok átadásakor tájékoztatta.

Amennyiben joggal feltételezhető, hogy az adatok törlése hátrányosan befolyásolná az adatalany érdekeit, az adatokat a nemzeti jogszabályok figyelembevételével kell tárolni.

16. cikk
Az adatvédelem és adatbiztonság biztosítása érdekében hozott technikai és szervezési intézkedések

(1) Az átadó és az átvevő szervek lépéseket tesznek annak biztosítására, hogy a személyes adatok hatékony védelemben részesüljenek a véletlen vagy jogosulatlan megsemmisítés, véletlen elvesztés, jogosulatlan hozzáférés, jogosulatlan vagy véletlen változtatás és jogosulatlan közzététel ellen.

(2) Az automatizált keresési eljárás technikai kialakításának jellemzőit a 20. cikkben említett végrehajtási intézkedések szabályozzák, amelyek garantálják, hogy:

(a) az adatvédelem és adatbiztonság biztosítása céljából sor kerüljön a technika jelenlegi állásának megfelelő olyan intézkedések meghozatalára, amelyek különösen az adatok titkosságát és sérthetetlenségét szavatolják;

(b) általánosan hozzáférhető hálózatok használata esetén a hatáskörrel rendelkező hatóságok által elismert kódolási és engedélyezési eljárásokat alkalmazzanak; és

(c) a 17. cikk (2), (4) és (5) bekezdésével összhangban ellenőrizhető legyen a keresések megengedhetősége.

17. cikk
Dokumentáció és jegyzőkönyvezés; az automatizált és a nem automatizált átadásra vonatkozó különleges szabályok

(1) Az átadás megengedhetőségének ellenőrzése érdekében minden Fél garantálja, hogy az állományt kezelő szerv és a keresést végző szerv a személyes adatok minden egyes nem automatizált átadását és nem automatizált átvételét dokumentálja. A dokumentáció a következő információkat tartalmazza:

(a) az átadás indoka;

(b) az átadott adatok;

(c) az átadás dátuma; és

(d) a keresést végző szerv és az állományt kezelő szerv neve vagy hivatkozási kódja.

(2) A 3., 4. és 6., valamint a 9. cikken alapuló automatizált adatkeresésre a következők vonatkoznak:

(a) automatizált kereséseket vagy összehasonlításokat kizárólag különleges engedéllyel rendelkező tisztviselők hajthatnak végre. Az automatizált keresések vagy összehasonlítások végrehajtására jogosult tisztviselők jegyzékét kérésre az (5) bekezdésben említett felügyeleti hatóságok és az egyéb Felek rendelkezésére kell bocsátani;

(b) minden Fél biztosítja, hogy az állományt kezelő szerv és a keresést végző szerv jegyzőkönyvet készítsen a személyes adatok minden egyes átadásáról és átvételéről, a találatról vagy annak hiányáról való értesítést is beleértve. A jegyzőkönyv a következő információkat tartalmazza:

(i) az átadott adatok;

(ii) az átadás dátuma és pontos időpontja; és

(iii) a keresést végző szerv és az állományt kezelő szerv neve vagy hivatkozási kódja.

A keresést végző szerv jegyzőkönyvbe veszi továbbá a keresés vagy az átadás indokát, valamint a keresést végrehajtó tisztviselő és a keresést vagy az átadást elrendelő tisztviselő ismertetőjelét.

(3) A jegyzőkönyvező szerv kérésre haladéktalanul közli a jegyzőkönyvbe vett adatokat az érintett Fél illetékes adatvédelmi hatóságaival, legkésőbb a kérelem kézhezvételétől számított négy héten belül. A jegyzőkönyvbe vett adatokat kizárólag a következő célokra lehet felhasználni:

(a) az adatvédelem ellenőrzése;

(b) az adatbiztonság biztosítása.

(4) A jegyzőkönyvbe vett adatokat megfelelő intézkedések segítségével védeni kell a nem megfelelő felhasználással és a helytelen felhasználás egyéb formáival szemben, valamint két évig meg kell őrizni azokat. A megőrzési idő lejárta után a jegyzőkönyvbe vett adatokat haladéktalanul törölni kell.

(5) A személyes adatok átadásának vagy átvételének jogi ellenőrzése a Felek független adatvédelmi hatóságainak, vagy adott esetben igazságügyi hatóságainak a feladata. A nemzeti jogszabályok figyelembevételével bárki felkérheti ezeket a hatóságokat arra, hogy azok ellenőrizzék a személyükre vonatkozó adatok kezelésének jogszerűségét. Ezek és a jegyzőkönyvezésért felelős hatóságok az ilyen kérésektől függetlenül az érintett állományok alapján szúrópróbaszerűen is ellenőrzik az átadás jogszerűségét.

(6) A független adatvédelmi hatóságok ellenőrzés céljából 18 hónapig megőrzik az ilyen ellenőrzések eredményeit. Ezen időtartam lejárta után haladéktalanul törlik ezeket. A nemzeti jogszabályokkal összhangban minden adatvédelmi hatóság felkérést kaphat egy másik Fél független adatvédelmi hatóságától hatáskörei gyakorlására. A Felek független adatvédelmi hatóságai – különösen a célirányos információk cseréje révén – elvégzik a kölcsönös együttműködéshez szükséges ellenőrzési feladatokat.

18. cikk
Az adatalanyok tájékoztatáshoz és kártérítéshez fűződő jogai

(1) Az adatalany részére személyazonossága igazolása után a nemzeti jogszabályok szerinti adatalany kérésére a nemzeti jogszabályok figyelembevételével, indokolatlan költségek nélkül, közérthető formában és elfogadhatatlan késedelem nélkül tájékoztatást kell nyújtani a személye tekintetében feldolgozott adatokról, az adatok eredetéről, az átvevőről vagy az átvevők kategóriáiról, az adatkezelés tervezett céljáról és – amennyiben a nemzeti jogszabályok előírják – a kezelés jogalapjáról. Ezen túlmenően az adatalanynak jogában áll a téves adatokat kijavíttatni és a jogszerűtlenül feldolgozott adatokat töröltetni. A Felek biztosítják továbbá, hogy az adatalany az adatvédelemmel kapcsolatos jogainak megsértése esetén panaszt nyújthat be egy, az emberi jogokról szóló európai egyezmény 6. cikke (1) bekezdésének megfelelően felállított független bírósághoz vagy törvényszékhez, vagy egy a nemzeti jogszabályok alapján és a 2016/680 (EU) irányelv, a valamint az Európa Tanács vonatkozó Egyezményében és ajánlásaiban megfogalmazott szabványok szerint létrejött független adatvédelmi hatósághoz, továbbá biztosítják, hogy az adatalanynak lehetősége legyen kártérítést követelni, vagy egyéb típusú jogi elégtétellel élni. Az ezen jogok érvényesítésére irányuló eljárás részleteire és a tájékoztatáshoz való jog korlátozásának indokaira azon Fél vonatkozó nemzeti jogszabályai az irányadóak, amelyben az adatalany jogait érvényesíti.

(2) Amennyiben valamely Fél egy szerve jelen Megállapodás értelmében személyes adatot adott át, a másik Fél fogadó szervezete nem használhatja fel az átadott adatok pontatlanságát jogalapként a sértett

féllel szembeni, a nemzeti jogszabályok szerinti felelőssége elhárításához. Ha a tévesen továbbított adatok felhasználása miatt az átvevő szervvel szemben kártérítést ítélnek meg, a kártérítésként kifizetett összeget az adatokat átadó szerv teljes mértékben megtéríti az átvevő szervnek.

19. cikk
A Felek által kért információ

Az átvevő Fél kérelemre tájékoztatja az átadó Felet az átadott adatok kezeléséről és az ezáltal elért eredményekről.

V. FEJEZET
ZÁRÓ RENDELKEZÉSEK

20. cikk
A Végrehajtási Megállapodás és a Felhasználói kézikönyvek

(1) Jelen Megállapodás alapján és alkalmazási körén belül a Felek az adminisztratív végrehajtásról Végrehajtási Megállapodást kötnek.

(2) A Felek képviselőit tömörítő szakértői munkacsoport Felhasználói kézikönyveket készít és tart naprakészen. A Felhasználói kézikönyvek a hatékony és eredményes információcseréhez szükséges adminisztratív és technikai információkat tartalmaznak.

21. cikk
Az adatcsere értékelése

(1) A Megállapodás II. fejezete szerinti adatcsere adminisztratív, technikai és pénzügyi alkalmazása értékelésének meg kell történnie. Az értékelést az adatcsere megkezdése előtt kell elvégezni. Szükség esetén az megismételhető a Megállapodás már alkalmazó Felek esetében. Az értékelést azon adatkategóriák tekintetében kell elvégezni, amelyek vonatkozásában az adatcsere az érintett Felek között már megkezdődött. Az értékelés az adott Felek jelentésein alapul.

(2) Az értékelést a Felek képviselőiből álló közös munkacsoport hatja végre. A munkacsoport valamely fél kérésére vagy ötévente rendszeresen ülésezik.

22. cikk
Más nemzetközi megállapodásokkal való kapcsolat

(1) Jelen Megállapodás nem érinti a Felek azon más nemzetközi megállapodásokból származó jogait, kötelezettségeit és felelősségét, amelyeknek részes felei.

(2) Amennyiben jelen Megállapodás kifejezetten másként nem rendelkezik, az együttműködés a Felek vonatkozó nemzeti jogszabályai szerint történik.

23. cikk
Végrehajtás és nyilatkozatok

(1) A Felek tájékoztatják a letéteményest arról, hogy a jelen Megállapodásból fakadó kötelezettségeket végrehajtották, és a Megállapodással összhangban kijelölték a nemzeti kapcsolattartó pontokat.

(2) Amennyiben a Fél jelen Megállapodás (21. cikk) alapján vagy az Európai Unió által pozitív értékelést kapott, egyúttal felhatalmazást kap arra, hogy jelen Megállapodást haladéktalanul alkalmazza azon többi Féllel szemben, akik szintén pozitív elbírálásban részesültek. Az érintett Fél ennek megfelelően tájékoztatja a letéteményest.

(3) Az (1) bekezdéssel összhangban tett nyilatkozatokat tetszőleges időpontban lehet módosítani.

24. cikk
Letéteményes

(1) Jelen Megállapodás letéteményese a Szerb Köztársaság.

(2) A letéteményes minden Félnek megküldi a Megállapodás hiteles másolatát.

(3) A letéteményes értesíti a Feleket bármilyen megerősítő, elfogadó, jóváhagyó vagy csatlakozási okirat letétbe helyezéséről vagy a Megállapodással kapcsolatban tett bármely nyilatkozatról, álláspontról vagy értesítésről.

(4) A letéteményes értesíti a Feleket jelen Megállapodásnak bármely, a 26. cikk szerinti hatálybalépési időpontjáról.

25. cikk
Megerősítés, elfogadás, jóváhagyás, csatlakozás vagy fenntartások

(1) Jelen Megállapodást a Feleknek meg kell erősíteniük, el kell fogadniuk vagy jóvá kell hagyniuk. A megerősítő, elfogadó vagy jóváhagyó okiratokat az Megállapodás letéteményesénél kell letétbe helyezni.

(2) Jelen Megállapodás csatlakozásra nyitva áll a Délkelet-Európai Rendőri Egyezmény bármely Fele számára. A csatlakozási okiratot a letéteményesnél kell letétbe helyezni.

(3) Jelen Megállapodással kapcsolatban fenntartásnak nincs helye.

26. cikk
Hatálybalépés

(1) Jelen Megállapodás a második megerősítő, elfogadó, jóváhagyó vagy csatlakozási okirat letétbe helyezésének napját követő hatvanadik napon lép hatályba.

(2) A Megállapodás a második megerősítő, elfogadó, jóváhagyó vagy csatlakozási okirat letétbe helyezését követően a Megállapodást megerősítő, elfogadó, jóváhagyó vagy ahhoz csatlakozó minden Fél esetében az ilyen Fél megerősítő, elfogadó, jóváhagyó vagy csatlakozási okiratának letétbe helyezését követő hatvanadik napon lép hatályba.

27. cikk
Felmondás és felfüggesztés

(1) Jelen Megállapodás határozatlan időre kerül megkötésre.

(2) Bármelyik Fél bármikor felmondhatja az Megállapodást a letéteményeshez intézett írásos értesítés útján. A felmondás az értesítésnek a letéteményes által történő kézhezvétel időpontjától számított hat hónapot követően válik hatályossá.

(3) Az átadott adat vonatkozásában a IV. fejezetben rögzített rendelkezéseket jelen Megállapodás megszűnése esetén is megfelelően alkalmazni kell.

(4) Jelen Megállapodást egészében, vagy részben bármely Fél felfüggesztheti, ha azt a közrend, a nemzetbiztonság vagy a közegészségügy védelme szükségessé teszi. A Felek haladéktalanul értesítik a letéteményest az ilyen intézkedések megtételéről vagy visszavonásáról. A jelen bekezdés alapján tett bármely intézkedés az értesítésnek a letéteményes által történő kézhezvétel időpontjától számított 15. naptól követően válik hatályossá.

(5) A letéteményes haladéktalanul értesíti a többi Felet a felmondásról vagy felfüggesztésről szóló értesítésről.

Fentiek tanúbizonyságául, az alulírott és az erre felhatalmazott megbízottak jelen Megállapodást aláírásukkal látták el.

az Albán Köztársaság részéről

az Osztrák Köztársaság részéről

Bosznia-Hercegovina részéről

a Bolgár Köztársaság részéről

Magyarország részéről

a Macedón Köztársaság részéről

a Moldovai Köztársaság részéről

Montenegró részéről

Románia részéről

a Szerb Köztársaság részéről

a Szlovén Köztársaság részéről

Készült Bécsben, 2018. szeptember 13. napján, egyetlen eredeti példányban, angol nyelven.

2. melléklet a 2022. évi … törvényhez

AGREEMENT
BETWEEN THE PARTIES TO THE POLICE COOPERATION CONVENTION
FOR SOUTHEAST EUROPE
ON THE AUTOMATED EXCHANGE OF DNA DATA, DACTYSLOSCOPIC DATA
AND VEHICLE REGISTRATION DATA

The Parties to this Agreement,

Based on the Police Cooperation Convention for Southeast Europe (hereinafter referred to as: "the PCC SEE"),

Desirous of strengthening cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration and endeavouring the implementation of the PCC SEE, in particular on the transmission and comparison of DNA profiles, dactyloscopic data and vehicle registration data,

Having in mind the Conclusions of the 11th PCC SEE Committee of Ministers (01/2014), the Conclusions of the 12th PCC SEE Committee of Ministers (05/2014) and the Conclusions of the 15th PCC SEE Committee of Ministers (01/2016), highlighting the strong need for the development of automated DNA data, dactyloscopic data and vehicle registration data information exchange, within the PCC SEE legal framework,

Acknowledging the PCC SEE developments in the Area of Data Protection, where all Parties have successfully passed the evaluations in the area of personal data protection and have, consequently, fulfilled the preconditions to exchange personal data, while taking into account the common European data protection principles and standards as enshrined in Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereinafter referred to as: "Directive (EU) 2016/680") and the relevant Convention of the Council of Europe on Protection of Personal Data and relevant Council of Europe recommendation for protection of personal data for the Police sector (hereinafter referred to as: "relevant Council of Europe Convention and recommendations"),

Having in mind the provisions deriving from the Treaty of 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration (hereinafter referred to as: "the Prüm Treaty"), the Implementing Agreement of the Prüm Treaty, the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (hereinafter referred to as: "the Prüm Decision") and the Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (hereinafter referred to as: "the Prüm Implementing Decision"),

Have agreed as follows:

CHAPTER I
General Provisions

Article 1
Aim, scope and definitions

(1) By means of this Agreement, the Parties intend to strengthen cross-border police cooperation with respect to fighting threats to public security with respect to prevention, detection and investigation of criminal offences as laid down in the PCC SEE. To this end, this Agreement contains rules for automated exchange of DNA data, dactyloscopic data and vehicle registration data and exchange of available subsequent personal and case-related data in case of a hit.

(2) For supporting the implementation of the transmission and comparison of DNA data, dactyloscopic data and vehicle registration data the Parties lay down:

(a) provisions on the conditions and procedure for the automated transfer of DNA profiles, dactyloscopic data and vehicle registration data;

(b) the necessary administrative and technical provisions for the implementation of automated exchange of DNA data, dactyloscopic data and vehicle registration data.

(3) For the purposes of this Agreement:

(a) "**search**" and "**comparison**" mean the procedures by which it is established whether there is a match between, respectively, DNA data or dactyloscopic data which have been communicated by one Party and DNA data or dactyloscopic data stored in the databases of one, several, or all of the Parties;
(b) "**automated searching**" means an online access procedure for consulting the databases of one, several, or all of the Parties;
(c) "**DNA profile**" means a letter or number code which represents a set of identification characteristics of the non-coding part of an analysed human DNA sample, i.e. the particular molecular structure at the various DNA locations (loci);
(d) "**non-coding part of DNA**" means chromosome regions not genetically expressed, i.e. not known to provide for any functional properties of an organism;
(e) "**DNA data**" mean DNA profile, reference number and personal identification data;
(f) "**DNA reference data**" mean DNA profile and reference number;
(g) "**reference DNA profile**" means the DNA profile of an identified person;
(h) "**unidentified DNA profile**" means the DNA profile obtained from traces collected during the investigation of criminal offences and belonging to a person not yet identified;
(i) "**note**" means a Party's marking on a DNA profile in its national database indicating that there has already been a match for that DNA profile on another Party's search or comparison;
(j) "**dactyloscopic data**" mean fingerprint images, images of fingerprint latents, palm prints, palm print latents and templates of such images (coded minutiae), when they are stored and dealt within an automated fingerprint identification system (AFIS) database;
(k) "**vehicle registration data**" mean the data-set as specified in Article 9;
(l) "**personal data**" shall mean any information relating to an identified or identifiable natural person (the "data subject");

(m)"**core personal data**" means Name (Family Name(s), First Name(s)), Date of Birth, Nationality, Gender, Alias Name(s) and Date(s) of Birth, Date Fingerprinted / DNA sampled, Reason Fingerprinted / DNA sampled, Place Fingerprinted / DNA sampled, and if available True Identity Confirmation Status, Address, Height, Weight, Number of Passport, Picture (Face);

(n) "**individual case**" means a single investigation or prosecution file. If such a file contains more than one DNA profile or one piece of dactyloscopic data they may be transmitted together as one request;

(o) "**processing of personal data**" means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, sorting, retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, alignment, combination, erasure or destruction of data. Processing within the meaning of this Agreement shall also include notification of whether or not a hit exists;

(p) "**automated search procedure**" means online access to the databases of another Party where the response to the search procedure is fully automated;

(q) "**missing persons**" means persons whose absence is assumed in connection to a crime, a suicide, an accident or a disaster;

(r) "**match / no-match**" means the result of a machine (AFIS or DNA-match-engine). It would also mean that a no-match is always a no-hit. On the other hand it is also possible that a match is a no-hit after the necessary forensic verification / validation;

(s) "**hit**" means the confirmed positive identification result confirmed by a human being (expert) after forensic verification / validation. Forensic confirmation has to be carried out in line with forensic quality management requirements (e.g. accreditation standards);

(t) "**DNA analysis files**" mean national DNA databases and linked administrative subsystems as e.g. crime scene stain / person identification databases and lab information systems (LIMs), which contain all relevant information for forensic and investigative confirmation of DNA profiles analysed with DNA technologies and will allow also secure linkage to Individual case / personal data of DNA profiles;

(u) "**criminal offences**" mean those offences which are prosecuted ex officio in accordance with the Parties' national legislation.

CHAPTER II
ONLINE ACCESS AND FOLLOW-UP REQUESTS

Article 2
Establishment of national DNA analysis files

(1) The Parties shall open and keep national DNA analysis files for the investigation of criminal offences and to assist in the identification of missing persons and unidentified human remains in accordance with the national legislation. Processing of data kept in those files, under this Agreement, shall be carried out in accordance with this Agreement, in compliance with the PCC SEE and the national legislation applicable to the data processing.

(2) For the purpose of implementing this Agreement, the Parties shall ensure the availability of reference data from their national DNA analysis files as referred to in the first sentence of paragraph 1. Reference data shall only include DNA profiles established from the non-coding part of DNA and a reference number. Reference data shall not contain any data from which the data subject can be directly

identified. Reference data which is not attributed to any individual (unidentified DNA profiles) shall be recognisable as such.

(3) Each Party shall inform the Depositary of the national DNA analysis files to which Articles 2 to 4 and Article 7 apply and the conditions for automated searching as referred to in Article 3(1).

Article 3
Automated searching of DNA profiles

(1) For the investigation of criminal offences and to assist in the identification of missing persons and unidentified human remains, the Parties shall allow other Parties' national contact points as referred to in Article 8, access to the reference data in their DNA analysis files, with the power to conduct automated searches by comparing DNA profiles. Searches may be conducted only in individual cases and in compliance with the requesting Party's national legislation.

(2) Should an automated search show that a DNA profile supplied matches DNA profiles entered in the receiving Party's searched file, the national contact point of the searching Party shall receive in an automated way the reference data with which a match has been found. If no match can be found, automated notification of this shall be given.

Article 4
Automated comparison of DNA profiles

(1) For the investigation of criminal offences and to assist in the identification of missing persons and unidentified human remains, the Parties shall, by mutual consent, via their national contact points, compare the DNA profiles of their unidentified DNA profiles with all DNA profiles from other national DNA analysis files' reference data. Profiles shall be supplied and compared in automated form. Unidentified DNA profiles shall be supplied for comparison only where provided for under the requesting Party's national legislation.

(2) Should a Party, as a result of the comparison referred to in paragraph 1, find that any DNA profiles supplied match any of those in its DNA analysis files, it shall, without delay, supply the other Party's national contact point with the DNA reference data with which a match has been found.

Article 5
Dactyloscopic data

For the purpose of implementing this Agreement, Parties shall ensure the availability of reference data from the file for the national automated fingerprint identification systems established for the prevention and investigation of criminal offences and to assist in the identification of missing persons and unidentified human remains. Reference data shall only include dactyloscopic data and a reference number. Reference data shall not contain any data from which the data subject can be directly identified. Reference data which is not attributed to any individual (unidentified dactyloscopic data) must be recognisable as such.

Article 6
Automated searching of dactyloscopic data

(1) For the prevention and investigation of criminal offences and to assist in the identification of missing persons and unidentified human remains, Parties shall allow other Parties' national contact points, as referred to in Article 8, access to the reference data in the automated fingerprint identification systems which they have established for that purpose, with the power to conduct automated searches by comparing dactyloscopic data. Searches may be conducted only in individual cases and in compliance with the requesting Party's national legislation.

(2) The confirmation of a match of dactyloscopic data with reference data held by the Party administering the file shall be carried out by the national contact point of the requesting Party by means of the automated supply of the reference data required for a hit.

Article 7
Supply of further personal data and other information

Should the procedures referred to in Articles 3 and 4 show a hit between DNA profiles or the procedures referred to in Article 6 show a hit between dactyloscopic data, the supply of further available personal data in addition to core personal data and other information relating to the reference data shall be governed by the national legislation, including the legal assistance rules, of the requested Party. Subject to Article 8 paragraph 2, the supply will be provided by a national contact point.

Article 8
National contact points

(1) For the purposes of the supply of data as referred to in Articles 3, 4 and 6, and subsequent supply of further available personal data and other information relating to the reference data, as referred to in Article 7, each Party shall designate national contact points. It shall indicate the national contact point, mentioned in Articles 3 and 4 for DNA data, the national contact point, mentioned in Article 6 for dactyloscopic data, the national contact point, mentioned in Article 9 for vehicle registration data and the national contact point, mentioned in Article 7 for personal data.

(2) The national contact point as referred to in Article 7 shall supply such subsequent personal data in accordance with the national legislation of the Party designating the responsible contact point. Other available legal assistance channels need not be used unless necessary in accordance with the national legislation, including the legal assistance rules, of the Parties.

Article 9
Automated searching of vehicle registration data

(1) For the prevention and investigation of criminal offences and to assist in the identification of missing persons and unidentified human remains and in dealing with other offences coming within the jurisdiction of the courts or the public prosecution service in the searching Party, as well as in maintaining public security, Parties shall allow other Parties' national contact points, access to the following national vehicle registration data, with the power to conduct automated searches in individual cases:

(a) data relating to owners or operators; and

(b) data relating to vehicles.

Searches may be conducted only with a full chassis number or a full registration number. Searches may be conducted only in compliance with the searching Party's national legislation.

(2) For the purposes of the supply of data as referred to in paragraph 1, each Party shall designate a national contact point for incoming requests. The powers of the national contact points shall be governed by the applicable national legislation. Details of technical arrangements for the procedure shall be laid down in a vehicle registration data User manual.

CHAPTER III
COMMON PROVISIONS ON THE FRAMEWORK FOR DATA EXCHANGE

Article 10
Principles of DNA and dactyloscopic data exchange

(1) The Parties shall use existing standards for DNA and dactyloscopic data exchange.

(2) The transmission procedure, in case of automated searching and comparison of DNA profiles and of dactyloscopic data shall take place within a decentralised structure.

(3) Appropriate measures shall be taken to ensure confidentiality and integrity for data being sent to other Parties, including their encryption.

(4) The Parties shall take the necessary measures to guarantee the integrity of the DNA profiles and dactyloscopic data made available or sent for comparison to the other Parties and to ensure that these measures comply with international standards.

Article 11
Technical and procedural specifications

(1) The Parties shall observe common technical specifications in connection with all requests and answers related to searches and comparisons of DNA profiles, dactyloscopic data and vehicle registration data.

(2) These technical and procedural specifications are laid down in the Implementing Agreement and User manuals.

CHAPTER IV
DATA PROTECTION

Article 12
Level of data protection

As regards the processing of personal data which are or have been supplied pursuant to this Agreement, each Party shall in its national legislation ensure an adequate level of protection of personal data

essentially equivalent to the principles and standards enshrined in Directive (EU) 2016/680 and the relevant Council of Europe Convention and recommendations.

Article 13
Purpose

(1) Processing of personal data by the receiving Party shall be permitted solely for the purposes for which the data have been supplied in accordance with this Agreement. Processing for other purposes shall be permitted solely with the prior authorisation of the Party administering the file and subject only to the national legislation of the receiving Party. Such authorisation may be granted provided that processing for such other purposes is permitted under the national legislation of the Party administering the file.

(2) Processing of data supplied pursuant to Articles 3, 4 and 6 by the searching or comparing Party shall be permitted solely in order to:

(a) establish whether there is a match between the compared DNA profiles;

(b) establish whether there is a match between the compared dactyloscopic data;

(c) prepare and submit a police or judicial request for legal assistance in compliance with national legislation if there is a hit between those data via the national contact point designated in accordance with Articles 7 and 8;

(d) record within the meaning of Article 17.

(3) The Party administering the file may process the data supplied to it in accordance with Articles 3, 4 and 6 solely where this is necessary for the purposes of comparison, providing automated replies to searches or recording pursuant to Article 17. The supplied data shall be deleted immediately following data comparison or automated replies to searches unless further processing is necessary for the purposes mentioned under points (b) and (c) of the second paragraph.

(4) Data supplied in accordance with Article 9 may be used by the Party administering the file solely where this is necessary for the purpose of providing automated replies to search procedures or recording as specified in Article 17. The data supplied shall be deleted immediately following automated replies to searches unless further processing is necessary for recording pursuant to Article 17. The searching Party may use data received in a reply solely for the procedure for which the search was made.

Article 14
Competent authorities

Personal data supplied may be processed only by the competent law enforcement authorities with responsibility for a task in furtherance of the aims mentioned in Article 13. In particular, data may be supplied to other entities only with the prior authorisation of the supplying Party and in compliance with the national legislation of the receiving Party.

Article 15
Accuracy, current relevance and storage time of data

(1) The Parties shall ensure the accuracy and current relevance of personal data. Should it transpire ex officio or from a notification by the data subject that incorrect data or data which should not have been supplied have been supplied, this shall be notified without delay to the receiving Party or Parties. The Party or Parties concerned shall be obliged to correct or delete the data. Moreover, personal data supplied shall be corrected if they are found to be incorrect. If the receiving body has reason to believe that the supplied data are incorrect or should be deleted the supplying body shall be informed forthwith.

(2) Data, the accuracy of which the data subject contests and the accuracy or inaccuracy of which cannot be established shall, in accordance with the national legislation of the Parties, be marked with a flag at the request of the data subject. If a flag exists, this may be removed subject to the national legislation of the Parties and only with the permission of the data subject or based on a decision of the competent court or independent data protection authority.

(3) Personal data supplied which should not have been supplied or received shall be deleted. Data which are lawfully supplied and received shall be deleted:

(a) if they are not or no longer necessary for the purposes for which they were supplied; if personal data have been supplied without request, the receiving body shall immediately check if they are necessary for the purposes for which they were supplied;

(b) following the expiry of the maximum period for keeping data laid down in the national legislation of the supplying Party where the supplying body informed the receiving body of that maximum period at the time of supplying the data.

Where there is reason to believe that deletion would prejudice the interests of the data subject, the data shall be kept in accordance with the national legislation.

Article 16
Technical and organisational measures to ensure data protection and data security

(1) The supplying and receiving bodies shall take steps to ensure that personal data is effectively protected against accidental or unauthorised destruction, accidental loss, unauthorised access, unauthorised or accidental alteration and unauthorised disclosure.

(2) The features of the technical specification of the automated search procedure are regulated in the implementing measures as referred to in Article 20 which guarantee that:

(a) state-of-the-art technical measures are taken to ensure data protection and data security, in particular data confidentiality and integrity;

(b) encryption and authorisation procedures recognised by the competent authorities are used when having recourse to dedicated networks; and

(c) the admissibility of searches in accordance with Article 17 (2), (4) and (5) can be checked.

Article 17
Logging and recording: special rules governing automated and non-automated supply

(1) Each Party shall guarantee that every non-automated supply and every non-automated receipt of personal data by the body administering the file and by the searching body is logged in order to verify the admissibility of the supply. Logging shall contain the following information:

(a) the reason for the supply;

(b) the data supplied;

(c) the date of the supply; and

(d) the name or reference code of the searching body and of the body administering the file.

(2) The following shall apply to automated searches for data based on Articles 3, 4 and 6 and Article 9:

(a) only specially authorised officers may carry out automated searches or comparisons. The list of officers authorised to carry out automated searches or comparisons shall be made available upon request to the supervisory authorities referred to in paragraph 5 and to the other Parties;

(b) each Party shall ensure that each supply and receipt of personal data by the body administering the file and the searching body is recorded, including notification of whether or not a match exists. Recording shall include the following information:

(i) the data supplied;

(ii) the date and exact time of the supply; and

(iii)the name or reference code of the searching body and of the body administering the file.

The searching body shall also record the reason for the search or supply as well as an identifier for the official who carried out the search and the official who ordered the search or supply.

(3) The recording body shall immediately communicate the recorded data upon request to the competent data protection authorities of the relevant Party at the latest within four weeks following receipt of the request. Recorded data may be used solely for the following purposes:

(a) monitoring data protection;

(b) ensuring data security.

(4) The recorded data shall be protected with suitable measures against inappropriate use and other forms of improper use and shall be kept for two years. After the conservation period the recorded data shall be deleted immediately.

(5) Responsibility for legal checks on the supply or receipt of personal data lies with the independent data protection authorities or, as appropriate, the judicial authorities of the respective Parties. Anyone can request these authorities to check the lawfulness of the processing of data in respect of their person in compliance with national legislation. Independently of such requests, these authorities and the bodies responsible for recording shall carry out random checks on the lawfulness of supply, based on the files involved.

(6) The results of such checks shall be kept for inspection for 18 months by the independent data protection authorities. After this period, they shall be immediately deleted. Each data protection authority may be requested by the independent data protection authority of another Party to exercise its powers in accordance with national legislation. The independent data protection authorities of the Parties shall perform the inspection tasks necessary for mutual cooperation, in particular by exchanging relevant information.

Article 18
Data subjects' rights to information and damages

(1) At the request of the data subject under national legislation, information shall be supplied in compliance with national legislation to the data subject upon production of proof of identity, without unreasonable expense, in general comprehensible terms and without unacceptable delays, on the data processed in respect of the person, the origin of the data, the recipient or groups of recipients, the intended purpose of the processing and, where required by national legislation, the legal basis for the processing. Moreover, the data subject shall be entitled to have inaccurate data corrected and unlawfully processed data deleted. The Parties shall also ensure that, in the event of violation of the rights in relation to data protection, the data subject shall be able to lodge an effective complaint to an independent court or a tribunal within the meaning of Article 6(1) of the European Convention on Human Rights or an independent data protection authority established by national legislation according to the standards essentially equivalent to Directive (EU) 2016/680 and the relevant Council of Europe Convention and recommendations and that the data subject is given the possibility to claim for damages or to seek another form of legal compensation. The detailed rules for the procedure to assert these rights and the reasons for limiting the right of access shall be governed by the relevant national legislation of the Party where the data subject asserts these rights.

(2) Where a body of one Party has supplied personal data under this Agreement, the receiving body of the other Party cannot use the inaccuracy of the data supplied as grounds to evade its liability vis-à-vis the injured Party under national legislation. If damages are awarded against the receiving body because of its use of inaccurate transfer data, the body which supplied the data shall refund the amount paid in damages to the receiving body in full.

Article 19
Information requested by the Parties

The receiving Party shall inform the supplying Party on request of the processing of supplied data and the result obtained.

CHAPTER V
FINAL PROVISIONS

Article 20
Implementing Agreement and User manuals

(1) On the basis and within the scope of this Agreement, the Parties shall conclude an agreement for its implementation.

(2) User manuals shall be prepared and kept up to date by expert working groups composed of representatives of the Parties. User manuals contain administrative and technical information needed for efficient and effective exchange of data.

Article 21
Evaluation of the data exchange

(1) An evaluation of the administrative, technical and financial application of the data exchange pursuant to Chapter II of this Agreement shall be carried out. The evaluation must be carried out before starting the data exchange. If needed, the evaluation can be repeated for those Parties already applying this Agreement. The evaluation shall be carried out with respect to the data categories for which data exchange has started among the Parties concerned. The evaluation shall be based on reports of the respective Parties.

(2) The evaluation shall be carried out by a joint working group made up of representatives of the Parties. The working group shall meet at the request of a Party or on a regular basis every five years.

Article 22
Relationship with other international agreements

(1) This Agreement shall not affect any rights, obligations and responsibilities of the Parties arising from other international agreements to which they are parties.

(2) Unless otherwise stipulated explicitly in this Agreement, cooperation shall be performed within the scope of the respective national legislation of the Parties.

Article 23
Implementation and Application

(1) The Parties shall inform the Depositary that they have implemented the obligations imposed on them under this Agreement and designated national contact points according to this Agreement.

(2) Once a positive evaluation of a Party in the context of this Agreement (Article 21) or the European Union has been made, the respective Party is entitled to apply this Agreement immediately in relation to all other Parties which also have been evaluated positively. The respective Party shall inform the Depositary accordingly.

(3) Declarations submitted in accordance with paragraph 1 of this Article may be amended at any time.

Article 24
Depositary

(1) Depositary of this Agreement is the Republic of Serbia.

(2) The Depositary shall send a certified copy of this Agreement to each Party.

(3) The Depositary shall notify the Parties of the deposit of any instrument of ratification, acceptance, approval or accession, of any declarations, statements or notifications made in connection with this Agreement.

(4) The Depositary shall notify all Parties on any date of entry into force of this Agreement in accordance with Article 26.

Article 25
Ratification, Acceptance, Approval, Accession or Reservation

(1) This Agreement is subject to ratification, acceptance, or approval of the Parties. The instruments of ratification, acceptance or approval shall be deposited with the Depositary.

(2) This Agreement shall be open for accession by any PCC SEE Party. The instrument of accession shall be deposited with the Depositary.

(3) No reservations may be made to this Agreement.

Article 26
Entry into Force

(1) This Agreement shall enter into force on the sixtieth day following the date of the deposit of the second instrument of ratification, acceptance, approval, or accession.

(2) For each Party ratifying, accepting, approving, or acceding to this Agreement after the deposit of the second instrument of ratification, acceptance, approval, or accession, the Agreement shall enter into force on the sixtieth day after deposit by such Party of its instrument of ratification, acceptance, approval, or accession.

Article 27
Withdrawal and Suspension

(1) This Agreement shall be concluded for an indefinite period of time.

(2) Any Party may withdraw from this Agreement at any time by written notification to the Depositary. The withdrawal shall take effect six months after the date of receipt of the notification by the Depositary.

(3) Regardless of the termination of this Agreement the provisions laid down in Chapter IV shall apply regarding to the processed data.

(4) Any Party may suspend the operation of this Agreement in full or in part if necessary for reasons of public order, protection of national security or protection of public health. The Parties shall notify the Depositary without delay of taking or revoking such a measure. Any measure taken under this paragraph shall take effect 15 days after the date of receipt of the notification by the Depositary.

(5) The Depositary shall inform other Parties of the notification of withdrawal or suspension without delay.

In witness whereof the undersigned, being duly authorised have signed this Agreement:

For the Republic of Albania

For the Republic of Austria

For Bosnia and Herzegovina

For the Republic of Bulgaria

For Hungary

For the Republic of Macedonia

For the Republic of Moldova

For Montenegro

For Romania

For the Republic of Serbia

For the Republic of Slovenia

Done in Vienna, on the 13 th day of September 2018, in a single original copy in the English language.