

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2019/818**ze dne 20. května 2019,****kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti policejní a justiční spolupráce, azylu a migrace a kterým se mění nařízení (EU) 2018/1726, (EU) 2018/1862 a (EU) 2019/816**

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na čl. 16 odst. 2, článek 74, čl. 78 odst. 2 písm. e), čl. 79 odst. 2 písm. c), čl. 82 odst. 1 písm. d), čl. 85 odst. 1, čl. 87 odst. 2 písm. a) a čl. 88 odst. 2 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru ⁽¹⁾,

po konzultaci s Výborem regionů,

v souladu s řádným legislativním postupem ⁽²⁾,

vzhledem k těmto důvodům:

- (1) Komise ve svém sdělení ze dne 6. dubna 2016 nazvaném Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost zdůraznila potřebu zlepšit unijní architekturu správy údajů pro správu hranic a bezpečnost. Toto sdělení zahájilo proces směřující k dosažení interoperability mezi informačními systémy EU pro bezpečnost, správu hranic a řízení migrace s cílem vyřešit strukturální nedostatky související s těmito systémy, které ztěžují práci vnitrostátních orgánů, a zajistit, aby příslušníci pohraniční stráže, celní úřady, policisté a justiční orgány měli k dispozici nezbytné informace.
- (2) Ve svém Plánu na posílení výměny informací a správy informací včetně řešení interoperability v oblasti spravedlnosti a vnitřních věcí ze dne 6. dubna 2016 Rada určila různé právní, technické a provozní problémy týkající se interoperability informačních systémů EU a vyzvala k hledání řešení.
- (3) Ve svém usnesení ze dne 6. července 2016 o strategických prioritách pro pracovní program Komise na rok 2017 ⁽³⁾ požadoval Evropský parlament návrhy na zdokonalení a rozvoj stávajících informačních systémů EU, vyřešení mezer v informacích a pokrok směrem k interoperabilitě těchto systémů, jakož i návrhy na závazné sdílení informací na úrovni EU doprovázené nezbytnými zárukami v oblasti ochrany údajů.
- (4) Ve svých závěrech ze dne 15. prosince 2016 Evropská rada vyzvala k dalšímu zlepšování interoperability informačních systémů a databází EU.
- (5) Ve své závěrečné zprávě ze dne 11. května 2017 dospěla expertní skupina na vysoké úrovni pro informační systémy a interoperabilitu k závěru, že je nezbytné a technicky proveditelné vypracovat praktická řešení pro interoperabilitu, a že interoperabilita by mohla v zásadě mít operativní přínosy a současně být vytvořena v souladu s požadavky na ochranu údajů.
- (6) Ve svém sdělení ze dne 16. května 2017 nazvaném Sedmá zpráva o pokroku na cestě k účinné a skutečně bezpečnostní unii Komise v souladu se svým sdělením ze dne 6. dubna 2016 a na základě zjištění a doporučení expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu stanovila nový přístup ke správě údajů pro ochranu hranic, bezpečnost a migraci, v němž jsou všechny informační systémy EU pro bezpečnost, správu hranic a řízení migrace interoperabilní, a to při plném dodržování základních práv.

⁽¹⁾ Úř. věst. C 283, 10.8.2018, s. 48.

⁽²⁾ Postoj Evropského parlamentu ze dne 16. dubna 2019 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne 14. května 2019.

⁽³⁾ Úř. věst. C 101, 16.3.2018, s. 116.

- (7) Ve svých závěrech ze dne 9. června 2017 o dalším postupu s cílem zlepšit výměnu informací a zajistit interoperabilitu informačních systémů EU vyzvala Rada Komisi, aby usilovala o řešení interoperability tak, jak je navrhl expertní skupina na vysoké úrovni.
- (8) Ve svých závěrech ze dne 23. června 2017 Evropská rada zdůraznila potřebu zlepšovat interoperabilitu mezi databázemi a vyzvala Komisi, aby na základě návrhů předložených expertní skupinou na vysoké úrovni pro informační systémy a interoperabilitu vypracovala co nejdříve návrh právního předpisu.
- (9) Aby bylo možné zlepšit efektivitu a účinnost kontrol na vnějších hranicích, přispět k prevenci a potírání nedovoleného přistěhovalectví a přispět k vysoké úrovni bezpečnosti v oblasti svobody, bezpečnosti a práva Unie, včetně udržování veřejné bezpečnosti a veřejného pořádku a zajišťování bezpečnosti na území členských států, zlepšit provádění společné vízové politiky, pomáhat při posuzování žádostí o mezinárodní ochranu, přispět k prevenci, odhalování a vyšetřování teroristických trestných činů a jiných závažných trestných činů, usnadnit zjišťování totožnosti neznámých osob, které nejsou schopny samy prokázat svou totožnost, nebo identifikaci lidských pozůstatků v případě přírodních katastrof, nehody nebo teroristického útoku a zachovat důvěru veřejnosti v migrační a azylový systém Unie, bezpečnostní opatření Unie a v její schopnost spravovat vnější hranice, je třeba zajistit interoperabilitu mezi informačními systémy EU, zejména Systému vstupu/výstupu (systém EES), Vízového informačního systému (VIS), Evropského systému pro cestovní informace a povolení (ETIAS), systému Eurodac (Eurodac), Schengenského informačního systému (SIS) a Evropského informačního systému rejstříků trestů pro státní příslušníky třetích zemí (ECRIS-TCN), tak aby se tyto informační systémy EU a jejich údaje navzájem doplňovaly, a to při současném dodržení základních práv jednotlivců, zejména práva na ochranu osobních údajů. V zájmu dosažení uvedeného cíle by se měl zřídit Evropský vyhledávací portál (ESP), sdílená služba pro porovnávání biometrických údajů (sdílená BMS), společné úložiště údajů o totožnosti (CIR) a detektor vícenásobné totožnosti (MID) jako složky interoperability.
- (10) Interoperabilita mezi informačními systémy EU by měla umožnit, aby se uvedené systémy navzájem doplňovaly s cílem usnadnit správné zjištění totožnosti osob, včetně totožnosti neznámých osob, které nejsou schopny samy prokázat svou totožnost, nebo identifikaci lidských pozůstatků, přispět k boji proti podvodnému zneužívání totožnosti, zlepšit a harmonizovat požadavky na kvalitu údajů příslušných informačních systémů EU, usnadnit technické a provozní provádění informačních systémů EU členskými státy, posílit záruky pro zabezpečení a ochranu údajů vztahující se na příslušné informační systémy EU, zjednodušit přístup pro účely prevence, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů k EES, VIS, ETIAS a Eurodac a podpořit účely EES, VIS, ETIAS, Eurodacu, SIS a ECRIS-TCN.
- (11) Složky interoperability by měly pokrývat EES, VIS, ETIAS, Eurodac, SIS a ECRIS-TCN. Rovněž by měly pokrývat údaje Europolu, ale pouze v takovém rozsahu, aby se umožnilo souběžné vyhledávání v údajích Europolu a v uvedených informačních systémech EU.
- (12) Složky interoperability by měly zpracovávat osobní údaje osob, jejichž osobní údaje jsou zpracovávány v základních informačních systémech EU a Eupolem.
- (13) ESP by měl být zřízen s cílem technicky usnadnit rychlý, plynulý, účinný, systematický a řízený přístup orgánů členských států a agentur Unie k informačním systémům EU, k údajům Europolu a k databázím Mezinárodní organizace kriminální policie (Interpolu), a to v rozsahu, který v souladu se svými přístupovými právy potřebují k plnění svých úkolů. ESP by měl být rovněž zřízen s cílem podpořit účely EES, VIS, ETIAS, Eurodacu, SIS, ECRIS-TCN a údajů Europolu. Tím, že umožní souběžné vyhledávání ve všech příslušných informačních systémech EU, v údajích Europolu a databázích Interpolu, měl by ESP fungovat jako jednotný portál nebo „zprostředkovatel zpráv“ pro vyhledávání v různých centrálních systémech, přičemž by plynule při plném dodržování požadavků na kontrolu přístupu a ochranu údajů základních systémů získával nezbytné informace.
- (14) Architektura ESP by měla zaručit, aby při vyhledávání v databázích Interpolu nebyly údaje používané uživatelem ESP k zahájení vyhledávání sdíleny s majiteli údajů Interpolu. Architektura ESP by měla rovněž zaručit, aby bylo vyhledávání v databázích Interpolu prováděno pouze v souladu s použitelným unijním a vnitrostátním právem.

- (15) Uživatelé ESP, kteří mají právo na přístup k údajům Europolu podle nařízení Evropského parlamentu a Rady (EU) 2016/794 ⁽⁴⁾, by měli mít možnost vyhledávat v údajích Europolu souběžně s informačními systémy EU, k nimž mají přístup. Jakékoli další zpracování údajů po takovém vyhledávání by mělo probíhat v souladu s nařízením (EU) 2016/794, včetně omezení uložených poskytovatelem údajů, pokud jde o přístup k údajům nebo jejich využití.
- (16) ESP by měl být vyvinut a nastaven tak, aby umožňoval pouze vyhledávání, které je prováděno za použití údajů týkajících se osob nebo cestovních dokladů obsažených v některém informačním systému EU, v údajích Europolu nebo v databázi Interpolu.
- (17) Aby se zajistilo systematické využívání příslušných informačních systémů EU, měl by se ESP používat pro vyhledávání v CIR, EES, VIS, ETIAS, Eurodacu a ECRIS-TCN. Vnitrostátní spojení s jednotlivými informačními systémy EU by však mělo zůstat zachováno, aby se zajistilo technické záložní řešení. ESP by také měly využívat agentury Unie k vyhledávání v centrálním SIS v souladu se svými přístupovými právy a za účelem plnění svých úkolů. ESP by měl být dalším prostředkem pro vyhledávání v centrálním SIS, údajích Europolu a databázích Interpolu, čímž doplní stávající vyhrazená rozhraní.
- (18) Biometrické údaje, jako jsou otisky prstů a zobrazení obličeje, jsou jedinečné, a pro účely zjištění totožnosti osob tedy mnohem spolehlivější než alfanumerické údaje. Sdílená BMS by měla představovat technický nástroj, který posílí a zjednoduší fungování příslušných informačních systémů EU a ostatních složek interoperability. Hlavním účelem sdílené BMS by mělo být usnadnění zjištění totožnosti osob, které jsou registrovány v několika databázích, s využitím jediné technické složky k porovnání biometrických údajů dané osoby v různých systémech, namísto několika složek. Sdílená BMS by měla přispět k bezpečnosti a rovněž přinést výhody v oblasti financí, údržby a provozu. Všechny systémy automatizované identifikace otisků prstů včetně těch, které se v současnosti používají pro Eurodac, VIS a SIS, využívají biometrické šablony složené z údajů odvozených na základě extrakce rysů ze skutečných biometrických vzorků. Sdílená BMS by měla všechny tyto biometrické šablony – logicky oddělené podle informačního systému, z něhož údaje pocházejí – seskupit a uložit na jediném místě, čímž se usnadní porovnávání mezi systémy na základě biometrických šablon a umožní značné úspory z rozsahu při vývoji a údržbě centrálních systémů Unie.
- (19) Biometrické šablony uložené ve sdílené BMS by měly být složeny z údajů odvozených na základě extrakce rysů ze skutečných biometrických vzorků a získávány způsobem, který neumožňuje zpětný proces extrakce. Biometrické šablony by měly být získávány z biometrických údajů, avšak nemělo by být možné získat tytéž biometrické údaje z biometrických šablon. Vzhledem k tomu, že údaje o otiscích dlaní a profily DNA jsou ukládány pouze v SIS a nemohou být používány k vzájemnému porovnávání s údaji uchovávanými v jiných informačních systémech podle zásady nezbytnosti a proporcionality, neměla by sdílená BMS uchovávat profily DNA nebo biometrické šablony získané z otisků dlaní.
- (20) Biometrické údaje představují citlivé osobní údaje. Toto nařízení by mělo stanovit základy a záruky pro zpracování takových údajů pro účely zjištění jediné totožnosti dotčených osob.
- (21) EES, VIS, ETIAS, Eurodac a ECRIS-TCN vyžadují přesné zjištění totožnosti osob, jejichž osobní údaje jsou v nich uloženy. CIR by tedy měl usnadnit správné zjišťování totožnosti osob registrovaných v těchto systémech.
- (22) Osobní údaje uložené v těchto informačních systémech EU se mohou vztahovat k týmž osobám, ale k jejich různým nebo neúplně uvedeným totožnostem. Členské státy mají k dispozici účinné způsoby ke zjištění totožnosti svých občanů nebo registrovaných osob s povolením k trvalému pobytu na jejich území. Interoperabilita mezi informačními systémy EU by měla přispět ke správnému zjištění totožnosti osob vyskytujících se v těchto systémech. CIR by mělo ukládat osobní údaje, které jsou nezbytné pro umožnění přesnějšího zjištění totožnosti těchto osob, jejichž údaje jsou uloženy v těchto systémech, včetně údajů o jejich totožnosti, údajů o cestovním dokladu a biometrických údajů, bez ohledu na to, v jakém systému byly údaje původně shromážděny. V CIR by se měly zaznamenávat pouze ty osobní údaje, které jsou k provedení přesné kontroly totožnosti nezbytně nutné. Osobní údaje zaznamenané v CIR by neměly být uchovávány déle, než je nezbytně nutné pro účely základních systémů, a měly by se automaticky vymazat, když se údaje vymažou v základním systému, a to v souladu s jejich logickým oddělením.

⁽⁴⁾ Nařízení Evropského parlamentu a Rady (EU) 2016/794 ze dne 11. května 2016 o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV (Úř. věst. L 135, 24.5.2016, s. 53).

- (23) Tento nový postup zpracování, sestávající z ukládání takových údajů do CIR, namísto jejich ukládání v jednotlivých oddělených systémech, je nezbytný, má-li se zvýšit přesnost zjišťování totožnosti díky automatizovanému porovnávání a zjišťování shod těchto údajů. Skutečnost, že údaje o totožnosti, údaje o cestovním dokladu a biometrické údaje jsou ukládány do CIR, by nijak neměla zpomalit zpracování údajů pro účely EES, VIS, ETIAS, Eurodacu nebo ECRIS-TCN, jelikož CIR by mělo být novou sdílenou složkou těchto základních systémů.
- (24) Je proto nezbytné v CIR vytvořit pro každou osobu, která je registrována v EES, VIS, ETIAS, Eurodacu nebo ECRIS-TCN, individuální soubor, aby bylo možné splnit účel správného zjištění totožnosti osob v schengenském prostoru a podpořit MID s dvojitým cílem, kterým je usnadnění kontrol totožnosti cestujících v dobré víře a potírání podvodného zneužívání totožnosti. Individuální soubor by měl všechny informace o totožnosti spojené s určitou osobou uložit na jediném místě a zpřístupnit je řádně zmocněným koncovým uživatelům.
- (25) CIR by tedy mělo usnadnit a urychlit přístup orgánů odpovědných za prevenci, odhalování a vyšetřování teroristických trestných činů nebo jiných závažných trestných činů k informačním systémům EU, které nejsou zřízeny výlučně pro účely prevence, odhalování nebo vyšetřování závažné trestné činnosti.
- (26) CIR by mělo zahrnovat sdílenou schránku pro údaje o totožnosti, cestovních dokladech a biometrické údaje osob registrovaných v EES, VIS, ETIAS, Eurodacu a ECRIS-TCN. Mělo by tvořit součást technické architektury těchto systémů a sloužit jako sdílená složka mezi těmito systémy pro účely ukládání a vyhledávání údajů o totožnosti, údajů o cestovních dokladech a biometrických údajů, které zpracovávají.
- (27) Všechny záznamy v CIR by měly být logicky odděleny prostřednictvím automatizovaného označování každého záznamu uvádějícího název základního systému, který je jeho vlastníkem. Toto označení by se mělo používat při kontrole přístupu do CIR za účelem určení, zda umožnit přístup k danému záznamu.
- (28) Pokud policejní orgán členského státu není schopen zjistit totožnost osoby, protože tato osoba nemá cestovní doklad ani jiný důvěryhodný doklad totožnosti, nebo pokud existují pochybnosti o údajích o totožnosti poskytnutých touto osobou nebo o pravosti cestovního dokladu a totožnosti jeho držitele, nebo pokud tato osoba není schopna nebo odmítá spolupracovat, měl by mít tento policejní orgán pravomoc vyhledávat údaje v CIR za účelem zjištění totožnosti této osoby. Za tímto účelem by policejní orgány měly snímat otisky prstů za použití technik pro přímé skenování otisků prstů, za předpokladu, že tento postup je zahájen za přítomnosti této osoby. Takovéto vyhledávání v CIR by nemělo být povoleno pro účely zjištění totožnosti nezletilých osob mladších dvanácti let, ledaže je to v nejlepším zájmu dítěte.
- (29) Pokud nelze biometrické údaje osoby použít nebo pokud vyhledávání na základě těchto údajů není úspěšné, měly by se pro vyhledávání použít údaje o totožnosti dané osoby ve spojení s údaji v cestovním dokladu. Pokud vyhledávání ukáže, že údaje o této osobě jsou uloženy v CIR, měly by mít orgány členského státu přístup do CIR za účelem nahlížení do údajů o totožnosti a údajů o cestovním dokladu této osoby, aniž by bylo v CIR jakkoli uvedeno, do kterého informačního systému EU tyto údaje patří.
- (30) Členské státy by měly přijmout vnitrostátní legislativní opatření, kterými určí orgány příslušné pro provádění kontrol totožnosti s využitím CIR a stanoví postupy, podmínky a kritéria těchto kontrol, které budou v souladu se zásadou proporcionality. Vnitrostátní právo by mělo zejména stanovit pravomoc, která zaměstnancům těchto orgánů umožní shromažďovat biometrické údaje při kontrole totožnosti osoby za její přítomnosti.
- (31) Toto nařízení by mělo také zavést novou možnost jednoduššího přístupu orgánů odpovědných za prevenci, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů určených členskými státy a Europolu k jiným údajům, než jsou údaje o totožnosti nebo údaje o cestovním dokladu, uloženým v EES, VIS, ETIAS nebo Eurodacu. Tyto údaje mohou být v konkrétních případech nezbytné pro prevenci, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů, pokud existují oprávněné důvody se domnívat, že přístup k nim přispěje k prevenci, odhalování a vyšetřování teroristických trestných činů nebo jiných závažných trestných činů, zejména existuje-li podezření, že podezřelá osoba, pachatel nebo oběť teroristického činu nebo jiného závažného trestného činu je osobou, jejíž údaje jsou uloženy v EES, VIS, ETIAS nebo Eurodacu.

- (32) Plný přístup, který je nezbytný pro účely prevence, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů, k potřebným údajům obsaženým v informačních systémech EU jiným, než jsou příslušné údaje o totožnosti nebo údaje o cestovním dokladu obsažené v CIR, by měl být i nadále upraven příslušnými právními nástroji. Určené orgány odpovědné za prevenci, odhalování a vyšetřování teroristických trestných činů nebo jiných závažných trestných činů a Europol předem nevědí, který informační systém EU obsahuje údaje o osobě, kterou potřebují vyhledat. Výsledkem jsou prodlevy a nedostatečná efektivita při plnění úkolů. Koncový uživatel zmocněný určeným orgánem by tedy měl mít právo vidět, ve kterém z těchto informačních systémů EU jsou údaje odpovídající výsledku vyhledávání zaznamenány. Dotčený systém by se tak označil na základě automatizovaného ověření výskytu shody v systému (tzv. funkce označení shody).
- (33) V této souvislosti by odpověď CIR neměla být vykládána ani použita jakožto podklad nebo odůvodnění pro to, aby byly vyvozeny závěry nebo přijata opatření vůči dané osobě, nýbrž by měla sloužit pouze pro účel podání žádosti o přístup k základním informačním systémům EU, a to za podmínek a na základě postupů stanovených v příslušných právních nástrojích upravujících tento přístup. Na jakoukoli žádost o přístup by se měla vztahovat kapitola VII tohoto nařízení a případně nařízení Evropského parlamentu a Rady (EU) 2016/679 ⁽⁵⁾, směrnice Evropského parlamentu a Rady (EU) 2016/680 ⁽⁶⁾ nebo v nařízení Evropského parlamentu a Rady (EU) 2018/1725 ⁽⁷⁾.
- (34) Zpravidla by v případě, kdy označená shoda ukáže, že jsou údaje zaznamenány v Eurodacu, měly určené orgány nebo Europol požádat o plný přístup do nejméně jednoho z dotčených informačních systémů EU. Pokud není ve výjimečných případech plný přístup požadován, například proto, že určené orgány nebo Europol již údaje získaly jiným způsobem, nebo získání těchto údajů není již podle vnitrostátního práva povoleno, měl by být proveden záznam odůvodnění, proč o přístup nebylo požádáno.
- (35) Z protokolů o vyhledávání v CIR by měl vyplývat účel vyhledávání. Pokud bylo takové vyhledávání provedeno s využitím dvoufázového postupu pro nahlížení do údajů, měly by protokoly obsahovat odkaz na vnitrostátní vyšetřovací spis nebo řízení, čímž by se označilo, že vyhledávání bylo zahájeno pro účely prevence, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů.
- (36) Vyhledávání v CIR prováděné určenými orgány a Eupolem s cílem obdržet odpověď s označením shody a uvedením informace, že údaje jsou zaznamenány v EES, VIS, ETIAS nebo Eurodacu, vyžaduje automatizované zpracovávání osobních údajů. Označení shody by nemělo odhalit osobní údaje dotčené osoby, pouze by mělo ukázat, že některé z jejích údajů jsou uloženy v jednom ze systémů. Oprávněný koncový uživatel by neměl přijmout žádné nepříznivé rozhodnutí v souvislosti s dotčenou osobou pouze na základě prostého označení shody. Přístup koncového uživatele k označení shody bude tedy znamenat velmi omezené narušení práva na ochranu osobních údajů dotčené osoby, i když bude určeným orgánům a Europolu umožněno, aby mohly účinněji žádat o přístup k osobním údajům.
- (37) MID by měl být zřízen s cílem podpořit fungování CIR a účely EES, VIS, ETIAS, Eurodacu, SIS a ECRIS-TCN. K zajištění toho, aby všechny uvedené informační systémy EU mohly účinně plnit příslušné cíle, je nezbytné přesné zjištění totožnosti osob, jejichž osobní údaje jsou v nich uloženy.
- (38) K lepšímu dosažení cílů informačních systémů EU by orgány využívající tyto systémy měly mít možnost dostatečně spolehlivě ověřit totožnost osob, jejichž údaje jsou uloženy v různých systémech. Soubor údajů o totožnosti nebo údajů o cestovním dokladu uložený v jednom konkrétním systému může být nesprávný,

⁽⁵⁾ Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

⁽⁶⁾ Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. L 119, 4.5.2016, s. 89).

⁽⁷⁾ Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

neúplný nebo podvodný, přičemž tyto nesprávné, neúplné nebo podvodné údaje o totožnosti nebo údaje o cestovním dokladu není možné v současnosti odhalit porovnáním s údaji uloženými v jiném systému. Pro nápravu této situace je zapotřebí zavést technický nástroj na úrovni Unie, který umožní přesné zjištění totožnosti osob pro tyto účely.

- (39) MID by měl vytvářet a uchovávat propojení mezi údaji v různých informačních systémech EU pro účely odhalování vícenásobných totožností, a to s dvojím účelem, kterým je usnadnění kontrol totožnosti cestujících v dobré víře a potírání podvodného zneužívání totožnosti. MID by měl obsahovat pouze propojení mezi údaji jednotlivců, kteří se vyskytují ve více než jednom informačním systému EU. Propojené údaje by měly být přísně omezeny na údaje nutné k ověření, zda je daná osoba zaznamenána pod různými totožnostmi v různých systémech oprávněně nebo neoprávněně, nebo k určení, zda dvě osoby s podobnými údaji o totožnosti nemohou být touž osobou. Zpracování údajů prostřednictvím ESP a sdílené služby za účelem propojení individuálních souborů v různých systémech by mělo zůstat naprosto minimální a omezí se tedy na zjištění vícenásobných totožností v okamžiku, kdy se do jednoho ze systémů, který má údaje uložené v CIR nebo doplněné do SIS, doplní nové údaje. MID by měl obsahovat záruky proti možné diskriminaci nebo nepříznivým rozhodnutím pro osoby s vícenásobnými zákonnými totožnostmi.
- (40) Toto nařízení stanoví nové postupy zpracování údajů zaměřené na správné zjištění totožnosti dotčených osob. To přináší narušení jejich základních práv chráněných články 7 a 8 Listiny základních práv Evropské unie. Jelikož účinné zavedení informačních systémů EU závisí na správném zjištění totožnosti dotčených jednotlivců, je toto narušení odůvodněno stejnými cíli, pro které byly jednotlivé systémy zřízeny, a sice účinnou správou hranic Unie, vnitřní bezpečností Unie a účinným prováděním azylové a vízové politiky Unie.
- (41) ESP a sdílená BMS by měly porovnávat údaje o osobách v CIR a SIS, jestliže vnitrostátní orgán nebo agentura Unie vytvoří nebo nahrají nové záznamy. Toto porovnávání by mělo být automatizované. CIR a SIS by měly využívat sdílené BMS k zjištění možných propojení na základě biometrických údajů. CIR a SIS by měly využívat ESP k zjištění možných propojení na základě alfanumerických údajů. CIR a SIS by měly být schopny identifikovat stejné nebo podobné údaje o dané osobě uložené v několika systémech. V takovém případě by se mělo vytvořit propojení signalizující, že jde o tutéž osobu. CIR a SIS by měly být nastaveny tak, aby byly odhalovány drobné chyby v přepisu nebo pravopisu, aniž by tím vytvářely nedůvodná omezení pro dotčenou osobu.
- (42) Vnitrostátní orgán nebo agentura Unie, které údaj zaznamenaly do příslušného informačního systému EU, by měly tato propojení potvrdit nebo změnit. Takový vnitrostátní orgán nebo agentura Unie by měly mít přístup k údajům uloženým v CIR nebo SIS a v MID pro účely manuálního ověření různých totožností.
- (43) Manuální ověření různých by mělo být zajištěno orgánem, který vytváří nebo aktualizuje údaje, jež vedly ke shodě a následně k propojení s údaji, které jsou již uloženy v jiném informačním systému EU. Orgán odpovědný za manuální ověření různých totožností by měl posoudit, zda existují vícenásobné totožnosti oprávněně nebo neoprávněně odkazující k téže osobě. Takové posouzení by mělo proběhnout pokud možno za přítomnosti dotčené osoby a, je-li to nutné, mělo by se požadovat další vysvětlení nebo doplňující informace. Toto posouzení by mělo proběhnout neprodleně, v souladu s právními požadavky na přesnost informací podle unijního a vnitrostátního práva.
- (44) U propojení získaných přes SIS týkajících se záznamů o osobách hledaných za účelem zatčení a předání nebo vydání, o pohřešovaných nebo zranitelných osobách, o osobách hledaných za účelem zajištění jejich spolupráce v soudním řízení nebo záznamů o osobách pořízených pro účely skrytých, dotazovacích a zvláštních kontrol, by měla být orgánem odpovědným za manuální ověření různých totožností centrála SIRENE členského státu, který záznam vytvořil. Tyto kategorie záznamů v SIS jsou citlivé a neměly by se nezbytně sdílet s orgány, které

vytvářejí nebo aktualizují údaje s nimi propojené v jednom z dalších informačních systémů EU. Vytvoření propojení s údaji SIS by mělo proběhnout bez ohledu na činnosti, které je nutno vykonat v souladu s nařízeními Evropského parlamentu a Rady (EU) 2018/1860 ⁽⁸⁾, (EU) 2018/1861 ⁽⁹⁾ a (EU) 2018/1862 ⁽¹⁰⁾.

- (45) Vytvoření těchto propojení vyžaduje transparentnost ve vztahu k dotčeným osobám. S cílem usnadnit provádění nezbytných záruk v souladu s platnými pravidly Unie pro ochranu údajů by osoby, v jejichž případě vzniklo po manuálním ověření různých totožností červené nebo bílé propojení, měly být písemně informovány, aniž by byla dotčena omezení z důvodu ochrany bezpečnosti a veřejného pořádku, prevence trestné činnosti a zaručení řádného průběhu vnitrostátních vyšetřování. Tyto osoby by měly obdržet jediné identifikační číslo, jež jim umožní určit orgán, na který by se měly obrátit za účelem vykonání svých práv.
- (46) Je-li vytvořeno žluté propojení, orgán odpovědný za manuální ověření různých totožností by měl mít přístup k MID. Existuje-li červené propojení, orgány členského státu a agentury Unie, které mají přístup alespoň do jednoho informačního systému EU zapojeného do CIR nebo do SIS, by měly mít přístup k MID. Červené propojení by mělo signalizovat, že daná osoba používá neoprávněně různé totožnosti nebo že daná osoba používá totožnost někoho jiného.
- (47) Existuje-li bílé nebo zelené propojení mezi údaji ze dvou informačních systémů EU, orgány členských států a agentury Unie by měly mít přístup k MID, pokud má dotčený orgán nebo agentura přístup k oběma informačním systémům. Tento přístup by měl být udělen za jediným účelem, a sice aby mohl uvedený orgán nebo agentura odhalit potenciální případy, kdy byly údaje propojeny nesprávně nebo zpracovány v MID, CIR a SIS v rozporu s tímto nařízením, a aby mohl přijmout opatření k nápravě této situace a propojení aktualizovat nebo vymazat.
- (48) Agentura Evropské unie pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (dále jen „agentura eu-LISA“) by měla zavést automatizované mechanismy kontroly kvality údajů a společné ukazatele kvality údajů. Agentura eu-LISA by měla odpovídat za vývoj centrální monitorovací kapacity kvality údajů a pravidelně vypracovávat zprávy o analýze údajů s cílem zlepšit kontrolu nad prováděním a uplatňováním informačních systémů EU členskými státy. Společné ukazatele kvality údajů by měly zahrnovat minimální normy kvality pro uchovávání údajů v informačních systémech EU nebo ve složkách interoperability. Cílem takových norem kvality údajů by mělo být, aby informační systémy EU a složky interoperability automaticky zjišťovaly zjevně nesprávné nebo nekonzistentní předložené údaje tak, aby členský stát původu mohl údaje ověřit a provést veškeré nezbytné kroky k nápravě.
- (49) Komise by měla vyhodnotit zprávy o kvalitě předkládané agenturou eu-LISA a ve vhodných případech vydat doporučení pro členské státy. Členské státy by měly být odpovědné za přípravu akčního plánu, který popíše kroky směřující k nápravě jakýchkoli nedostatků v kvalitě údajů, a měly by pravidelně podávat zprávy o jeho pokroku.
- (50) Univerzální formát pro zprávy (UMF) by měl sloužit jako norma strukturované přeshraniční výměny informací mezi informačními systémy, orgány nebo organizacemi v oblasti justice a vnitřních věcí. Aby se usnadnila interoperabilita, měl by UMF definovat společný slovník a logické struktury pro běžně vyměňované informace tím, že umožní vytvoření a přečtení obsahu výměny jednotným a sémanticky odpovídajícím způsobem.
- (51) Zavedení normy UMF může být zváženo v případě systému VIS, SIS a v jakýchkoli jiných stávajících nebo nových modelech pro přeshraniční výměnu informací a v informačních systémech v oblasti justice a vnitřních věcí, které vyvíjejí členské státy.

⁽⁸⁾ Nařízení Evropského parlamentu a Rady (EU) 2018/1860 ze dne 28. listopadu 2018 o využívání Schengenského informačního systému při navracení neoprávněně pobývajících státních příslušníků třetích zemí (Úř. věst. L 312, 7.12.2018, s. 1).

⁽⁹⁾ Nařízení Evropského parlamentu a Rady (EU) 2018/1861 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol, o změně Úmluvy k provedení Schengenské dohody a o změně a zrušení nařízení (ES) č. 1987/2006 (Úř. věst. L 312, 7.12.2018, s. 14).

⁽¹⁰⁾ Nařízení Evropského parlamentu a Rady (EU) 2018/1862 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, o změně a o zrušení rozhodnutí Rady 2007/533/SVV a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 a rozhodnutí Komise 2010/261/EU (Úř. věst. L 312, 7.12.2018, s. 56).

- (52) Mělo by být zřízeno centrální úložiště pro podávání zpráv a statistiky (CRRS) s cílem vytvářet mezisystémové statistické údaje a analytické zprávy pro účely politiky, provozu a kvality údajů, a to v souladu s příslušnými právními nástroji. Agentura eu-LISA by měla zřídit, provést a ve svých technických prostorách provozovat CRRS. CRRS by mělo obsahovat anonymizované statistické údaje z informačních systémů EU, CIR, MID a sdílené BMS. Údaje obsažené v CRRS by neměly umožnit zjištění totožnosti jednotlivců. Agentura eu-LISA by měla zajistit automatizovanou anonymizaci údajů a anonymizované údaje zaznamenat do CRRS. Anonymizace údajů by měla probíhat automatizovaně a pracovníkům agentury eu-LISA by neměl být udělen přímý přístup k žádným osobním údajům uloženým v informačních systémech EU nebo ve složkách interoperability.
- (53) Na zpracování osobních údajů vnitrostátními orgány pro účely interoperability podle tohoto nařízení se vztahuje nařízení (EU) 2016/679, pokud je neprovádějí určené orgány nebo ústřední přístupové body členských států pro účely prevence, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů.
- (54) Pokud je zpracování osobních údajů členskými státy za účelem interoperability podle tohoto nařízení prováděno příslušnými orgány pro účely prevence, odhalování nebo vyšetřování teroristických trestných činů či jiných závažných trestných činů, použije se směrnice (EU) 2016/680.
- (55) Nařízení (EU) 2016/679, nařízení (EU) 2018/1725 nebo případně směrnice (EU) 2016/680 by se měly vztahovat na veškeré předávání osobních údajů třetím zemím nebo mezinárodním organizacím, které je prováděno podle tohoto nařízení. Aniž jsou dotčeny důvody pro předání podle kapitoly V nařízení (EU) 2016/679 nebo případně podle směrnice (EU) 2016/680, mělo by být jakékoli rozhodnutí soudu a jakékoli rozhodnutí správního orgánu třetí země požadující, aby správce nebo zpracovatel předal nebo zveřejnil osobní údaje, uznáno nebo jakýmkoli způsobem vymáháno pouze tehdy, zakládá-li se na platné mezinárodní dohodě mezi žádající třetí zemí a Uníí nebo členským státem.
- (56) Zvláštní ustanovení o ochraně údajů nařízení (EU) 2018/1862 a nařízení Evropského parlamentu a Rady (EU) 2019/816 ⁽¹⁾ by se měla použít pro zpracování osobních údajů v systémech, které se řídí uvedenými nařízeními.
- (57) Nařízení (EU) 2018/1725 se vztahuje na zpracování osobních údajů agenturou eu-LISA a dalšími orgány a institucemi Unie při plnění jejich povinností podle tohoto nařízení, aniž je tím dotčeno nařízení (EU) 2016/794, které se vztahuje na zpracování osobních údajů Europolem.
- (58) Vnitrostátní dozorové úřady uvedené v nařízení (EU) 2016/679 nebo směrnici (EU) 2016/680 by měly monitorovat zákonnost zpracování osobních údajů členskými státy. Evropský inspektor ochrany údajů by měl monitorovat činnost orgánů a institucí Unie související se zpracováním osobních údajů. Evropský inspektor ochrany údajů a dozorové úřady by měly při monitorování zpracovávání osobních údajů složkami interoperability vzájemně spolupracovat. Evropskému inspektorovi ochrany údajů je nutno k tomu, aby mohl plnit úkoly jemu svěřené podle tohoto nařízení, přidělit dostatečné zdroje, a to jak lidské, tak finanční.
- (59) V souladu s čl. 28 odst. 2 nařízení Evropského parlamentu a Rady (ES) č. 45/2001 16. dubna 2018 ⁽¹²⁾ byl konzultován evropský inspektor ochrany údajů, který své stanovisko předložil dne 16. dubna 2018 ⁽¹³⁾.
- (60) Pracovní skupina pro ochranu údajů podle článku 29 vydala dne 11. dubna 2018 své stanovisko.
- (61) Členské státy i agentura eu-LISA by měly mít bezpečnostní plány s cílem usnadnit provádění bezpečnostních povinností a měly by navzájem spolupracovat na řešení bezpečnostních otázek. Agentura eu-LISA by také měla zajistit průběžné využívání nejnovějšího technologického vývoje pro zajištění integrity údajů, pokud jde o vývoj, návrh a správu složek interoperability. K povinnostem agentury eu-LISA by v tomto ohledu mělo patřit přijímání

⁽¹⁾ Nařízení Evropského parlamentu a Rady (EU) 2019/816 ze dne 17. dubna 2019, kterým se zřizuje centralizovaný systém pro identifikaci členských států, jež mají informace o odsouzeních státních příslušníků třetích zemí a osob bez státní příslušnosti (ECRIS-TCN), na doplnění Evropského informačního systému rejstříků trestů, a kterým se mění nařízení (EU) 2018/1726 (viz strana 1 v tomto čísle Úředního věstníku).

⁽¹²⁾ Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, 12.1.2001, s. 1).

⁽¹³⁾ Úř. věst. C 233, 4.7.2018, s. 12.

opatření nezbytných k tomu, aby se neoprávněným osobám, jako jsou externí poskytovatelé služeb, zabránilo v přístupu k osobním údajům zpracovávaným s využitím složek interoperability. Při zadávání zakázek na poskytování služeb by členské státy a agentura eu-LISA měly zvažovat veškerá opatření nezbytná k zajištění souladu s právními předpisy týkajícími se ochrany osobních údajů a soukromí jednotlivců nebo ochrany základních bezpečnostních zájmů podle nařízení Evropského parlamentu a Rady (EU) 2018/1046 ⁽¹⁴⁾ a platných mezinárodních úmluv. Při vývoji složek interoperability by agentura eu-LISA měla uplatňovat zásady záměrné a standardní ochrany osobních údajů.

- (62) Na podporu účelů statistik a podávání zpráv je nutné udělit přístup zmocněným pracovníkům příslušných orgánů, institucí a agentur Unie uvedených v tomto nařízení k nahlížení do určitých údajů v souvislosti s určitými složkami interoperability bez umožnění zjištění totožnosti osob.
- (63) Aby se orgány členských států a agentury Unie mohly přizpůsobit novým požadavkům kladeným na používání ESP, je nutné stanovit přechodné období. Obdobně pak, aby se zajistilo soudržné a optimální fungování MID, je nutné stanovit přechodná opatření pro spuštění jeho provozu.
- (64) Jelikož cíle této směrnice, totiž zřízení rámce pro interoperabilitu mezi informačními systémy EU, nemůže být dosaženo uspokojivě členskými státy, ale spíše jej, z důvodu rozsahu a účinků činnosti, může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné k dosažení tohoto cíle.
- (65) Zbývající částka v rozpočtu vyčleněná pro inteligentní hranice v nařízení Evropského parlamentu a Rady (EU) č. 515/2014 ⁽¹⁵⁾ by měla být přerozdělena na toto nařízení v souladu s čl. 5 odst. 5 písm. b) nařízení (EU) č. 515/2014, aby se pokryly náklady na vývoj složek interoperability.
- (66) Za účelem doplnění určitých podrobných technických aspektů tohoto nařízení by měla být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování Evropské unie, pokud jde o
- prodloužení přechodného období pro používání ESP;
 - prodloužení přechodného období pro odhalování vícenásobné totožnosti ústřední jednotkou ETIAS;
 - postupy při určování případů, kdy lze údaje o totožnosti považovat za stejné nebo podobné;
 - pravidla pro provoz CRRS, včetně zvláštních záruk pro zpracování osobních údajů a bezpečnostních pravidel týkajících se úložiště, a
 - podrobná pravidla pro fungování internetového portálu.

Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů ⁽¹⁶⁾. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup na zasedání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

- (67) Za účelem zajištění jednotných podmínek k provedení tohoto nařízení by měly být Komisi svěřeny prováděcí pravomoci, aby stanovila data, od nichž bude zahájen provoz ESP, sdílené BMS, CIR, MID a CRRS.

⁽¹⁴⁾ Nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 ze dne 18. července 2018, kterým se stanoví finanční pravidla pro souhrnný rozpočet Unie, mění nařízení (EU) č. 1296/2013, (EU) č. 1301/2013, (EU) č. 1303/2013, (EU) č. 1304/2013, (EU) č. 1309/2013, (EU) č. 1316/2013, (EU) č. 223/2014 a (EU) č. 283/2014 a rozhodnutí č. 541/2014/EU a zrušuje nařízení (EU, Euratom) č. 966/2012 (Úř. věst. L 193, 30.7.2018, s. 1).

⁽¹⁵⁾ Nařízení Evropského parlamentu a Rady (EU) č. 515/2014 ze dne 16. dubna 2014, kterým se jako součást Fondu pro vnitřní bezpečnost zřizuje nástroj pro finanční podporu v oblasti vnějších hranic a víz a zrušuje rozhodnutí č. 574/2007/ES (Úř. věst. L 150, 20.5.2014, s. 143).

⁽¹⁶⁾ Úř. věst. L 123, 12.5.2016, s. 1.

- (68) Prováděcí pravomoci by měly být svěřeny Komisi rovněž, pokud jde o přijetí podrobných pravidel pro technické detaily profilů uživatelů ESP; specifikace technických řešení umožňující vyhledávání v informačních systémech EU, údajích Europolu a databázích Interpolu prostřednictvím ESP a pro formát odpovědí ESP; technická pravidla pro vytvoření propojení v MID mezi údaji z různých informačních systémů EU; obsah a formu formuláře a způsoby informování daného subjektu údajů v případě, kdy je vytvořeno červené propojení; požadavky na výkonnost a sledování výkonnosti sdílené BMS; mechanismy a postupy automatizované kontroly kvality a ukazatele kontroly kvality; vývoj normy UMF; postup spolupráce v případě bezpečnostních incidentů; a specifikace technických řešení pro členské státy, aby mohly vyřizovat žádosti uživatelů o přístup. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011 ⁽¹⁷⁾
- (69) Vzhledem k tomu, že složky interoperability budou zahrnovat zpracování velkého množství citlivých osobních údajů, je důležité, aby osoby, jejichž údaje jsou zpracovávány prostřednictvím těchto složek, mohly účinně vykonávat svá práva jako subjekty údajů podle nařízení (EU) 2016/679, směrnice (EU) 2016/680 a nařízení (ES) 2018/1725. Tyto subjekty údajů by měly mít k dispozici internetový portál, který jim usnadňuje výkon jejich práv na přístup k jejich osobním údajům, na jejich opravu, výmaz a omezení jejich zpracování. Takový internetový portál by měla zřídit a provozovat agentura eu-LISA.
- (70) Jednou ze základních zásad ochrany údajů je minimalizace údajů. Podle čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 musí být zpracování osobních údajů přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány. Z tohoto důvodu by složky interoperability neměly umožňovat ukládání jakýchkoli nových osobních údajů s výjimkou propojení, která budou uložena v MID, a které představují minimum nezbytné pro účely tohoto nařízení.
- (71) Toto nařízení by mělo obsahovat jasná ustanovení týkající se odpovědnosti a práva na náhradu újmy za nezákonné zpracování osobních údajů nebo jakýkoli čin neslučitelný s tímto nařízením. Tato ustanovení by se neměla dotýkat práva na náhradu újmy správcem nebo zpracovatelem a jejich odpovědnosti podle nařízení (EU) 2016/679, směrnice (EU) 2016/680 a nařízení (EU) 2018/1725. Agentura eu-LISA by měla odpovídat za jakoukoli újmu, kterou způsobí jakožto zpracovatel údajů, pokud nesplnila povinnosti, jež jí byly zvláště uloženy tímto nařízením, nebo pokud jednala nad rámec zákonných pokynů členského státu, který je správcem údajů, nebo v rozporu s nimi.
- (72) Tímto nařízením není dotčeno použití směrnice Evropského parlamentu a Rady 2004/38/ES ⁽¹⁸⁾.
- (73) V souladu s články 1 a 2 Protokolu č. 22 o postavení Dánska, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, se Dánsko neúčastní přijímání tohoto nařízení a toto nařízení pro ně není závazné ani použitelné. Vzhledem k tomu, že toto nařízení, v rozsahu, v jakém se jeho ustanovení týkají SIS ve smyslu úpravy obsažené v nařízení (EU) 2018/1862, navazuje na schengenské *acquis*, rozhodne se Dánsko v souladu s článkem 4 uvedeného protokolu do šesti měsíců po rozhodnutí Rady o tomto nařízení, zda je provede ve svém vnitrostátním právu.
- (74) V rozsahu, v jakém se ustanovení tohoto nařízení týkají SIS ve smyslu úpravy obsažené v nařízení (EU) 2018/1862, se Spojené království tohoto nařízení účastní v souladu s čl. 5 odst. 1 Protokolu č. 19 o schengenském *acquis* začleněném do rámce Evropské unie, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, a v souladu s čl. 8 odst. 2 rozhodnutí Rady 2000/365/ES ⁽¹⁹⁾. Dále pak v rozsahu, v jakém se ustanovení tohoto nařízení týkají Eurodacu a ECRIS-TCN, v souladu s článkem 3 Protokolu č. 21 o postavení Spojeného království a Irsku s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, oznámilo Spojené království dopisem ze dne 18. května 2018 své přání účastnit se přijímání a používání tohoto nařízení.

⁽¹⁷⁾ Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13).

⁽¹⁸⁾ Směrnice Evropského parlamentu a Rady 2004/38/ES ze dne 29. dubna 2004 o právu občanů Unie a jejich rodinných příslušníků svobodně se pohybovat a pobývat na území členských států, o změně nařízení (EHS) č. 1612/68 a o zrušení směrnic 64/221/EHS, 68/360/EHS, 72/194/EHS, 73/148/EHS, 75/34/EHS, 75/35/EHS, 90/364/EHS, 90/365/EHS a 93/96/EHS (Úř. věst. L 158, 30.4.2004, s. 77).

⁽¹⁹⁾ Rozhodnutí Rady 2000/365/ES ze dne 29. května 2000 o žádosti Spojeného království Velké Británie a Severního Irsku, aby se na ně vztahovala některá ustanovení schengenského *acquis* (Úř. věst. L 131, 1.6.2000, s. 43).

- (75) V rozsahu, v jakém se ustanovení nařízení týkají SIS ve smyslu úpravy obsažené v nařízení (EU) 2018/1862, by se Irsko v zásadě mohlo účastnit tohoto nařízení v souladu s čl. 5 odst. 1 Protokolu č. 19 o schengenském *acquis* začleněném do rámce Evropské unie, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, a v souladu s čl. 6 odst. 2 rozhodnutí Rady 2002/192/ES⁽²⁰⁾. Dále pak v rozsahu, v jakém se ustanovení tohoto nařízení týkají Eurodacu a ECRIS-TCN, v souladu s články 1 a 2 Protokolu č. 21 o postavení Spojeného království a Irska s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o Evropské unii a Smlouvě o fungování Evropské unie, a aniž je dotčen článek 4 uvedeného protokolu, se Irsko neúčastní přijímání tohoto nařízení a toto nařízení není pro ně závazné ani použitelné. Jelikož není za těchto okolností možné zajistit, aby bylo toto nařízení v celém rozsahu použitelné na Irsko, jak to vyžaduje článek 288 Smlouvy o fungování Evropské unie, neúčastní se Irsko přijímání tohoto nařízení a toto nařízení není pro ně závazné ani použitelné, aniž jsou dotčena práva Irska podle protokolů č. 19 a č. 21.
- (76) Pokud jde o Island a Norsko, rozvíjí toto nařízení v rozsahu, v jakém se ustanovení nařízení týkají SIS ve smyslu úpravy obsažené v nařízení (EU) 2018/1862, ustanovení schengenského *acquis* ve smyslu Dohody uzavřené Radou Evropské unie a Islandskou republikou a Norským královstvím o přidružení těchto dvou států k uplatňování a rozvoji schengenského *acquis*⁽²¹⁾, která spadají do oblasti uvedené v čl. 1 bodu G rozhodnutí Rady 1999/437/ES⁽²²⁾.
- (77) Pokud jde o Švýcarsko, rozvíjí toto nařízení v rozsahu, v jakém se ustanovení nařízení týkají SIS ve smyslu úpravy obsažené v nařízení (EU) 2018/1862, ta ustanovení schengenského *acquis* ve smyslu Dohody mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis*⁽²³⁾, která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí 1999/437/ES ve spojení s článkem 3 rozhodnutí Rady 2008/146/ES⁽²⁴⁾.
- (78) Pokud jde o Lichtenštejnsko, rozvíjí toto nařízení v rozsahu, v jakém se ustanovení nařízení týkají SIS ve smyslu úpravy obsažené v nařízení (EU) 2018/1862, ta ustanovení schengenského *acquis* ve smyslu Protokolu mezi Evropskou unií, Evropským společenstvím, Švýcarskou konfederací a Lichtenštejnským knížectvím o přistoupení Lichtenštejnského knížectví k Dohodě mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis*⁽²⁵⁾, která spadají do oblasti uvedené v čl. 1 bodu G rozhodnutí 1999/437/ES ve spojení s článkem 3 rozhodnutí Rady 2011/350/EU⁽²⁶⁾.
- (79) Toto nařízení dodržuje základní práva a ctí zásady uznané zejména Listinou základních práv Evropské unie a mělo by být uplatňováno v souladu s těmito právy a zásadami.
- (80) Aby toto nařízení odpovídalo stávajícímu právnímu rámci, měla by být odpovídajícím způsobem změněna nařízení Evropského parlamentu a Rady (EU) 2018/1726⁽²⁷⁾ a nařízení (EU) 2018/1862 a (EU) 2019/816,

⁽²⁰⁾ Rozhodnutí Rady 2002/192/ES ze dne 28. února 2002 o žádosti Irska, aby se na ně vztahovala některá ustanovení schengenského *acquis* (Úř. věst. L 64, 7.3.2002, s. 20).

⁽²¹⁾ Úř. věst. L 176, 10.7.1999, s. 36.

⁽²²⁾ Rozhodnutí Rady 1999/437/ES ze dne 17. května 1999 o některých opatřeních pro uplatňování dohody uzavřené mezi Radou Evropské unie a Islandskou republikou a Norským královstvím o přidružení těchto dvou států k provádění, uplatňování a rozvoji schengenského *acquis* (Úř. věst. L 176, 10.7.1999, s. 31).

⁽²³⁾ Úř. věst. L 53, 27.2.2008, s. 52.

⁽²⁴⁾ Rozhodnutí Rady 2008/149/SVV ze dne 28. ledna 2008 o uzavření Dohody mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis* jménem Evropského společenství (Úř. věst. L 53, 27.2.2008, s. 50).

⁽²⁵⁾ Úř. věst. L 160, 18.6.2011, s. 21.

⁽²⁶⁾ Rozhodnutí Rady 2011/350/EU ze dne 7. března 2011 o uzavření Protokolu mezi Evropskou unií, Evropským společenstvím, Švýcarskou konfederací a Lichtenštejnským knížectvím o přistoupení Lichtenštejnského knížectví k dohodě mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis* jménem Evropské unie, pokud jde o zrušení kontrol na vnitřních hranicích a pohyb osob (Úř. věst. L 160, 18.6.2011, s. 19).

⁽²⁷⁾ Nařízení Evropského parlamentu a Rady (EU) 2018/1726 ze dne 14. listopadu 2018 o Agentuře Evropské unie pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (eu-LISA) a o změně nařízení (ES) č. 1987/2006 a rozhodnutí Rady 2007/533/SVV a zrušení nařízení (EU) č. 1077/2011 (Úř. věst. L 295, 21.11.2018, s. 99).

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I

Obecná ustanovení

Článek 1

Předmět

1. Toto nařízení zřizuje společně s nařízením Evropského parlamentu a Rady (EU) 2019/817 ⁽²⁸⁾ rámec, který má zajistit interoperabilitu mezi Systémem vstupu/výstupu (EES), Vízovým informačním systémem (VIS), Evropským systémem pro cestovní informace a povolení (ETIAS), systémem Eurodac (Eurodac), Schengenským informačním systémem (SIS) a Evropským informačním systémem rejstříků trestů pro státní příslušníky třetích zemí (ECRIS-TCN).
2. Tento rámec zahrnuje tyto složky interoperability:
 - a) Evropský vyhledávací portál (ESP);
 - b) sdílenou službu pro porovnávání biometrických údajů (sdílená BMS);
 - c) společné úložiště údajů o totožnosti (CIR);
 - d) detektor vícenásobné totožnosti (MID).
3. Toto nařízení dále upravuje požadavky na kvalitu údajů, univerzální formát pro zprávy (UMF), centrální úložiště pro podávání zpráv a statistiky (CRRS) a povinnosti členských států a Agentury Evropské unie pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (eu-LISA) s ohledem na návrh, vývoj a provoz složek interoperability.
4. Toto nařízení rovněž upravuje postupy a podmínky pro přístup určených orgánů a Agentury Evropské unie pro spolupráci v oblasti prosazování práva (Europol) k EES, VIS, ETIAS a Eurodacu pro účely prevence, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů.
5. Toto nařízení dále stanoví rámec pro ověřování a zjišťování totožnosti osob.

Článek 2

Cíle

1. Zajištěním interoperability sleduje toto nařízení tyto cíle:
 - a) zlepšit účinnost a účelnost hraničních kontrol na vnějších hranicích;
 - b) pomáhat při prevenci a potírání nedovoleného přistěhovalectví;
 - c) přispívat k vysoké úrovni bezpečnosti v oblasti svobody, bezpečnosti a práva Unie, včetně udržování veřejné bezpečnosti a veřejného pořádku a zajišťování bezpečnosti na území členských států;
 - d) zlepšit provádění společné vízové politiky;
 - e) pomáhat při posuzování žádostí o mezinárodní ochranu;
 - f) přispívat k prevenci, odhalování a vyšetřování teroristických trestných činů a jiných závažných trestných činů;
 - g) usnadňovat zjišťování totožnosti neznámých osob, které nejsou schopny samy prokázat svou totožnost, nebo identifikaci lidských pozůstatků v případě přírodní katastrofy, nehody nebo teroristického útoku.
2. Cílů uvedených v odstavci 1 se dosahuje těmito kroky:
 - a) zajištěním správného zjištění totožnosti osob;
 - b) přispíváním k potírání podvodného zneužívání totožnosti;

⁽²⁸⁾ Nařízení Evropského parlamentu a Rady (EU) 2019/817 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti hranic a víz a mění nařízení Evropského parlamentu a Rady (ES) č. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 a (EU) 2018/1861 a rozhodnutí Rady 2004/512/ES a 2008/633/SVV (viz strana 27 v tomto čísle Úředního věstníku).

- c) zlepšováním kvality údajů uložených v informačních systémech EU a sladováním požadavků na kvalitu těchto údajů při dodržení požadavků na zpracování údajů stanovených právními nástroji upravujícími jednotlivé systémy a se standardy a zásadami ochrany údajů;
- d) usnadněním a podporou technického a provozního zavádění informačních systémů EU členskými státy;
- e) zpřísněním, zjednodušením a sjednocením podmínek pro zabezpečení a ochranu údajů, kterými se řídí jednotlivé informační systémy EU, aniž jsou dotčena zvláštní ochranná opatření a záruky vyžadované u některých kategorií údajů;
- f) zjednodušováním podmínek pro přístup určených orgánů k EES, VIS, ETIAS a Eurodacu při zajištění nezbytných a přiměřených podmínek tohoto přístupu;
- g) podporou účelů EES, VIS, ETIAS, Eurodac, SIS a ECRIS-TCN.

Článek 3

Oblast působnosti

1. Toto nařízení se vztahuje na Eurodac, SIS a ECRIS-TCN.
2. Toto nařízení se rovněž vztahuje na údaje Europolu v rozsahu, který umožňuje jejich vyhledávání souběžně s informačními systémy EU uvedenými v odstavci 1.
3. Toto nařízení se vztahuje na osoby, jejichž osobní údaje mohou být zpracovávány v informačních systémech EU uvedených v odstavci 1 a v rámci údajů Europolu uvedených v odstavci 2.

Článek 4

Definice

Pro účely tohoto nařízení se rozumí:

- 1) „vnějšími hranicemi“ vnější hranice ve smyslu čl. 2 bodu 2 nařízení Evropského parlamentu a Rady (EU) 2016/399 ⁽²⁹⁾;
- 2) „hraničními kontrolami“ hraniční kontroly ve smyslu čl. 2 bodu 11 nařízení (EU) 2016/399;
- 3) „pohraničním orgánem“ pohraniční stráž, která je v souladu s vnitrostátním právem pověřena prováděním hraničních kontrol;
- 4) „dozorovými úřady“ dozorový úřad uvedený v čl. 51 odst. 1 nařízení (EU) 2016/679 a dozorový úřad uvedený v čl. 41 odst. 1 směrnice (EU) 2016/680;
- 5) „ověřením“ proces porovnání souborů údajů, jehož účelem je zjistit, zda je deklarovaná totožnost správná (kontrola porovnáním dvou údajů);
- 6) „zjištěním totožnosti“ proces určení totožnosti osoby pomocí prohledávání databáze podle vícenásobných souborů údajů (kontrola porovnáním více údajů);
- 7) „alfanumerickými údaji“ údaje vyjádřené písmeny, číslicemi, zvláštními znaky, mezerami a interpunkčními znaménky;
- 8) „údaji o totožnosti“ údaje uvedené v čl. 27 odst. 3 písm. a) až e);
- 9) „údaji o otiscích prstů“ zobrazení otisků prstů a zobrazení latentních otisků prstů, které vzhledem ke své jedinečné povaze a charakteristickým znakům umožňují přesné a průkazné porovnání týkající se totožnosti osoby;

⁽²⁹⁾ Nařízení Evropského parlamentu a Rady (EU) 2016/399 ze dne 9. března 2016, kterým se stanoví kodex Unie o pravidlech upravujících přeshraniční pohyb osob (Schengenský hraniční kodex) (Úř. věst. L 77, 23.3.2016, s. 1).

- 10) „zobrazením obličeje“ digitální zobrazení obličeje;
- 11) „biometrickými údaji“ údaje o otiscích prstů nebo zobrazení obličeje nebo obojí;
- 12) „biometrickou šablonou“ matematické vyjádření získané extrakcí rysů z biometrických údajů omezených na charakteristiky, které jsou nezbytné pro zjištění totožnosti a ověření;
- 13) „cestovním dokladem“ pas nebo jiný rovnocenný doklad, který držitele opravňuje překračovat vnější hranice a do kterého lze vyznačit vízum;
- 14) „údaji o cestovním dokladu“ druh, číslo a země vydání cestovního dokladu, datum konce platnosti cestovního dokladu a trojmístný kód země, která cestovní doklad vydala;
- 15) „informačními systémy EU“ EES, VIS, ETIAS, Eurodac, SIS a ECRIS-TCN;
- 16) „údaji Europolu“ osobní údaje, které zpracovává Europol pro účely uvedené v čl. 18 odst. 2 písm. a), b) a c) nařízení (EU) 2016/794;
- 17) „databázemi Interpolu“ databáze odcizených a ztracených cestovních dokladů vedená Interpolem (databáze SLTD) a databáze cestovních dokladů s údaji uvedenými v oběžnících vedená Interpolem (databáze TDAWN);
- 18) „shodou“ existence odpovídajícího údaje zjištěná automatizovaným porovnáním osobních údajů, které jsou zaznamenány v informačním systému či databázi nebo jejichž záznam právě probíhá;
- 19) „policejním orgánem“ příslušný orgán ve smyslu čl. 3 bodu 7 směrnice (EU) 2016/680;
- 20) „určenými orgány“ určené orgány členského státu ve smyslu čl. 3 odst. 1 bodu 26 nařízení Evropského parlamentu a Rady (EU) 2017/2226 ⁽³⁰⁾, čl. 2 odst. 1 písm. e) rozhodnutí Rady 2008/633/SVV ⁽³¹⁾ a čl. 3 odst. 1 bodu 21 nařízení Evropského parlamentu a Rady (EU) 2018/1240 ⁽³²⁾;
- 21) „teroristickým trestným činem“ trestný čin, který odpovídá nebo je rovnocenný jednomu z trestných činů uvedených ve směrnici Evropského parlamentu a Rady (EU) 2017/541 ⁽³³⁾;
- 22) „závažným trestným činem“ trestný čin, který odpovídá nebo je rovnocenný jednomu z trestných činů uvedených v čl. 2 odst. 2 rámcového rozhodnutí Rady 2002/584/SVV ⁽³⁴⁾, pokud za něj lze podle vnitrostátního práva uložit trest odnětí svobody s horní hranicí sazby v délce nejméně tři roky nebo ochranné opatření spojené s omezením svobody ve stejné délce;
- 23) „Systémem vstupu/výstupu“ nebo „EES“ Systém vstupu/výstupu zřízený nařízením (EU) 2017/2226;
- 24) „Vízovým informačním systémem“ nebo „VIS“ Vízový informační systém zřízený nařízením Evropského parlamentu a Rady (ES) č. 767/2008 ⁽³⁵⁾;
- 25) „Evropským systémem pro cestovní informace a povolení“ nebo „ETIAS“ evropský systém pro cestovní informace a povolení zřízený nařízením (EU) 2018/1240;

⁽³⁰⁾ Nařízení Evropského parlamentu a Rady (EU) 2017/2226 ze dne 30. listopadu 2017, kterým se zřizuje Systém vstupu/výstupu (EES) pro registraci údajů o vstupu a výstupu a údajů o odepření vstupu, pokud jde o státní příslušníky třetích zemí překračující vnější hranice členských států, kterým se stanoví podmínky přístupu do systému EES pro účely vymáhání práva a kterým se mění Úmluva k provedení Schengenské dohody a nařízení (ES) č. 767/2008 a (EU) č. 1077/2011 (Úř. věst. L 327, 9.12.2017, s. 20).

⁽³¹⁾ Rozhodnutí Rady 2008/633/SVV ze dne 23. června 2008 o konzultačním přístupu určených orgánů členských států a Europolu do Vízového informačního systému (VIS) pro účely prevence, odhalování a vyšetřování teroristických trestných činů a jiných závažných trestných činů (Úř. věst. L 218, 13.8.2008, s. 129).

⁽³²⁾ Nařízení Evropského parlamentu a Rady (EU) 2018/1240 ze dne 12. září 2018, kterým se zřizuje Evropský systém pro cestovní informace a povolení (ETIAS) a kterým se mění nařízení (EU) č. 1077/2011, (EU) č. 515/2014, (EU) 2016/399, (EU) 2016/1624 a (EU) 2017/2226 (Úř. věst. L 236, 19.9.2018, s. 1).

⁽³³⁾ Směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV (Úř. věst. L 88, 31.3.2017, s. 6).

⁽³⁴⁾ Rámcové rozhodnutí Rady 2002/584/SVV ze dne 13. června 2002 o evropském zatýkáacím rozkazu a postupech předávání mezi členskými státy (Úř. věst. L 190, 18.7.2002, s. 1).

⁽³⁵⁾ Nařízení Evropského parlamentu a Rady (ES) č. 767/2008 ze dne 9. července 2008 o Vízovém informačním systému (VIS) a o výměně údajů o krátkodobých vízech mezi členskými státy (nařízení o VIS) (Úř. věst. L 218, 13.8.2008, s. 60).

- 26) „Eurodacem“ systém Eurodac zřízený nařízením Evropského parlamentu a Rady (EU) č. 603/2013 ⁽³⁶⁾;
- 27) „Schengenským informačním systémem“ nebo „SIS“ Schengenský informační systém zřízený nařízeními (EU) 2018/1860, (EU) 2018/1861 a (EU) 2018/1862;
- 28) „ECRIS-TCN“ centralizovaný systém identifikace členských států, které mají informace o odsouzení státních příslušníků třetích zemí a osob bez státní příslušnosti, zřízený nařízením (EU) 2019/816.

Článek 5

Zákaz diskriminace a základní práva

Zpracování osobních údajů pro účely tohoto nařízení nesmí vést k diskriminaci osob na základě pohlaví, rasy, barvy pleti, etnického nebo sociálního původu, genetických rysů, jazyka, náboženského vyznání nebo přesvědčení, politických nebo jakýchkoli názorů, příslušnosti k národnostní menšině, majetku, narození, zdravotního postižení, věku nebo sexuální orientace. Musí plně respektovat lidskou důstojnost a integritu a základní práva, včetně práva na respektování soukromého života a práva na ochranu osobních údajů. Zvláštní pozornost se musí věnovat dětem, starším osobám, osobám se zdravotním postižením a osobám, které potřebují mezinárodní ochranu. Na prvním místě musí vždy být nejlepší zájem dítěte.

KAPITOLA II

Evropský vyhledávací portál

Článek 6

Evropský vyhledávací portál

1. Zřizuje se Evropský vyhledávací portál (ESP), jehož účelem je usnadnit rychlý, plynulý, účinný, systematický a řízený přístup orgánů členských států a agentur Unie, v souladu s jejich přístupovými právy, k informačním systémům EU, k údajům Europolu a k databázím Interpolu, který potřebují k plnění svých úkolů, v souladu s cíli a účely EES, VIS, ETIAS, Eurodacu, SIS a ECRIS-TCN.
2. ESP se skládá:
 - a) z centrální infrastruktury včetně vyhledávacího portálu, který umožňuje souběžné vyhledávání v EES, VIS, ETIAS, Eurodacu, SIS a ECRIS-TCN a rovněž v údajích Europolu a databázích Interpolu;
 - b) ze zabezpečeného komunikačního kanálu mezi ESP, členskými státy a agenturami Unie, které jsou oprávněny využívat ESP;
 - c) ze zabezpečené komunikační infrastruktury mezi ESP a EES, VIS, ETIAS, Eurodacem, centrálním SIS, ECRIS-TCN, údaji Europolu a databázemi Interpolu, jakož i mezi ESP a centrálními infrastrukturami CIR a MID.
3. ESP vyvine a jeho technickou správu zajišťuje agentura eu-LISA.

Článek 7

Používání Evropského vyhledávacího portálu

1. Používání ESP je vyhrazeno orgánům členských států a agenturám Unie s přístupem alespoň do jednoho z informačních systémů EU v souladu s právními nástroji upravujícími tyto informační systémy EU, do CIR a MID v souladu s tímto nařízením, k údajům Europolu v souladu s nařízením (EU) 2016/794 nebo k databázím Interpolu v souladu s unijním či vnitrostátním právem upravujícím takový přístup.

Tyto orgány členských států a agentury Unie mohou využívat ESP a údaje, které poskytuje, pouze pro cíle a účely stanovené v právních nástrojích upravujících informační systémy EU, v nařízení (EU) 2016/794 a v tomto nařízení.

⁽³⁶⁾ Nařízení Evropského parlamentu a Rady (EU) č. 603/2013 ze dne 26. června 2013 o zřízení systému „Eurodac“ pro porovnávání otisků prstů za účelem účinného uplatňování nařízení (EU) č. 604/2013 kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o mezinárodní ochranu podané státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států, a pro podávání žádostí orgánů pro vymáhání práva členských států a Europolu o porovnání údajů s údají systému Eurodac pro účely vymáhání práva a o změně nařízení (EU) č. 1077/2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (Úř. věst. L 180, 29.6.2013, s. 1).

2. Orgány členských států a agentury Unie uvedené v odstavci 1 využívají ESP k vyhledávání údajů souvisejících s osobami nebo jejich cestovními doklady v centrálních systémech Eurodacu a ECRIS-TCN v souladu se svými přístupovými právy uvedenými v právních nástrojích, jimiž se řídí tyto informační systémy EU, a ve vnitrostátním právu. Využívají ESP také k vyhledávání v CIR v souladu se svými přístupovými právy podle tohoto nařízení pro účely uvedené v článcích 20, 21 a 22.
3. Orgány členských států uvedené v odstavci 1 mohou využívat ESP k vyhledávání údajů souvisejících s osobami nebo jejich cestovními doklady v centrálním SIS uvedeném v nařízeních (EU) 2018/1860 a (EU) 2018/1861.
4. Stanoví-li tak unijní právo, využívají agentury Unie uvedené v odstavci 1 ESP k vyhledávání údajů týkajících se osob nebo jejich cestovních dokladů v centrálním SIS.
5. Orgány členských států a agentury Unie uvedené v odstavci 1 mohou využívat ESP k vyhledávání údajů týkajících se osob nebo jejich cestovních dokladů v údajích Europolu v souladu se svými přístupovými právy podle unijního a vnitrostátního práva.

Článek 8

Profily uživatelů Evropského vyhledávacího portálu

1. Aby umožnila používání ESP, vytvoří agentura eu-LISA ve spolupráci s členskými státy profil každé kategorie uživatelů ESP a pro účely jejich vyhledávání v souladu s technickými podrobnostmi a přístupovými právy uvedenými v odstavci 2. Každý profil obsahuje v souladu s unijním a vnitrostátním právem tyto informace:
 - a) datová pole používaná při vyhledávání;
 - b) ty informační systémy EU, údaje Europolu a databáze Interpolu, v nichž se má vyhledávat, ty, v nichž lze vyhledávat, a ty, které mají uživatelé poskytnout odpověď;
 - c) konkrétní údaje v informačních systémech EU, údaje Europolu a databáze Interpolu, v nichž lze vyhledávat;
 - d) kategorie údajů, které mohou být uvedeny v každé odpovědi.
2. Komise přijme prováděcí akty, jimiž stanoví technické podrobnosti profilů uvedených v odstavci 1 v souladu s přístupovými právy uživatelů ESP podle právních nástrojů upravujících informační systémy EU a podle vnitrostátního práva. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 70 odst. 2.
3. Agentura eu-LISA ve spolupráci s členskými státy pravidelně a nejméně jednou ročně přezkoumává profily uvedené v odstavci 1 a v případě potřeby je aktualizuje.

Článek 9

Vyhledávání

1. Uživatelé ESP zahájí vyhledávání tak, že do něj zadají alfanumerické nebo biometrické údaje. Po zahájení vyhledávání začne ESP na základě údajů zadaných uživatelem a v souladu s profilem uživatele prohledávat souběžně EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, CIR, údaje Europolu a databáze Interpolu.
2. Kategorie údajů použitých k zahájení vyhledávání prostřednictvím ESP musí odpovídat kategoriím údajů týkajících se osob nebo cestovních dokladů, které lze používat pro vyhledávání v různých informačních systémech EU, údajích Europolu a databázích Interpolu v souladu s právními nástroji upravujícími tyto systémy.
3. Agentura eu-LISA zavede ve spolupráci s členskými státy pro účely ESP dokument pro ovládání rozhraní založený na UMF uvedeném v článku 38.
4. Při zahájení vyhledávání uživatelem ESP poskytnou EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, CIR, MID, údaje Europolu a databáze Interpolu jako odpověď na vyhledávání relevantní údaje, které mají.

Aniž je dotčen článek 20, uvede se v odpovědi od ESP, do kterého informačního systému EU nebo do které databáze daný údaj patří.

ESP neposkytuje žádné informace o údajích v informačních systémech EU, údajích Europolu a databázích Interpolu, k nimž uživatel nemá podle unijního ani vnitrostátního práva přístup.

5. Veškeré vyhledávání v databázích Interpolu zahájené prostřednictvím ESP se provádí tak, aby majiteli záznamu Interpolu nebyly odhaleny žádné informace.
6. ESP uživateli odpoví, jakmile má k dispozici údaje z jednoho z informačních systémů EU, údajů Eurovalu nebo databází Interpolu. Tato odpověď obsahuje pouze údaje, k nimž má uživatel přístup podle unijního a vnitrostátního práva.
7. Komise přijme prováděcí akt, jímž stanoví technický postup pro ESP při vyhledávání v informačních systémech EU, údajích Eurovalu a databázích Interpolu a formát odpovědí ESP. Tento prováděcí akt se přijme přezkumným postupem podle čl. 70 odst. 2.

Článek 10

Vedení a uchovávání protokolů

1. Aniž jsou dotčeny články 12 a 18 nařízení (EU) 2018/1862, článek 29 nařízení (EU) 2019/816 a článek 40 nařízení (EU) 2016/794, agentura eu-LISA vede a uchovává protokoly o všech operacích zpracování údajů v rámci ESP. V těchto protokolech se uvádí:
 - a) členský stát nebo agentura Unie, které zahájily vyhledávání, a použitý profil ESP;
 - b) datum a čas vyhledávání;
 - c) informační systémy EU a údaje Eurovalu, v nichž vyhledávání proběhlo.
2. Každý členský stát vede a uchovává protokoly o vyhledávání, jež provádějí jeho orgány a jejich pracovníci řádně zmocnění k používání ESP. Každá agentura Unie vede a uchovává protokoly o vyhledávání, které provádějí její řádně zmocnění pracovníci.
3. Protokoly uvedené v odstavcích 1 a 2 lze použít pouze pro účely monitorování ochrany údajů, včetně kontroly přípustnosti žádostí a zákonnosti zpracování údajů, a pro zabezpečení údajů a zajištění jejich integrity. Tyto protokoly musí být chráněny vhodnými opatřeními proti neoprávněnému přístupu a vymazány po uplynutí jednoho roku od vytvoření. Pokud jsou však nezbytné pro zahájené monitorovací postupy, vymažou se v okamžiku, kdy již pro ně nebudou zapotřebí.

Článek 11

Záložní postupy pro případ technické nemožnosti použít Evropský vyhledávací portál

1. Pokud je technicky nemožné použít ESP k vyhledávání v jednom či více informačních systémech EU nebo CIR z důvodu selhání ESP, agentura eu-LISA o tom automaticky uvědomí uživatele ESP.
2. Pokud je technicky nemožné použít ESP k vyhledávání v jednom či více informačních systémech EU nebo v CIR z důvodu selhání vnitrostátní infrastruktury v členském státě, členský stát o této skutečnosti automaticky uvědomí agenturu eu-LISA a Komisi.
3. V případech uvedených v odstavci 1 nebo 2 tohoto článku a až do vyřešení technického selhání se neuplatní povinnost uvedená v čl. 7 odst. 2 a 4 a členské státy získají v případě, že tak musí podle unijního nebo vnitrostátního práva učinit, přímý přístup k informačním systémům EU nebo CIR.
4. Pokud je technicky nemožné použít ESP k vyhledávání v jednom či více informačních systémech EU nebo v CIR z důvodu selhání infrastruktury některé agentury Unie, tato agentura o tom automaticky uvědomí agenturu eu-LISA a Komisi.

KAPITOLA III

Sdílená služba pro porovnávání biometrických údajů

Článek 12

Sdílená služba pro porovnávání biometrických údajů

1. Na podporu CIR a MID a cílů EES, VIS, Eurodacu, SIS a ECRIS-TCN se zřizuje sdílená služba pro porovnávání biometrických údajů (sdílená BMS), která ukládá biometrické šablony získané na základě biometrických údajů uvedených v článku 13, které jsou uchovávány v CIR a SIS, a umožňuje vyhledávání s využitím biometrických údajů v několika informačních systémech EU.

2. Sdílenou BMS tvoří:
 - a) centrální infrastruktura, která nahrazuje příslušné centrální systémy EES, VIS, SIS, Eurodacu a ECRIS-TCN v takovém rozsahu, v jakém uchovává biometrické šablony a umožňuje vyhledávat s využitím biometrických údajů;
 - b) zabezpečená komunikační infrastruktura mezi sdílenou BMS, centrálním SIS a CIR.
3. Sdílenou BMS vyvine a její technickou správu zajišťuje agentura eu-LISA.

Článek 13

Ukládání biometrických šablon ve sdílené službě pro porovnávání biometrických údajů

1. Sdílená BMS ukládá biometrické šablony, které získá z těchto biometrických údajů:
 - a) údajů uvedených v čl. 20 odst. 3 písm. w) a y) nařízení (EU) 2018/1862, kromě údajů o otiscích dlaní;
 - b) údajů uvedených v čl. 5 odst. 1 písm. b) a odst. 2 nařízení (EU) 2019/816.

Biometrické šablony se ukládají ve sdílené BMS logicky odděleně podle informačního systému EU, z něhož údaje pocházejí.

2. Pro každý soubor údajů uvedený v odstavci 1 obsahuje sdílená BMS v každé biometrické šabloně odkaz na informační systémy EU, v nichž jsou odpovídající biometrické údaje uloženy, a odkaz na vlastní záznamy v těchto informačních systémech EU.
3. Biometrické šablony lze zadávat do sdílené BMS pouze po automatizované kontrole kvality biometrických údajů přidaných do jednoho z informačních systémů EU, kterou sdílená BMS provede, aby se ověřilo, zda jsou splněny minimální normy kvality údajů.
4. Ukládání údajů uvedených v odstavci 1 musí splňovat normy kvality uvedené v čl. 37 odst. 2.
5. Komise stanoví prostřednictvím prováděcího aktu požadavky na výkonnost a praktické postupy při sledování výkonnosti sdílené BMS, aby bylo zajištěno, že účinnost biometrického vyhledávání odpovídá naléhavosti postupů, jako jsou hraniční kontroly a identifikace. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 70 odst. 2.

Článek 14

Vyhledávání biometrických údajů s využitím sdílené služby pro porovnávání biometrických údajů

CIR a SIS používají k vyhledání biometrických údajů v nich uložených biometrické šablony uložené ve sdílené BMS. Vyhledávání na základě biometrických údajů probíhá v souladu s účely stanovenými v tomto nařízení a v nařízeních (ES) č. 767/2008, (EU) 2017/2226, (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 a (EU) 2019/816.

Článek 15

Uchovávání údajů ve sdílené službě pro porovnávání biometrických údajů

Údaje uvedené v čl. 13 odst. 1 a 2 jsou ve sdílené BMS uloženy jen tak dlouho, dokud jsou odpovídající biometrické údaje uloženy v CIR nebo SIS. Vymaží se ze sdílené BMS automaticky.

Článek 16

Vedení a uchování protokolů

1. Aniž jsou dotčeny články 12 a 18 nařízení (EU) 2018/1862 a článek 29 nařízení (EU) 2019/816, agentura eu-LISA vede a uchovává protokoly o všech operacích zpracování údajů ve sdílené BMS. V těchto protokolech se uvádí:

- a) členský stát nebo agentura Unie, která zahájila vyhledávání;
- b) historie vytváření a ukládání biometrických šablon;
- c) informační systémy EU, v nichž se vyhledává s použitím biometrických šablon uložených ve sdílené BMS;
- d) datum a čas vyhledávání;
- e) druh biometrických údajů použitých k zahájení vyhledávání;
- f) výsledky vyhledávání a datum a čas výsledku.

2. Každý členský stát vede a uchovává protokoly o vyhledávání, jež provádějí jeho orgány a jejich pracovníci řádně zmocnění k používání sdílené BMS. Každá agentura Unie vede a uchovává protokoly o vyhledávání, které provádějí její řádně zmocnění pracovníci.

3. Protokoly uvedené v odstavcích 1 a 2 lze použít pouze pro účely monitorování ochrany údajů, včetně kontroly přípustnosti žádostí a zákonnosti zpracování údajů, a pro zabezpečení údajů a zajištění jejich integrity. Tyto protokoly musí být chráněny vhodnými opatřeními proti neoprávněnému přístupu a vymazány po uplynutí jednoho roku od vytvoření. Pokud jsou však nezbytné pro zahájené monitorovací postupy, vymažou se v okamžiku, kdy již pro ně nebudou zapotřebí.

KAPITOLA IV**Společné úložiště údajů o totožnosti**

Článek 17

Společné úložiště údajů o totožnosti

1. Zřizuje se společné úložiště údajů o totožnosti (CIR), které vytváří samostatný soubor pro každou osobu zaznamenanou v EES, VIS, ETIAS, Eurodacu nebo ECRIS-TCN a obsahuje údaje uvedené v článku 18, s cílem usnadnit v souladu s článkem 20 správné zjištění totožnosti osob registrovaných v EES, VIS, ETIAS, Eurodacu a ECRIS-TCN a napomáhat k němu, podpořit v souladu s článkem 21 fungování MID a v souladu s článkem 22 usnadnit a zjednodušit přístup určených orgánů a Europolu k EES, VIS, ETIAS a Eurodacu, pokud je to nezbytné k prevenci, odhalování nebo vyšetřování teroristických trestných činů či jiných závažných trestných činů.

2. CIR se skládá:

- a) z centrální infrastruktury, která nahrazuje příslušné centrální systémy EES, VIS, ETIAS, Eurodacu a ECRIS-TCN v takovém rozsahu, v jakém uchovává údaje uvedené v článku 18;
- b) ze zabezpečeného komunikačního kanálu mezi CIR, členskými státy a agenturami Unie, které jsou oprávněny používat CIR v souladu s unijním a vnitrostátním právem;
- c) ze zabezpečené komunikační infrastruktury mezi CIR a EES, VIS, ETIAS, Eurodacem a ECRIS-TCN, jakož i centrálními infrastrukturami ESP, sdílené BMS a MID.

3. CIR vyvine a jeho technickou správu zajišťuje agentura eu-LISA.

4. Pokud je z důvodu selhání CIR technicky nemožné v něm vyhledávat pro účely zjištění totožnosti určité osoby podle článku 20, pro odhalování vícenásobné totožnosti podle článku 21 nebo pro účely prevence, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů podle článku 22, agentura eu-LISA o tom automaticky uvědomí uživatele CIR.

5. Agentura eu-LISA zavede ve spolupráci s členskými státy pro účely CIR dokument pro ovládání rozhraní založený na UMF uvedeném v článku 38.

Článek 18

Údaje společného úložiště údajů o totožnosti

1. CIR ukládá následující údaje logicky odděleně podle informačního systému, z něhož pocházejí: údaje uvedené v čl. 5 odst. 1 písm. b) a odst. 2 a následující údaje uvedené v čl. 5 odst. 1 písm. a) nařízení (EU) 2019/816: příjmení, jméno (jména), datum narození, místo narození (obec a země), státní příslušnost (příslušnosti), pohlaví, případné předchozí jméno (jména) nebo příjmení, pseudonymy nebo přezdívky, existují-li, případně informace uvedené v cestovních dokladech.
2. Pro každý soubor údajů uvedený v odstavci 1 obsahuje CIR odkaz na informační systémy EU, do kterých údaje patří.
3. Orgány vstupující do CIR tak činí v souladu se svými přístupovými právy podle právních nástrojů upravujících informační systémy EU a podle vnitrostátního práva a pro účely uvedené v článcích 20, 21 a 22 v souladu se svými přístupovými právy podle tohoto nařízení.
4. Pro každý soubor údajů uvedený v odstavci 1 obsahuje úložiště CIR odkaz na vlastní záznam v informačních systémech EU, do nichž údaje patří.
5. Ukládání údajů uvedených v odstavci 1 musí splňovat normy kvality uvedené v čl. 37 odst. 2.

Článek 19

Doplnění, změna a výmaz údajů ve společném úložišti údajů o totožnosti

1. Pokud jsou údaje v Eurodacu nebo v ECRIS-TCN doplněny, změněny nebo vymazány, automaticky se odpovídajícím způsobem doplní, změní nebo vymaže údaje uvedené v článku 18 uložené v individuálním souboru CIR.
2. Pokud je v MID vytvořeno v souladu s článkem 32 nebo 33 bílé nebo červené propojení mezi údaji dvou nebo více informačních systémů EU, z nichž se CIR skládá, CIR namísto vytvoření nového individuálního souboru doplní nové údaje do individuálního souboru propojených údajů.

Článek 20

Přístup do společného úložiště údajů o totožnosti pro účely zjištění totožnosti

1. Policejní orgán provede vyhledávání v CIR v souladu s odstavci 2 a 5 pouze za těchto okolností:
 - a) pokud policejní orgán není schopen zjistit totožnost osoby, protože tato osoba nemá cestovní doklad ani jiný důvěryhodný doklad prokazující její totožnost;
 - b) pokud existují pochybnosti o údajích o totožnosti poskytnutých určitou osobou;
 - c) pokud existují pochybnosti o pravosti cestovního dokladu nebo jiného důvěryhodného dokladu poskytnutého určitou osobou;
 - d) pokud existují pochybnosti o totožnosti držitele cestovního dokladu nebo jiného věrohodného dokladu, nebo
 - e) pokud určitá osoba není schopna nebo odmítá spolupracovat.

Toto vyhledávání není povoleno v případě nezletilých osob mladších 12 let, ledaže je to v nejlepším zájmu dítěte.

2. Pokud nastane jedna z okolností uvedených v odstavci 1 a policejní orgán je k tomu zmocněn vnitrostátními legislativními opatřeními uvedenými v odstavci 5, může výhradně pro účely zjištění totožnosti osoby vyhledávat v CIR s využitím biometrických údajů této osoby, které získal přímo během kontroly totožnosti za podmínky, že daný postup byl zahájen v přítomnosti této osoby.

3. Pokud vyhledávání ukáže, že údaje o určité osobě jsou uloženy v CIR, má policejní orgán přístup k údajům uvedeným v čl. 18 odst. 1.

Pokud nelze biometrické údaje osoby použít nebo pokud vyhledávání na základě těchto údajů není úspěšné, měly by se pro vyhledávání použít údaje o totožnosti této osoby ve spojení s údaji v cestovním dokladu nebo s použitím údajů o totožnosti poskytnutých touto osobou.

4. Pokud je k tomu policejní orgán zmocněn vnitrostátními legislativními opatřeními uvedenými v odstavci 6, může v případě přírodní katastrofy, nehody nebo teroristického útoku vyhledávat v CIR s využitím biometrických údajů, a to výhradně pro účely zjištění totožnosti neznámých osob, které nejsou schopny samy svou totožnost prokázat, nebo identifikaci lidských pozůstatků.
5. Členské státy, které si přejí využít možnost stanovenou v odstavci 2, přijmou příslušná vnitrostátní legislativní opatření. Členské státy přitom zohlední potřebu zamezit jakékoli diskriminaci státních příslušníků třetích zemí. Taková legislativní opatření vymezí přesné účely zjištění totožnosti v rámci účelů uvedených v čl. 2 odst. 1 písm. b) a c). Členské státy určí příslušné policejní orgány a stanoví postupy, podmínky a kritéria takových kontrol.
6. Členské státy, které si přejí využít možnost stanovenou v odstavci 4, přijmou vnitrostátní legislativní opatření stanovující postupy, podmínky a kritéria.

Článek 21

Přístup do společného úložiště údajů o totožnosti pro odhalování vícenásobných totožností

1. Pokud je výsledkem vyhledávání v CIR žluté propojení v souladu s čl. 28 odst. 4, orgán odpovědný za manuální ověření různých totožností určený v souladu s článkem 29 má výhradně pro účely takového ověření přístup k údajům uvedeným ve čl. 18 odst. 1 a 2, které jsou uloženy v CIR a spojeny žlutým propojením.
2. Pokud je výsledkem vyhledávání v CIR červené propojení v souladu s článkem 32, mají orgány uvedené v čl. 26 odst. 2 výhradně pro účely boje proti podvodnému zneužívání totožnosti přístup k údajům uvedeným ve čl. 18 odst. 1 a 2, které jsou uloženy v CIR a spojeny červeným propojením.

Článek 22

Vyhledávání ve společném úložišti údajů o totožnosti pro účely prevence, odhalování a vyšetřování teroristických trestných činů nebo jiných závažných trestných činů

1. Ve zvláštním případě, kdy existují oprávněné důvody se domnívat, že nahlédnutí do informačních systémů EU přispěje k prevenci, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů, zejména pokud existuje důvodné podezření, že podezřelý, pachatel nebo oběť teroristického trestného činu nebo jiného závažného trestného činu je osobou, jejíž údaje jsou uloženy v Eurodacu, určené orgány členských států a Europol mohou nahlédnout do CIR za účelem získání informací o tom, zda se údaje týkající se konkrétní osoby vyskytují v Eurodacu.
2. Pokud CIR v odpovědi na vyhledávání uvede, že se údaje o dané osobě vyskytují v Eurodacu, poskytne určeným orgánům a Europolu odpověď v podobě odkazu podle čl. 18 odst. 2 uvádějícího, že Eurodac obsahuje odpovídající údaje. CIR odpoví takovým způsobem, aby nebylo narušeno zabezpečení těchto údajů.

Odpověď, že se v Eurodacu vyskytují údaje o dané osobě, lze použít pouze pro podání žádosti o plný přístup v souladu s podmínkami a postupy stanovenými v právním nástroji upravujícím takový přístup.

V případě shody nebo více shod požádá určený orgán nebo Europol o plný přístup do nejméně jednoho z informačních systémů, které shodu nahlásily.

Pokud není ve výjimečných případech plný přístup požadován, určené orgány zaznamenají odůvodnění, proč o plný přístup nepožádaly, které musí být dohledatelné ve vnitrostátním spisu. Europol zaznamená odůvodnění do příslušného spisu.

3. Plný přístup k údajům obsaženým v Eurodacu pro účely prevence, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů nadále podléhá podmínkám a postupům stanoveným v právním nástroji upravujícím takový přístup.

Článek 23

Uchovávání údajů ve společném úložišti údajů o totožnosti

1. Údaje uvedené v čl. 18 odst. 1, 2 a 4 se z CIR automaticky vymažou v souladu s příslušnými ustanoveními o uchovávání údajů nařízení (EU) 2019/816.
2. Individuální soubor je v CIR uložen jen tak dlouho, dokud jsou odpovídající údaje uloženy alespoň v jednom z informačních systémů EU, jejichž údaje jsou obsaženy v CIR. Vytvoření propojení nemá vliv na dobu uchovávání jednotlivých položek propojených údajů.

Článek 24

Vedení a uchovávání protokolů

1. Aniž je dotčen článek 29 nařízení (EU) 2019/816, agentura eu-LISA vede a uchovává protokoly o všech operacích zpracování údajů v rámci CIR v souladu s odstavci 2, 3 a 4 tohoto článku.
2. Agentura eu-LISA vede a uchovává protokoly o všech operacích zpracování údajů podle článku 20 v rámci CIR. V těchto protokolech se uvádí:
 - a) členský stát nebo agentura Unie, která zahájila vyhledávání;
 - b) účel přístupu uživatele, který vyhledává prostřednictvím CIR;
 - c) datum a čas vyhledávání;
 - d) druh údajů použitých k zahájení vyhledávání;
 - e) výsledky vyhledávání.
3. Agentura eu-LISA vede a uchovává protokoly o všech operacích zpracování údajů podle článku 21 v rámci CIR. V těchto protokolech se uvádí:
 - a) členský stát nebo agentura Unie, která zahájila vyhledávání;
 - b) účel přístupu uživatele, který vyhledává prostřednictvím CIR;
 - c) datum a čas vyhledávání;
 - d) údaje použité k zahájení vyhledávání, pokud je vytvořeno propojení, a výsledky vyhledávání uvádějící informační systém EU, ze kterého údaje pocházejí.
4. Agentura eu-LISA vede a uchovává protokoly o všech operacích zpracování údajů podle článku 22 v CIR. V těchto protokolech se uvádí:
 - a) datum a čas vyhledávání;
 - b) údaje použité k zahájení vyhledávání;
 - c) výsledky vyhledávání;
 - d) členský stát nebo agentura Unie vyhledávající v CIR.

Protokoly o takovém přístupu pravidelně ověřuje příslušný dozorový úřad v souladu s článkem 41 směrnice (EU) 2016/680 nebo evropský inspektor ochrany údajů v souladu s článkem 43 nařízení (EU) 2016/794, a to s odstupy nepřekračujícími šest měsíců, s cílem ověřit, zda jsou dodržovány postupy a podmínky stanovené v čl. 22 odst. 1 a 2 tohoto nařízení.

5. Každý členský stát vede a uchovává protokoly o vyhledávání, jež provádějí jeho orgány a jejich pracovníci řádně zmocnění k používání CIR podle článků 20, 21 a 22. Každá agentura Unie vede a uchovává protokoly o vyhledávání, které provádějí její řádně zmocnění pracovníci podle článků 21 a 22.

Kromě toho v souvislosti s jakýmkoli přístupem do CIR podle článku 22 každý členský stát vede a uchovává protokoly, v nichž se uvádí:

- a) odkaz na vnitrostátní spis;
- b) účel přístupu;
- c) v souladu s vnitrostátními pravidly jedinečný identifikátor pracovníka, který provedl vyhledání, a pracovníka, který vyhledání nařídil.

6. V souladu s nařízením (EU) 2016/794 Europol vede a uchovává pro jakýkoli přístup do CIR podle článku 22 tohoto nařízení protokoly s jedinečným identifikátorem pracovníka, který vyhledávání provedl, a pracovníka, který vyhledávání nařídil.

7. Protokoly uvedené v odstavcích 2 až 6 lze použít pouze pro účely monitorování ochrany údajů, včetně kontroly přípustnosti vyhledávání a zákonnosti zpracování údajů, a pro zabezpečení údajů a zajištění jejich integrity. Tyto protokoly musí být chráněny vhodnými opatřeními proti neoprávněnému přístupu a vymazány po uplynutí jednoho roku od vytvoření. Pokud jsou však nezbytné pro zahájené monitorovací postupy, vymaže se v okamžiku, kdy již pro ně nebudou zapotřebí.

8. Agentura eu-LISA ukládá protokoly související s historií údajů do individuálních souborů. Automaticky je vymaže, jakmile jsou vymazány údaje.

KAPITOLA V

Detektor vícenásobné totožnosti

Článek 25

Detektor vícenásobné totožnosti

1. Na podporu fungování CIR a cílů EES, VIS, ETIAS, Eurodacu, SIS a ECRIS-TCN se zřizuje detektor vícenásobné totožnosti (MID), který vytváří a ukládá soubory údajů souvisejících s potvrzením totožnosti uvedené v článku 34 obsahující propojení mezi údaji v informačních systémech EU zahrnutých v CIR a v SIS a umožňující odhalení vícenásobné totožnosti s dvojitým účelem, kterým je usnadnění kontrol totožnosti a potírání podvodného zneužívání totožnosti.

2. MID se skládá:

- a) z centrální infrastruktury, která ukládá propojení a odkazy na informační systémy EU;
- b) ze zabezpečené komunikační infrastruktury k propojení MID se SIS a centrálními infrastrukturami ESP a CIR.

3. MID vyvine a jeho technickou správu zajišťuje agentura eu-LISA.

Článek 26

Přístup k detektoru vícenásobné totožnosti

1. Pro účely manuálního ověření různých totožností uvedeného v článku 29 se přístup k údajům uvedeným v článku 34 uloženým v MID udělí:

- a) centrále SIRENE členského státu, která vytváří nebo aktualizuje záznam v souladu s nařízením (EU) 2018/1862;
- b) ústředním orgánům odsuzujícího členského státu při záznamu nebo změně údajů v ECRIS-TCN v souladu s článkem 5 nebo 9 nařízení (EU) 2019/816.

2. Orgány členských států a agentury Unie s přístupem alespoň do jednoho informačního systému EU, který je součástí CIR, nebo do SIS mají přístup k údajům uvedeným v čl. 34 písm. a) a b), pokud jde o červená propojení uvedená v článku 32.

3. Orgány členských států a agentury Unie mají přístup k bílým propojením uvedeným ve článku 33, pokud mají přístup k těm dvěma informačním systémům EU, které obsahují údaje, mezi nimiž bylo bílé propojení vytvořeno.

4. Orgány členských států a agentury Unie mají přístup k zeleným propojením uvedeným ve článku 31, pokud mají přístup k těm dvěma informačním systémům EU obsahujícím údaje, mezi nimiž bylo zelené propojení vytvořeno, a vyhledávání v těchto informačních systémech odhalilo shodu se dvěma soubory propojených údajů.

Článek 27

Odhalování vícenásobné totožnosti

1. Odhalování vícenásobné totožnosti v CIR a v SIS je zahájeno, je-li:
 - a) v SIS vytvořen nebo aktualizován záznam o určité osobě v souladu s článkem kapitolami VI až IX nařízení (EU) 2018/1862;
 - b) v ECRIS-TCN je vytvořen nebo změněn datový záznam v souladu s článkem 5 nebo 9 nařízení (EU) 2019/816.
2. Pokud údaje obsažené v informačním systému EU uvedeném v odstavci 1 obsahují biometrické údaje, CIR a centrální SIS použijí sdílenou BMS, aby odhalily vícenásobnou totožnost. Sdílená BMS porovnává biometrické šablony získané ze všech nových biometrických údajů s biometrickými šablonami již obsaženými ve sdílené BMS, aby se ověřilo, zda údaje patřící téže osobě jsou již uloženy v CIR nebo v centrálním SIS.
3. Vedle postupu uvedeného v odstavci 2 CIR a centrální SIS využívají ESP k vyhledání údajů uložených v centrálním SIS nebo případně v CIR s využitím následujících údajů:
 - a) příjmení, jméno (jména), rodné (rodná) příjmení, dříve užívané (užívaná) jméno (jména) a alias, místo narození, datum narození, pohlaví a veškeré státní příslušnosti dotčené osoby uvedené v čl. 20 odst. 3 nařízení (EU) 2018/1862;
 - b) příjmení, jméno (jména), datum narození, místo narození (obec a země), státní příslušnost (příslušnosti) a pohlaví uvedené v čl. 5 odst. 1 písm. a) nařízení (EU) 2019/816.
4. Vedle postupu uvedeného v odstavcích 2 a 3 CIR a centrální SIS využívají ESP k vyhledání údajů uložených v centrálním SIS a v CIR s využitím údajů o cestovních dokladech.
5. Odhalování vícenásobné totožnosti lze zahájit pouze za účelem porovnání údajů dostupných v jednom informačním systému EU s údaji dostupnými v jiných informačních systémech EU.

Článek 28

Výsledky odhalení vícenásobné totožnosti

1. Pokud vyhledávání uvedené v čl. 27 odst. 2, 3 a 4 nevykáže žádnou shodu, pokračují postupy uvedené v čl. 27 odst. 1 v souladu s právními nástroji, které je upravují.
2. Pokud vyhledávání uvedené v čl. 27 odst. 2, 3 a 4 vykáže jednu či více shod, CIR a tam, kde je to relevantní, i SIS vytvoří propojení mezi údaji použitými k zahájení vyhledávání a údaji, které vedly ke shodě.

Pokud je více shod, vytvoří se propojení mezi všemi údaji, které ke shodě vedly. Pokud propojení mezi údaji již bylo vytvořeno, stávající propojení se rozšíří i na údaje použité k zahájení vyhledávání.
3. Pokud vyhledávání uvedené v čl. 27 odst. 2, 3 a 4 vykáže jednu či více shod a údaje o totožnosti v propojených souborech jsou stejné nebo podobné, vytvoří se v souladu s článkem 33 bílé propojení.
4. Pokud vyhledávání uvedené v čl. 27 odst. 2, 3 a 4 vykáže jednu či více shod a údaje o totožnosti v propojených souborech nelze považovat za podobné, vytvoří se v souladu s článkem 30 žluté propojení a použije se postup uvedený v článku 29.
5. Komise přijme akty v přenesené pravomoci v souladu s článkem 69, kterými stanoví postupy pro určení případů, kdy lze údaje o totožnosti považovat za stejné nebo podobné.
6. Propojení se ukládají v souboru údajů souvisejících s potvrzením totožnosti uvedeném v článku 34.
7. Komise stanoví ve spolupráci s agenturou eu-LISA technická pravidla pro vytváření propojení mezi údaji z různých informačních systémů EU prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 70 odst. 2.

Článek 29

Manuální ověření různých totožností a odpovědné orgány

1. Aniž je dotčen odstavec 2, jsou orgány odpovědnými za manuální ověření různých totožností:
 - a) centrála SIRENE členského státu v případě shod, které se vyskytnou při vytváření nebo aktualizaci záznamu v SIS v souladu s nařízením (EU) 2018/1862;
 - b) ústřední orgány odsuzujícího členského státu v případě shod, které se vyskytnou při zaznamenávání nebo změně údajů v ECRIS-TCN v souladu s článkem 5 nebo 9 nařízení (EU) 2019/816.

MID označí orgán odpovědný za manuální ověření různých totožností v souboru údajů souvisejících s potvrzením totožnosti.

2. Orgánem odpovědným za manuální ověření různých totožností v souboru údajů souvisejících s potvrzením totožnosti je centrála SIRENE členského státu, který vytvořil záznam, v němž je vytvořeno propojení s údaji obsaženými v záznamu:

- a) o osobách hledaných za účelem zatčení a předání nebo vydání uvedeném v článku 26 nařízení (EU) 2018/1862;
- b) o pohřešovaných nebo zranitelných osobách uvedeném v článku 32 nařízení (EU) 2018/1862;
- c) o osobách hledaných za účelem zajištění jejich spolupráce v soudním řízení uvedeném v článku 34 nařízení (EU) 2018/1862;
- d) o osobách pro účely skrytých, dotazovacích nebo zvláštních kontrol uvedeném v článku 36 nařízení (EU) 2018/1862.

3. Orgán odpovědný za manuální ověření různých totožností má přístup k propojeným údajům obsaženým v příslušném souboru údajů souvisejících s potvrzením totožnosti a k údajům o totožnosti spojeným v CIR a případně v SIS. Bezodkladně posuzuje různé totožnosti. Jakmile je toto posouzení dokončeno, v souladu s články 31, 32 a 33 aktualizuje propojení a neprodleně je doplní do souboru údajů souvisejících s potvrzením totožnosti

4. Pokud je vytvořeno více než jedno propojení, posoudí orgán odpovědný za manuální ověření různých totožností každé propojení zvlášť.

5. Pokud již byly údaje vykazující shodu propojeny, orgán odpovědný za manuální ověření různých totožností stávající propojení zohlední při posuzování potřeby vytvořit nová propojení.

Článek 30

Žluté propojení

1. Neproběhlo-li ještě manuální ověření různých totožností, propojení údajů ze dvou či více informačních systémů EU se označí jako žluté ve všech těchto případech:

- a) propojené údaje sdílejí stejné biometrické údaje, ale mají podobné nebo odlišné údaje o totožnosti;
- b) propojené údaje mají odlišné údaje o totožnosti, ale sdílejí stejné údaje o cestovním dokladu, a alespoň jeden z informačních systémů EU neobsahuje biometrické údaje o dotčené osobě;
- c) propojené údaje sdílejí stejné údaje o totožnosti, ale mají odlišné biometrické údaje;
- d) propojené údaje mají podobné nebo odlišné údaje o totožnosti a sdílejí stejné údaje o cestovním dokladu, ale mají odlišné biometrické údaje.

2. Pokud se propojení označí v souladu s odstavcem 1 jako žluté, použije se postup stanovený v článku 29.

Článek 31

Zelené propojení

1. Propojení mezi údaji ze dvou či více informačních systémů EU se označí jako zelené, pokud:
 - a) propojené údaje mají odlišné biometrické údaje, ale sdílejí stejné údaje o totožnosti, a orgán odpovědný za manuální ověření různých totožností dospěl k závěru, že tyto propojené údaje odkazují na dvě různé osoby;
 - b) propojené údaje mají odlišné biometrické údaje, mají podobné nebo odlišné údaje o totožnosti, sdílejí stejné údaje o cestovním dokladu a orgán odpovědný za manuální ověření různých totožností dospěl k závěru, že tyto propojené údaje odkazují na dvě různé osoby;
 - c) propojené údaje mají odlišné údaje o totožnosti, ale sdílejí stejné údaje o cestovním dokladu, alespoň jeden z informačních systémů EU neobsahuje biometrické údaje o dotčené osobě a orgán odpovědný za manuální ověření různých totožností dospěl k závěru, že tyto propojené údaje odkazují na dvě různé osoby.
2. Pokud se vyhledávání uskuteční v CIR nebo v SIS a pokud existuje zelené propojení mezi údaji ve dvou či více informačních systémech EU, uvede MID, že údaje o totožnosti propojených údajů neodpovídají téže osobě.
3. Pokud má orgán členského státu důkazy, z nichž vyplývá, že zelené propojení bylo v MID zaznamenáno nesprávně, není aktuální nebo že údaje byly v MID nebo v informačních systémech EU zpracovány v rozporu s tímto nařízením, zkontroluje příslušné údaje uložené v CIR a v SIS a v případě potřeby propojení v MID neprodleně opraví nebo vymaže. Orgán členského státu neprodleně uvědomí členský stát odpovědný za manuální ověření různých totožností.

Článek 32

Červené propojení

1. Propojení mezi údaji ze dvou či více informačních systémů EU se označí jako červené ve všech těchto případech:
 - a) propojené údaje sdílejí stejné biometrické údaje, ale mají podobné nebo odlišné údaje o totožnosti a orgán odpovědný za manuální ověření různých totožností dospěl k závěru, že tyto propojené údaje neoprávněně odkazují na tutéž osobu;
 - b) propojené údaje mají stejné, podobné nebo odlišné údaje o totožnosti a sdílejí stejné údaje o cestovním dokladu, ale mají odlišné biometrické údaje a orgán odpovědný za manuální ověření různých totožností dospěl k závěru, že tyto propojené údaje odkazují na dvě odlišné osoby a alespoň jedna z nich používá stejný cestovní doklad neoprávněně;
 - c) propojené údaje sdílejí stejné údaje o totožnosti, ale mají odlišné biometrické údaje, mají odlišné nebo nemají žádné údaje o cestovním dokladu a orgán odpovědný za manuální ověření různých totožností dospěl k závěru, že tyto propojené údaje neoprávněně odkazují na dvě různé osoby;
 - d) propojené údaje mají odlišné údaje o totožnosti, ale sdílejí stejné údaje o cestovním dokladu, alespoň jeden z informačních systémů EU neobsahuje biometrické údaje o dotčené osobě a orgán odpovědný za manuální ověření různých totožností dospěl k závěru, že tyto propojené údaje neoprávněně odkazují na tutéž osobu.
2. Pokud se vyhledávání uskuteční v CIR nebo v SIS a pokud existuje červené propojení mezi údaji ve dvou či více informačních systémech EU, uvede MID údaje uvedené v článku 34. Opatření v návaznosti na červené propojení se provádějí v souladu s unijním a vnitrostátním právem a jakékoli právní důsledky pro dotčenou osobu se zakládají jen na údajích pro ni relevantních. Pro dotčenou osobu nevyplývají z pouhé existence červeného propojení žádné právní důsledky.
3. Pokud se vytvoří červené propojení mezi údaji v EES, VIS, ETIAS, Eurodacu nebo ECRIS-TCN, individuální soubor uložený v CIR se aktualizuje v souladu s čl. 19 odst. 2.

4. Aniž jsou dotčena ustanovení nařízení (EU) 2018/1860, (EU) 2018/1861 a (EU) 2018/1862 o zpracování záznamů v SIS a aniž jsou dotčena omezení nutná z důvodu ochrany bezpečnosti a veřejného pořádku, prevence trestné činnosti a zaručení řádného průběhu vnitrostátních vyšetřování, pokud se vytvoří červené propojení, informuje orgán odpovědný za manuální ověření různých totožností dotčenou osobu o existenci údajů o nezákonné vícenásobné totožnosti a poskytne jí jediné identifikační číslo uvedené ve čl. 34 písm. c) tohoto nařízení, odkaz na orgán odpovědný za manuální ověření různých totožností uvedený ve čl. 34 písm. d) tohoto nařízení a internetovou adresu internetového portálu zřízeného v souladu s článkem 49 tohoto nařízení.

5. Informace uvedené v odstavci 4 poskytne orgán odpovědný za manuální ověření různých totožností písemně prostřednictvím standardního formuláře. Komise stanoví obsah a formu tohoto formuláře prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 70 odst. 2.

6. Pokud se vytvoří červené propojení, oznámí to MID automaticky orgánům odpovědným za propojené údaje.

7. Mají-li orgán členského státu nebo agentura Unie s přístupem k CIR nebo SIS důkaz nasvědčující tomu, že červené propojení bylo v MID zaznamenáno nesprávně nebo že údaje byly zpracovány v MID, CIR nebo SIS v rozporu s tímto nařízením, zkontroluje relevantní údaje uložené v CIR a SIS a:

- a) informují okamžitě příslušnou centrálu SIRENE členského státu, který záznam v SIS vytvořil, pokud se propojení týká jednoho ze záznamů v SIS uvedených ve čl. 29 odst. 2; nebo
- b) ve všech ostatních případech propojení v MID okamžitě opraví či vymaže.

Je-li kontaktována centrála SIRENE podle prvního pododstavce písm. a), ověří důkazy poskytnuté orgánem členského státu nebo agenturou Unie a v případě potřeby okamžitě propojení v MID opraví nebo vymaže.

Orgán členského státu, který získá uvedený důkaz, neprodleně informuje orgán členského státu odpovědný za manuální ověření různých totožností o jakýchkoli relevantních opravách nebo výmazech červeného propojení.

Článek 33

Bílé propojení

1. Propojení údajů ze dvou či více informačních systémů EU se označí jako bílé ve všech těchto případech:

- a) propojené údaje sdílejí stejné biometrické údaje a stejné nebo podobné údaje o totožnosti;
- b) propojené údaje sdílejí stejné nebo podobné údaje o totožnosti a stejné údaje o cestovním dokladu a alespoň jeden z informačních systémů EU neobsahuje biometrické údaje o dané osobě;
- c) propojené údaje sdílejí stejné biometrické údaje a stejné údaje o cestovním dokladu a mají podobné údaje o totožnosti;
- d) propojené údaje sdílí stejné biometrické údaje, ale mají podobné nebo odlišné údaje o totožnosti a orgán odpovědný za manuální ověření různých totožností dospěl k závěru, že tyto propojené údaje oprávněně odkazují na tutéž osobu.

2. Pokud se vyhledávání uskuteční v CIR nebo v SIS a pokud existuje bílé propojení mezi údaji ve dvou či více informačních systémech EU, uvede MID, že údaje o totožnosti propojených údajů odpovídají téže osobě. Prohledávané informační systémy EU v relevantních případech v odpovědi uvedou veškeré propojené údaje o dané osobě, což povede ke shodě na základě údajů, které jsou propojeny bílým propojením, jestliže má orgán, který vyhledávání zahájil, podle unijního nebo vnitrostátního práva k propojeným údajům přístup.

3. Pokud se vytvoří bílé propojení mezi údaji v EES, VIS, ETIAS, Eurodacu nebo ECRIS-TCN, individuální soubor uložený v CIR se aktualizuje v souladu s čl. 19 odst. 2.

4. Aniž jsou dotčena ustanovení nařízení (EU) 2018/1860, (EU) 2018/1861 a (EU) 2018/1862 o zpracování záznamů v SIS a aniž jsou dotčena omezení nutná z důvodu ochrany bezpečnosti a veřejného pořádku, prevence trestné činnosti a zaručení řádného průběhu vnitrostátních vyšetřování, pokud se po manuálním ověření různých totožností vytvoří bílé propojení, informuje orgán odpovědný za manuální ověření různých totožností dotčenou osobu o podobných nebo odlišných údajích o totožnosti a poskytne jí písemně jediné identifikační číslo uvedené ve čl. 34 písm. c) tohoto nařízení, odkaz na orgán odpovědný za manuální ověření různých totožností uvedený ve čl. 34 písm. d) tohoto nařízení a internetovou adresu internetového portálu zřízeného v souladu s článkem 49 tohoto nařízení.

5. Pokud má orgán členského státu důkazy, z nichž vyplývá, že bílé propojení bylo v MID zaznamenáno nesprávně, že není aktuální nebo že údaje byly v MID nebo v informačních systémech EU zpracovány v rozporu s tímto nařízením, zkontroluje relevantní údaje uložené v CIR a v SIS a v případě potřeby propojení v MID neprodleně opraví nebo vymaže. Orgán členského státu neprodleně uvědomí členský stát odpovědný za manuální ověření různých totožností.

6. Informace uvedené v odstavci 4 poskytne orgán odpovědný za manuální ověření různých totožností písemně prostřednictvím standardního formuláře. Komise stanoví obsah a formu tohoto formuláře prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 70 odst. 2.

Článek 34

Soubor údajů souvisejících s potvrzením totožnosti

Soubor údajů souvisejících s potvrzením totožnosti obsahuje tyto údaje:

- a) propojení uvedená v člácích 30 až 33;
- b) odkaz na informační systémy EU, v nichž jsou uchovávány propojené údaje;
- c) jediné identifikační číslo umožňující získat propojené údaje z odpovídajících informačních systémů EU;
- d) orgán odpovědný za manuální ověření různých totožností;
- e) datum vytvoření nebo aktualizace propojení.

Článek 35

Uchovávání údajů v detektoru vícenásobné totožnosti

Soubory údajů souvisejících s potvrzením totožnosti a údaje v těchto souborech, včetně propojení, jsou v MID uloženy jen tak dlouho, dokud jsou propojené údaje uloženy ve dvou či více informačních systémech EU. Vymaží se z MID automaticky.

Článek 36

Vedení a uchovávání protokolů

1. Agentura eu-LISA vede a uchovává protokoly o všech operacích zpracování údajů v MID. V těchto protokolech se uvádí:

- a) členský stát, který zahájil vyhledávání;
- b) účel přístupu uživatele;
- c) datum a čas vyhledávání;
- d) druh údajů použitých k zahájení vyhledávání;
- e) odkaz na propojené údaje;
- f) historie souboru údajů souvisejících s potvrzením totožnosti;

2. Každý členský stát vede a uchovává protokoly o vyhledávání, jež provádějí jeho orgány a jejich pracovníci řádně zmocnění k používání MID. Každá agentura Unie vede a uchovává protokoly o vyhledávání, které provádějí její řádně zmocnění pracovníci.

3. Protokoly uvedené v odstavcích 1 a 2 lze použít pouze pro účely monitorování ochrany údajů, včetně kontroly přípustnosti vyhledávání a zákonnosti zpracování údajů, a pro zabezpečení údajů a zajištění jejich integrity. Tyto protokoly musí být chráněny vhodnými opatřeními proti neoprávněnému přístupu a vymazány po uplynutí jednoho roku od vytvoření. Pokud jsou však nezbytné pro zahájené monitorovací postupy, vymaže se v okamžiku, kdy již pro ně nebudou postupy zapotřebí.

KAPITOLA VI

Opatření na podporu interoperability

Článek 37

Kvalita údajů

1. Aniž je dotčena odpovědnost členských států za kvalitu údajů vkládaných do systémů, zavede agentura eu-LISA mechanismy a postupy pro automatizovanou kontrolu kvality údajů, jež se budou vztahovat na údaje uložené v SIS, Eurodacu, ECRIS-TCN, sdílené BMS a CIR.

2. Agentura eu-LISA zavede mechanismy pro hodnocení přesnosti sdílené BMS, společné ukazatele kvality údajů a minimální normy kvality pro ukládání údajů v SIS, Eurodacu, ECRIS-TCN, sdílené BMS a CIR.

Do SIS, Eurodacu, ECRIS-TCN, sdílené BMS, CIR a MID mohou být vkládány pouze údaje, které splňují minimální normy kvality.

3. Agentura eu-LISA pravidelně předkládá členským státům zprávy o mechanismech a postupech pro automatizovanou kontrolu kvality údajů a o společných ukazatelích kvality údajů. Agentura eu-LISA rovněž pravidelně předkládá Komisi zprávy o vzniklých problémech a dotčených členských státech. Tuto zprávu na požádání předloží rovněž Evropskému parlamentu a Radě. Zprávy předkládané podle tohoto odstavce nesmějí obsahovat osobní údaje.

4. Podrobnosti o mechanismech a postupech pro automatizovanou kontrolu kvality údajů, společných ukazatelích kvality údajů a minimálních normách kvality pro ukládání údajů v SIS, Eurodacu, ECRIS-TCN, sdílené BMS a CIR, zejména v souvislosti s biometrickými údaji, se stanoví v prováděcích aktech. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 70 odst. 2.

5. Po uplynutí jednoho roku od zavedení mechanismů a postupů pro automatizovanou kontrolu kvality údajů, společných ukazatelů kvality údajů a minimálních standardů kvality údajů a poté každý rok Komise vyhodnotí zavádění kvality údajů členskými státy a učiní nezbytná doporučení. Členské státy poskytnou Komisi akční plán na nápravu nedostatků zjištěných v hodnotící zprávě, a zejména problémů s kvalitou údajů plynoucích z výskytu chybných údajů v informačních systémech EU. Členské státy podávají pravidelně zprávu o pokroku v plnění tohoto akčního plánu až do jeho plného provedení.

Komise předá hodnotící zprávu Evropskému parlamentu, Radě, evropskému inspektorovi ochrany údajů, Evropskému sboru pro ochranu osobních údajů a Agentuře Evropské unie pro základní práva, zřízené nařízením Rady (ES) č. 168/2007 ⁽³⁷⁾.

Článek 38

Univerzální formát pro zprávy

1. Zavádí se norma univerzálního formátu pro zprávy (UMF). UMF vymezuje standardy pro určité prvky přeshraniční výměny informací mezi informačními systémy, orgány nebo organizacemi v oblasti justice a vnitřních věcí.

⁽³⁷⁾ Nařízení Rady (ES) č. 168/2007 ze dne 15. února 2007, kterým se zřizuje Agentura Evropské unie pro základní práva (Úř. věst. L 53, 22.2.2007, s. 1).

2. Norma UMF se použije při vývoji Eurodacu, ECRIS-TCN, ESP, CIR, MID a případně, je-li to vhodné, při vývoji nových modelů pro výměnu informací a informačních systémů v oblasti justice a vnitřních věcí agenturou eu-LISA nebo jakoukoli jinou agenturou Unie.
3. Komise přijme prováděcí akt, kterým stanoví a vypracuje normu UMF uvedenou v odstavci 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 70 odst. 2.

Článek 39

Centrální úložiště pro podávání zpráv a statistiky

1. Zřizuje se centrální úložiště pro podávání zpráv a statistiky (CRRS) na podporu cílů SIS, Eurodacu a ECRIS-TCN, v souladu s příslušnými právními nástroji upravujícími tyto systémy, a poskytování mezisystémových statistických údajů a analytických zpráv pro politické a provozní účely a pro účely kvality údajů.
 2. Agentura eu-LISA zřídí, provede a provozuje ve svých technických prostorách CRRS obsahující údaje a statistiky uvedené v článku 74 nařízení (EU) 2018/1862 a článku 32 nařízení (EU) 2019/816, které jsou logicky odděleny podle informačního systému EU. Přístup k CRRS je poskytován pomocí kontrolovaného zabezpečeného přístupu se specifickými uživatelskými profily, a to výlučně pro podávání zpráv a statistiky orgánům uvedeným v článku 74 nařízení (EU) 2018/1862 a článku 32 nařízení (EU) 2019/816.
 3. Agentura eu-LISA údaje anonymizuje a tyto anonymizované údaje zaznamená v CRRS. Anonymizace údajů je automatizovaná.
- Údaje obsažené v CRRS nesmějí umožnit zjištění totožnosti jednotlivců.
4. CRRS se skládá:
 - a) z nástrojů sloužících k anonymizaci údajů;
 - b) z centrální infrastruktury, kterou tvoří úložiště anonymizovaných údajů;
 - c) ze zabezpečené komunikační infrastruktury pro připojení CRRS k SIS, Eurodacu a ECRIS-TCN, jakož i k centrálním infrastrukturám sdílené BMS, CIR a MID.
 5. Komise přijme akt v přenesené pravomoci v souladu s článkem 69, kterým stanoví podrobná pravidla pro fungování CRRS, včetně ochranných opatření pro zpracovávání osobních údajů podle odstavců 2 a 3 tohoto článku a bezpečnostních pravidel týkajících se úložiště.

KAPITOLA VII

Ochrana údajů

Článek 40

Správce údajů

1. V souvislosti se zpracováním údajů ve sdílené BMS jsou orgány členských států, které jsou správci pro Eurodac, SIS a ECRIS-TCN, správci ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679 nebo čl. 3 bodu 8 směrnice (EU) 2016/680, pokud jde o biometrické šablony získané z údajů uvedených v článku 13 tohoto nařízení, které zadávají do základních systémů, a odpovídají za zpracování biometrických šablon ve sdílené BMS.
2. V souvislosti se zpracováním údajů v CIR jsou orgány členských států, které jsou správci pro Eurodac a ECRIS-TCN, správci ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679 nebo čl. 3 bodu 8 směrnice (EU) 2016/680, pokud jde o údaje uvedené v článku 18 tohoto nařízení, které zadávají do základních systémů, a odpovídají za zpracování těchto osobních údajů v CIR.
3. V souvislosti se zpracováním údajů v MID:
 - a) Evropská agentura pro pohraniční a pobřežní stráž je správcem údajů ve smyslu s čl. 3 bodu 8 nařízení (ES) 2018/1725 ve vztahu ke zpracování osobních údajů ústřední jednotkou ETIAS;
 - b) orgány členského státu, které doplňují nebo mění údaje v souboru údajů souvisejících s potvrzením totožnosti, jsou správci ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679 nebo čl. 3 bodu 8 směrnice (EU) 2016/680 a odpovídají za zpracování osobních údajů v MID.

4. Pro účely dohledu nad ochranou údajů, včetně kontroly přípustnosti vyhledávání a zákonnosti zpracování údajů, mají správci údajů přístup k protokolům uvedeným v člancích 10, 16, 24 a 36 za účelem vlastní kontroly podle článku 44.

Článek 41

Zpracovatel údajů

V souvislosti se zpracováním osobních údajů ve sdílené BMS, v CIR a MID je zpracovatelem údajů ve smyslu čl. 3 bodu 12 písm. a) nařízení (EU) 2018/1725 agentura eu-LISA.

Článek 42

Bezpečnost zpracování

1. Agentura eu-LISA, ústřední jednotka ETIAS, Europol a orgány členských států zajistí bezpečnost zpracování osobních údajů, k němuž dochází v souladu s tímto nařízením. Spolupracují rovněž na úkolech týkajících se bezpečnosti údajů.
2. Aniž je dotčen článek 33 nařízení (EU) 2018/1725, přijme agentura eu-LISA nezbytná opatření k zajištění bezpečnosti složek interoperability a jejich související komunikační infrastruktury.
3. Agentura eu-LISA zejména přijme nezbytná opatření, včetně bezpečnostního plánu, plánu kontinuity provozu a plánu pro obnovení provozu po havárii, aby:
 - a) údaje fyzicky chránila, mimo jiné vypracováním plánů pro mimořádné situace pro ochranu kritické infrastruktury;
 - b) zabránila neoprávněným osobám v přístupu k zařízení a instalacím pro zpracování údajů;
 - c) zabránila neoprávněnému čtení, kopírování, změnám či odstranění nosičů dat;
 - d) zabránila neoprávněnému vkládání údajů a neoprávněnému prohlížení, pozměňování nebo vymazávání zaznamenaných osobních údajů;
 - e) zabránila neoprávněnému zpracovávání údajů a jakémukoli neoprávněnému kopírování, změnám nebo vymazávání údajů;
 - f) zabránila neoprávněným osobám využívajícím zařízení pro přenos údajů v použití automatizovaných systémů zpracování údajů;
 - g) zajistila, aby osoby oprávněné k přístupu ke složkám interoperability měly přístup pouze k údajům, na které se vztahuje jejich oprávnění k přístupu, a pouze na základě jedinečných totožností uživatelů a chráněných režimů přístupu k informacím;
 - h) zajistila, aby bylo možné ověřit a zjistit, kterým subjektům se mohou osobní údaje předávat prostřednictvím zařízení pro přenos údajů;
 - i) zajistila, aby bylo možné ověřit a zjistit, které údaje byly zpracovány složkami interoperability, kdy, kým a pro jaký účel;
 - j) zabránila neoprávněnému čtení, kopírování, změnám nebo vymazávání osobních údajů během jejich přenosu do složek interoperability a z nich nebo během přepravy nosičů dat, zejména pomocí vhodných technik šifrování;
 - k) zajistila, aby v případě přerušení bylo možné obnovit běžný provoz nainstalovaných systémů;
 - l) zajistila spolehlivost tým, že zaručí, aby veškeré závady fungování složek interoperability byly řádně nahlášeny;
 - m) sledovala účinnost bezpečnostních opatření uvedených v tomto odstavci a přijala nezbytná organizační opatření související s interním sledováním pro zajištění dodržování tohoto nařízení a vyhodnocení bezpečnostních opatření s ohledem na nový technický vývoj.
4. Členské státy, Europol a ústřední jednotka ETIAS přijmou bezpečnostní opatření rovnocenná opatřením uvedeným v odstavci 3, pokud jde o zpracování osobních údajů orgány s oprávněným přístupem k jakýmkoli složkám interoperability.

Článek 43

Bezpečnostní incidenty

1. Každá událost, která má nebo může mít dopad na zabezpečení složek interoperability a může poškodit údaje v nich uchovávané nebo způsobit jejich ztrátu, je považována za bezpečnostní incident, zejména v případě, kdy mohlo dojít k neoprávněnému přístupu k údajům nebo pokud byla či mohla být ohrožena dostupnost, integrita a důvěrnost údajů.

2. Bezpečnostní incidenty musí být řešeny tak, aby byla zajištěna rychlá, účinná a náležitá odezva.

3. Aniž je dotčeno ohlašování a oznamování případů porušení zabezpečení osobních údajů podle článku 33 nařízení (EU) 2016/679 nebo článku 30 směrnice (EU) 2016/680 či podle obou ustanovení, ohlásí členské státy veškeré bezpečnostní incidenty neprodleně Komisi, agentuře eu-LISA, příslušným dozorovým úřadům a evropskému inspektorovi ochrany údajů.

Aniž jsou dotčeny články 34 a 35 nařízení (EU) 2018/1725 a článek 34 nařízení (EU) 2016/794, ohlásí ústřední jednotka ETIAS a Europol jakékoli bezpečnostní incidenty neprodleně Komisi, agentuře eu-LISA a evropskému inspektorovi ochrany údajů.

Jakékoli bezpečnostní incidenty v souvislosti s centrální infrastrukturou složek interoperability ohlásí agentura eu-LISA neprodleně Komisi a evropskému inspektorovi ochrany údajů.

4. Informace o bezpečnostním incidentu, který má nebo může mít dopad na provoz složek interoperability nebo na dostupnost, integritu a důvěrnost údajů, se neprodleně poskytnou členským státům, ústřední jednotce ETIAS a Europolu a nahlásí v souladu s plánem pro řešení incidentů poskytnutým agenturou eu-LISA.

5. V případě bezpečnostního incidentu dotyčné členské státy, ústřední jednotka ETIAS, Europol a agentura eu-LISA spolupracují. Komise stanoví parametry tohoto procesu spolupráce prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 70 odst. 2.

Článek 44

Vlastní kontrola

Členské státy a příslušné agentury Unie zajistí, aby každý orgán, který má právo na přístup ke složkám interoperability, přijal opatření nezbytná pro monitorování dodržování tohoto nařízení a v případě potřeby spolupracoval s dozorovým úřadem.

Správci údajů uvedení v článku 40 přijmou nezbytná opatření pro monitorování zpracování údajů v souladu s tímto nařízením, včetně časté kontroly protokolů uvedených v článcích 10, 16, 24 a 36, a spolupracují podle potřeby s dozorovými úřady a s evropským inspektorem ochrany údajů.

Článek 45

Sankce

Členské státy zajistí, aby jakékoli zneužití údajů či jakékoli zpracování údajů nebo jejich výměna v rozporu s tímto nařízením byly trestné podle vnitrostátního práva. Stanovené sankce musí být účinné, přiměřené a odrazující.

Článek 46

Odpovědnost

1. Aniž je dotčeno právo na náhradu újmy správcem nebo zpracovatelem a jejich odpovědnost podle nařízení (EU) 2016/679, směrnice (EU) 2016/680 a nařízení (EU) 2018/1725:

a) každá osoba nebo členský stát, jimž vznikla majetková či nemajetková újma v důsledku nezákonného zpracování osobních údajů nebo jiného činu některého členského státu neslučitelného s tímto nařízením, má nárok na náhradu vzniklé újmy od tohoto členského státu;

- b) každá osoba nebo členský stát, jimž vznikla majetková či nemajetková újma v důsledku jakéhokoli činu Europolu, Evropské agentury pro pohraniční a pobřežní stráž nebo agentury eu-LISA neslučitelného s tímto nařízením, má nárok na náhradu vzniklé újmy od dotčené agentury.

Dotčený členský stát, Europol nebo Evropská agentura pro pohraniční a pobřežní stráž jsou zcela nebo zčásti zproštěny odpovědnosti podle prvního pododstavce, pokud prokáží, že nenesou odpovědnost za událost vedoucí ke vzniku újmy.

2. Pokud jakékoli nesplnění povinností členského státu podle tohoto nařízení způsobí složkám interoperability újmu, odpovídá za ni tento členský stát, ledaže agentura eu-LISA nebo jiný členský stát, který je vázán tímto nařízením, opomenuly přijmout přiměřená opatření k zabránění vzniku újmy nebo zmírnění jejích následků.

3. Uplatnění nároku na náhradu újmy uvedené v odstavcích 1 a 2 vůči členskému státu se řídí vnitrostátním právem žalovaného členského státu. Uplatnění nároku na náhradu újmy uvedené v odstavcích 1 a 2 vůči správci nebo agentuře eu-LISA podléhá podmínkám stanoveným ve Smlouvách.

Článek 47

Právo na informace

1. Orgán shromažďující osobní údaje, jež mají být uloženy ve sdílené BMS, v CIR nebo v MID, poskytne osobám, jejich údaje byly shromážděny, informace požadované podle článků 13 a 14 nařízení (EU) 2016/679, článků 12 a 13 směrnice (EU) 2016/680 a článků 15 a 16 nařízení (EU) 2018/1725. Učiní tak v době, kdy jsou tyto údaje shromažďovány.

2. Veškeré informace se zpřístupní s použitím jasných a jednoduchých formulací v jazykové verzi, které dotčená osoba rozumí nebo lze důvodně předpokládat, že jí rozumí. To zahrnuje poskytnutí informací způsobem, který je přiměřený věku nezletilých subjektů údajů.

3. Na osobní údaje zaznamenané v ECRIS-TCN a zpracovávané pro účely tohoto nařízení se vztahují pravidla týkající se práva na informace obsažená v příslušných pravidlech Unie pro ochranu údajů.

Článek 48

Právo na přístup k osobním údajům uloženým v MID, na jejich opravu a výmaz a na omezení jejich zpracování

1. Za účelem výkonu svých práv podle článků 15 až 18 nařízení (EU) 2016/679, článků 17 až 20 nařízení (EU) 2018/1725 a článků 14, 15 a 16 směrnice (EU) 2016/680 má každá osoba právo obrátit se na příslušný orgán členského státu, který žádost prověří a odpoví na ni.

2. Členský stát, který žádost prověřuje, na ni odpoví bez zbytečného prodlení, v každém případě do 45 dnů od obdržení žádosti. Tuto lhůtu lze v případě potřeby prodloužit o dalších 15 dní s ohledem na složitost a počet žádostí. Členský stát, který žádost prověřuje, informuje subjekt údajů o každém takovém prodloužení a o důvodech pro ně do 45 dnů od obdržení žádosti. Členské státy mohou rozhodnout, že tyto odpovědi mají poskytovat ústřední úřady.

3. Pokud je žádost o opravu nebo výmaz osobních údajů podána jinému členskému státu, než je členský stát odpovědný za manuální ověření různých totožností, obrátí se členský stát, kterému byla žádost podána, na orgány členského státu odpovědného za manuální ověření různých totožností do sedmi dnů. Členský stát odpovědný za manuální ověření různých totožností zkontroluje přesnost údajů a zákonnost zpracování údajů bez zbytečného odkladu a v každém případě do 30 dní ode dne, kdy se na něj jiný členský stát obrátil. Tuto lhůtu lze v případě potřeby prodloužit o dalších 15 dní s ohledem na složitost a počet žádostí. Členský stát odpovědný za manuální ověření různých totožností uvědomí členský stát, který se na něj obrátil, o každém takovém prodloužení a o důvodech pro ně. Členský stát, který se obrátí na orgán členského státu odpovědného za manuální ověření různých totožností, informuje dotčenou osobu o dalším postupu.

4. Pokud je žádost o opravu nebo výmaz osobních údajů podána členskému státu, kde byla za manuální ověření různých totožností odpovědná ústřední jednotka ETIAS, obrátí se členský stát, jemuž byla žádost podána, do sedmi dnů na ústřední jednotku ETIAS s žádostí o stanovisko. Ústřední jednotka ETIAS vydá své stanovisko bez zbytečného odkladu a v každém případě do 30 dnů ode dne, kdy se na ni členský stát obrátil. Tuto lhůtu lze v případě potřeby prodloužit o dalších 15 dnů s ohledem na složitost a počet žádostí. Členský stát, který se na ústřední jednotku ETIAS obrátil, informuje dotčenou osobu o dalším postupu.
5. Pokud je po prověření zjištěno, že údaje uložené v MID jsou nepřesné nebo že byly zaznamenány nezákonně, členský stát odpovědný za manuální ověření různých totožností nebo, pokud za manuální ověření různých totožností nebyl odpovědný žádný členský stát či za ně byla odpovědná ústřední jednotka ETIAS, členský stát, kterému byla žádost podána, tyto údaje bez zbytečného odkladu opraví nebo vymaže. Dotčená osoba je o tom, že její údaje byly opraveny nebo vymazány, informována písemně.
6. Pokud jsou údaje uložené v MID členským státem během doby jejich uchovávání pozměněny, provede tento členský stát zpracování stanovené v článku 27 a tam, kde je to relevantní, v článku 29, aby se určilo, zda se pozměněné údaje mají propojit. Pokud zpracování nevykáže žádnou shodu, vymaže tento členský stát údaje ze souboru údajů souvisejících s potvrzením totožnosti. Pokud automatizované zpracování vykáže jednu či více shod, vytvoří tento členský stát odpovídající propojení nebo je aktualizuje v souladu s příslušnými ustanoveními tohoto nařízení.
7. Pokud se členský stát odpovědný za manuální ověření různých totožností nebo případně členský stát, kterému byla žádost podána, domnívá, že údaje uložené v MID nejsou přesné, ani nebyly zaznamenány nezákonně, neprodleně přijme správní rozhodnutí a písemně vyrozumí dotčenou osobu, proč není ochoten opravit nebo vymazat údaje, které se jí týkají.
8. V rozhodnutí uvedeném v odstavci 7 se dotčené osobě poskytnou rovněž informace o tom, že má možnost napadnout rozhodnutí přijaté ve vztahu k žádosti o přístup k osobním údajům, jejich opravu či výmaz nebo omezení jejich zpracování, a případně informace o tom, jakým způsobem podat žalobu nebo stížnost u příslušných orgánů nebo soudů a o veškeré pomoci, kterou má k dispozici, včetně pomoci od dozorových úřadů.
9. Každá žádost o přístup k osobním údajům, jejich opravu či výmaz nebo omezení jejich zpracování musí obsahovat nezbytné informace pro zjištění totožnosti dotčené osoby. Tyto informace se použijí výhradně k umožnění výkonu práv uvedených v tomto článku a ihned poté se vymažou.
10. Členský stát odpovědný za manuální ověření různých totožností nebo případně členský stát, kterému byla žádost podána, uchová písemný záznam o podání žádosti o přístup k osobním údajům, jejich opravu či výmaz nebo omezení jejich zpracování a způsobu, jakým byla vyřešena, a neprodleně tento záznam zpřístupní dozorovým úřadům.
11. Tímto článkem nejsou dotčena omezení práv uvedených v tomto článku podle nařízení (EU) 2016/679 a směrnice (EU) 2016/680.

Článek 49

Internetový portál

1. Zřizuje se internetový portál pro usnadnění výkonu práv na přístup k osobním údajům, jejich opravu či výmaz nebo omezení jejich zpracování.
2. Internetový portál obsahuje informace o právech a postupech uvedených v člácích 47 a 48 a uživatelské rozhraní, jehož prostřednictvím mohou osoby, jejichž údaje jsou zpracovávány v MID a které byly informovány o výskytu červeného propojení v souladu s čl. 32 odst. 4, obdržet kontaktní údaje příslušného orgánu členského státu odpovědného za manuální ověření různých totožností.
3. Pro získání kontaktních údajů příslušného orgánu členského státu odpovědného za manuální ověření různých totožností by měla osoba, jejíž údaje jsou zpracovávány v MID, zadat odkaz na orgán odpovědný za manuální ověření různých totožností uvedený v čl. 34 písm. d). Internetový portál pomocí tohoto odkazu získá kontaktní údaje příslušného orgánu členského státu odpovědného za manuální ověření různých totožností. Internetový portál rovněž obsahuje šablonu e-mailu pro usnadnění komunikace mezi uživatelem portálu a příslušným orgánem členského státu odpovědného za manuální ověření různých totožností. Tento e-mail obsahuje pole pro jediné identifikační číslo uvedené v čl. 34 písm. c), které příslušnému orgánu členského státu odpovědného za manuální ověření různých totožností umožní určit údaje, o které se jedná.

4. Členské státy poskytnou agentuře eu-LISA kontaktní údaje všech orgánů příslušných k prověřování a zodpovídání žádostí uvedených v článcích 47 a 48 a pravidelně ověřují, zda jsou aktuální.
5. Internetový portál vyvine a jeho technickou správu zajišťuje agentura eu-LISA.
6. Komise přijme akt v přenesené pravomoci v souladu s článkem 69, které stanoví podrobná pravidla fungování internetového portálu, včetně uživatelského rozhraní, jazyků, v nichž je internetový portál k dispozici, a šablony e-mailu.

Článek 50

Předávání osobních údajů třetím zemím, mezinárodním organizacím a soukromým subjektům

Aniž jsou dotčeny článek 31 nařízení (ES) č. 767/2008, články 25 a 26 nařízení (EU) 2016/794, článek 41 nařízení (EU) 2017/2226, článek 65 nařízení (EU) 2018/1240 a vyhledávání v databázích Interpolu prostřednictvím ESP v souladu s čl. 9 odst. 5 tohoto nařízení, které dodržují kapitolu V nařízení (EU) 2018/1725 a kapitolu V nařízení (EU) 2016/679, nesmějí být osobní údaje uloženy ve složkách interoperability nebo jimi zpracovávány nebo přístupné jejich prostřednictvím předány ani zpřístupněny žádné třetí zemi, mezinárodní organizaci ani soukromému subjektu.

Článek 51

Dohled dozorových úřadů

1. Každý členský stát zajistí, aby dozorové úřady nezávisle dohlížely na zákonnost zpracovávání osobních údajů podle tohoto nařízení dotčeným členským státem, včetně jejich přenosu do složek interoperability a ze složek operability.
2. Každý členský stát zajistí, aby byly vnitrostátní právní a správní předpisy přijaté podle směrnice (EU) 2016/680 použitelné, je-li to relevantní, také na přístup jeho policejních orgánů a určených orgánů do složek interoperability, a to i ve vztahu k právům osob, k jejichž údajům je takto umožněn přístup.
3. Dozorové úřady zajistí, aby byl alespoň jednou za čtyři roky v souladu s příslušnými mezinárodními auditorskými standardy proveden audit operací zpracování osobních údajů příslušnými vnitrostátními orgány pro účely tohoto nařízení.

Dozorové úřady každoročně zveřejní informace o počtu žádostí o opravu či výmaz osobních údajů nebo omezení jejich zpracovávání, následně přijatých opatřeních a o počtu oprav či výmaz osobních údajů nebo omezení jejich zpracovávání provedených v reakci na žádosti dotčených osob.

4. Členské státy zajistí, aby jejich dozorové úřady měly dostatek zdrojů a odborných znalostí k plnění úkolů, které jim toto nařízení ukládá.
5. Členské státy poskytnou veškeré informace, které si vyžádá dozorový úřad uvedený v čl. 51 odst. 1 nařízení (EU) 2016/679, a zejména mu poskytnou informace o činnostech prováděných v souladu s jejich povinnostmi podle tohoto nařízení. Členské státy poskytnou dozorovým úřadům uvedeným v čl. 51 odst. 1 nařízení (EU) 2016/679 přístup ke svým protokolům uvedeným v článcích 10, 16, 24 a 36 tohoto nařízení a k odůvodněním uvedeným v čl. 22 odst. 2 tohoto nařízení a umožní jim kdykoli přístup do všech svých prostor využívaných pro účely interoperability.

Článek 52

Audity prováděné evropským inspektorem ochrany údajů

Evropský inspektor ochrany údajů zajistí, aby byl alespoň jednou za čtyři roky v souladu s příslušnými mezinárodními auditorskými standardy proveden audit operací zpracování osobních údajů agenturou eu-LISA, ústřední jednotkou ETIAS a Europol pro účely tohoto nařízení. Zpráva o tomto auditu se zasílá Evropskému parlamentu, Radě, agentuře eu-LISA, Komisi, členským státům a dotčené agentuře Komise. Agentura eu-LISA, ústřední jednotka ETIAS a Europol mají možnost se ke zprávám před jejich přijetím vyjádřit.

Agentura eu-LISA, ústřední jednotka ETIAS a Europol poskytují evropskému inspektorovi ochrany údajů informace, o které požádá, udělují mu přístup ke všem dokumentům, o které požádá, a ke svým protokolům podle článků 10, 16, 24 a 36 a umožňují mu nepřetržitý přístup do všech svých prostor.

Článek 53

Spolupráce dozorových úřadů s evropským inspektorem ochrany údajů

1. Dozorové úřady a evropský inspektor ochrany údajů, každý v rozsahu svých pravomocí, aktivně spolupracují v rámci svých povinností a zajišťují koordinovaný dohled nad používáním složek interoperability a uplatňováním dalších ustanovení tohoto nařízení, zejména pokud evropský inspektor ochrany údajů nebo dozorový úřad zjistí značné nesrovnalosti mezi postupy členských států nebo potenciálně nezákonné předávání údajů komunikačními kanály složek interoperability.
2. V případech uvedených v odstavci 1 tohoto článku se zajistí koordinovaný dozor v souladu s článkem 62 nařízení (EU) 2018/1725.
3. Evropský sbor pro ochranu osobních údajů zašle Evropskému parlamentu, Radě, Komisi, Europolu, Evropské agentuře pro pohraniční a pobřežní stráž a agentuře eu-LISA do 12. června 2021 a poté každé dva roky společnou zprávu o svých činnostech podle tohoto článku. V uvedené zprávě je každému členskému státu věnována jedna kapitola, kterou vypracuje dozorový úřad daného členského státu.

KAPITOLA VIII**Povinnosti**

Článek 54

Povinnosti agentury eu-LISA během fáze návrhu a vývoje

1. Agentura eu-LISA zajistí, aby centrální infrastruktury složek interoperability byly provozovány v souladu s tímto nařízením.
2. Složky interoperability jsou provozovány v technických prostorách agentury eu-LISA a zajišťují funkce stanovené tímto nařízením v souladu s podmínkami bezpečnosti, dostupnosti, kvality a výkonu uvedenými v čl. 55 odst. 1.
3. Agentura eu-LISA odpovídá za vývoj složek interoperability a za veškeré změny nezbytné k zajištění interoperability mezi centrálními systémy EES, VIS, ETIAS, SIS, Eurodacu, ECRIS-TCN a ESP, sdílenou BMS, CIR, MID a CRRS.

Aniž je dotčen článek 62, nemá agentura eu-LISA přístup k osobním údajům zpracovávaným prostřednictvím ESP, sdílené BMS, CIR a MID.

Agentura eu-LISA navrhne fyzickou architekturu složek interoperability, včetně jejich komunikačních infrastruktur, jakož i technické specifikace a jejich vývoj s ohledem na centrální infrastrukturu a zabezpečenou komunikační infrastrukturu, které přijme správní rada po obdržení kladného stanoviska Komise. Agentura eu-LISA rovněž provede veškeré nezbytné úpravy SIS, Eurodacu nebo ECRIS-TCN vyplývající z vytvoření interoperability a stanovené tímto nařízením.

Agentura eu-LISA vyvine a realizuje složky interoperability co nejdříve po vstupu tohoto nařízení v platnost a poté, co Komise přijme opatření stanovená v čl. 8 odst. 2, čl. 9 odst. 7, čl. 28 odst. 5 a 7, čl. 37 odst. 4, čl. 38 odst. 3, čl. 39 odst. 5, čl. 43 odst. 5 a čl. 74 odst. 10.

Vývoj sestává z vypracování a realizace technických specifikací, testování a celkové projektové správy a koordinace.

4. Během fáze návrhu a vývoje se ustaví rada pro řízení programu složená nejvýše z 10 členů. Skládá se ze sedmi členů jmenovaných správní radou agentury eu-LISA, vybraných z jejich členů nebo náhradníků, dále z předsedy Poradní skupiny pro interoperabilitu uvedené v článku 71, z jednoho člena zastupujícího agenturu eu-LISA jmenovaného jejím výkonným ředitelem a z jednoho člena jmenovaného Komisí. Členové jmenovaní správní radou agentury eu-LISA jsou voleni pouze z těch členských států, které jsou podle práva Unie v plné míře vázány právními nástroji upravujícími vývoj, zřizování, provoz a používání všech informačních systémů EU a které budou zapojeny do složek interoperability.

5. Rada pro řízení programu se schází pravidelně a nejméně třikrát za čtvrtletí. Zajistí přiměřené řízení fáze návrhu a vývoje složek interoperability.

Rada pro řízení programu předkládá správní radě agentury eu-LISA každý měsíc písemné zprávy o pokroku projektu. Nemá rozhodovací pravomoc ani není zmocněna zastupovat členy správní rady agentury eu-LISA.

6. Správní rada agentury eu-LISA stanoví jednací řád rady pro řízení programu, který zahrnuje zejména pravidla pro:
- a) předsednictví;
 - b) místa zasedání;
 - c) přípravu jednání;
 - d) přizvání odborníků na zasedání;
 - e) komunikační plány zajišťující plné informování nezúčastněných členů správní rady.

Radě předsedá některý z členských států, který je podle práva Unie v plné míře vázán právními nástroji upravujícími vývoj, zřizování, provoz a používání všech informačních systémů EU a který bude zapojen do složek interoperability.

Všechny cestovní výdaje a výdaje na pobyt členů rady pro řízení programu hradí agentura eu-LISA a článek 10 jednacího řádu agentury eu-LISA se použije obdobně. Sekretariát rady pro řízení programu zajišťuje agentura eu-LISA.

Poradní skupina pro interoperabilitu uvedená v článku 71 se schází pravidelně až do zahájení provozu složek interoperability. Po každé schůzi podává zprávu radě pro řízení programu. Zajišťuje odborné znalosti pro podporu úkolů rady pro řízení programu a podniká kroky v návaznosti na stav připravenosti členských států.

Článek 55

Povinnosti agentury eu-LISA po zahájení provozu

1. Po zahájení provozu každé ze složek interoperability odpovídá agentura eu-LISA za technickou správu centrální infrastruktury složek interoperability, včetně jejich údržby a technického vývoje. Ve spolupráci s členskými státy zajišťuje, aby byla používána nejlepší dostupná technologie určená na základě analýzy nákladů a přínosů. Agentura eu-LISA rovněž odpovídá za technickou správu komunikační infrastruktury uvedené v článcích 6, 12, 17, 25 a 39.

Technická správa složek interoperability sestává ze všech úkolů a technických řešení nezbytných pro zachování funkčnosti složek interoperability a poskytování nepřetržité služby členským státům a agenturám Unie 24 hodin denně sedm dní v týdnu v souladu s tímto nařízením. To zahrnuje údržbu a technický rozvoj nezbytný k tomu, aby složky fungovaly na uspokojivé úrovni technické kvality, zejména co se týče doby odezvy na dotazování v centrálních databázích v souladu s technickými specifikacemi.

Všechny složky interoperability musí být vytvořeny a spravovány tak, aby zajišťovaly rychlý, bezproblémový, účinný a řízený přístup, plnou, nepřetržitou dostupnost složek a údajů uložených v MID, sdílené BMS a CIR a takovou dobu odezvy, která odpovídá provozním potřebám orgánů členských států a agentur Unie.

2. Aniž je dotčen článek 17 služebního řádu úředníků Evropské unie, použije agentura eu-LISA na své pracovníky, u nichž je vyžadováno, aby pracovali s údaji uloženými ve složkách interoperability, vhodná pravidla zachování služebního tajemství nebo jiné srovnatelné povinnosti zachování důvěrnosti. Tato povinnost platí i poté, co dotyčné osoby opustí svou funkci nebo zaměstnanecký poměr, nebo poté, co ukončí svou činnost.

Aniž je dotčen článek 62, nemá agentura eu-LISA přístup k osobním údajům zpracovávaným prostřednictvím ESP, sdílené BMS, CIR a MID.

3. Agentura eu-LISA vyvine a spravuje mechanismus a postupy pro provádění kontrol kvality údajů uložených ve sdílené BMS a CIR v souladu s článkem 37.

4. Agentura eu-LISA plní rovněž úkoly související s odbornou přípravou zaměřenou na technické aspekty používání složek interoperability.

Článek 56

Povinnosti členských států

1. Každý členský stát zajistí:
 - a) připojení ke komunikační infrastruktuře ESP a CIR;
 - b) začlenění stávajících vnitrostátních systémů a infrastruktur do ESP, CIR a MID;
 - c) organizaci, správu, provoz a údržbu své stávající vnitrostátní infrastruktury a jejího propojení se složkami interoperability;
 - d) správu a úpravu přístupu pro řádně zmocněné pracovníky příslušných vnitrostátních orgánů do ESP, CIR a MID v souladu s tímto nařízením a vypracování a pravidelnou aktualizaci seznamu těchto pracovníků a jejich profilů;
 - e) přijetí legislativních opatření uvedených v čl. 20 odst. 5 a 6, aby byl zajištěn přístup do CIR pro účely zjištění totožnosti;
 - f) manuální ověření různých totožností uvedené v článku 29;
 - g) soulad s požadavky na kvalitu údajů stanovenými na základě práva Unie;
 - h) dodržování pravidel jednotlivých informačních systémů EU pro zajištění bezpečnosti a integrity osobních údajů;
 - i) nápravu veškerých nedostatků zjištěných v hodnotící zprávě Komise o kvalitě údajů uvedené v čl. 37 odst. 5.
2. Každý členský stát propojí své určené orgány s CIR.

Článek 57

Povinnosti Europolu

1. Europol zajistí zpracování vyhledávání v údajích Europolu prostřednictvím ESP a odpovídajícím způsobem upraví rozhraní pro údaje základního stupně ochrany (BPL) svých vyhledávacích systémů (Querying Europol Systems, QUEST).
2. Europol odpovídá za řízení a opatření týkající se jeho řádně zmocněných pracovníků, aby podle tohoto nařízení mohli využívat ESP a CIR a měli k nim přístup, a za vypracování a pravidelnou aktualizaci seznamu těchto pracovníků a jejich profilů.

Článek 58

Povinnosti ústřední jednotky ETIAS

Ústřední jednotka ETIAS zajistí:

- a) manuální ověření různých totožností v souladu s článkem 29;
- b) odhalování vícenásobných totožností mezi údaji uloženými v systému EES, VIS, Eurodac a SIS uvedené v článku 65.

KAPITOLA IX**Změny jiných nástrojů Unie**

Článek 59

Změny nařízení (EU) 2018/1726

Nařízení (EU) 2018/1726 se mění takto:

- 1) Článek 12 se nahrazuje tímto:

„Článek 12

Kvalita údajů

1. Aniž jsou dotčeny povinnosti členských států v souvislosti s údaji zadávanými do systémů, za jejichž provoz agentura odpovídá, zavede agentura za intenzivní účasti svých poradních skupin automatizované mechanismy a postupy pro kontrolu kvality údajů a společné ukazatele kvality údajů a minimální normy kvality pro uchovávání údajů pro všechny systémy, za jejichž provoz odpovídá, v souladu s příslušnými ustanoveními právních nástrojů upravujících tyto informační systémy a článkem 37 nařízení Evropského parlamentu a Rady (EU) 2019/817 (*) a (EU) 2019/818 (**).

2. Agentura zřídí centrální úložiště obsahující pouze anonymizované údaje pro podávání zpráv a statistiky v souladu s článkem 39 nařízení (EU) 2019/817 a (EU) 2019/818, s výhradou zvláštních ustanovení právních nástrojů upravujících vývoj, zřízení, provoz a používání rozsáhlých informačních systémů řízených agenturou.

(*) Nařízení Evropského parlamentu a Rady (EU) 2019/817 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti hranic a víz a mění nařízení Evropského parlamentu a Rady (ES) č. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 a (EU) 2018/1861 a rozhodnutí Rady 2004/512/ES a 2008/633/SVV (Úř. věst. L 135, 22.5.2019, s. 27).

(**) Nařízení Evropského parlamentu a Rady (EU) 2019/818 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti policejní a justiční spolupráce, azylu a migrace a kterým se mění nařízení (EU) 2018/1726, (EU) 2018/1862 a (EU) 2019/816 (Úř. věst. L 135, 22.5.2019, s. 85).“

2) V článku 19 se odstavec 1 se mění takto:

a) vkládá se nové písmeno, které zní:

„eea) přijímá zprávy o aktuálním stavu vývoje složek interoperability podle čl. 78 odst. 2 nařízení (EU) 2019/817 a čl. 74 odst. 2 nařízení (EU) 2019/818;“

b) písmeno ff) se nahrazuje tímto:

„ff) přijímá zprávy o technickém fungování SIS podle čl. 60 odst. 7 nařízení Evropského parlamentu a Rady (EU) 2018/1861 (*) a čl. 74 odst. 8 nařízení Evropského parlamentu a Rady (EU) 2018/1862 (**), o technickém fungování VIS podle čl. 50 odst. 3 nařízení (ES) č. 767/2008 a čl. 17 odst. 3 rozhodnutí 2008/633/SVV, o technickém fungování EES podle čl. 72 odst. 4 nařízení (EU) 2017/2226, o technickém fungování ETIAS podle čl. 92 odst. 4 nařízení (EU) 2018/1240, o technickém fungování ECRIS-TCN a referenčního provedení ECRIS podle čl. 36 odst. 8 nařízení Evropského parlamentu a Rady (EU) 2019/816 (***) a o technickém fungování složek interoperability podle čl. 78 odst. 3 nařízení (EU) 2019/817 a čl. 74 odst. 3 nařízení (EU) 2019/818;

(*) Nařízení Evropského parlamentu a Rady (EU) 2018/1861 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol, o změně Úmluvy k provedení Schengenské dohody a o změně a zrušení nařízení (ES) č. 1987/2006 (Úř. věst. L 312, 7.12.2018, s. 14).

(**) Nařízení Evropského parlamentu a Rady (EU) 2018/1862 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, o změně a o zrušení rozhodnutí Rady 2007/533/SVV a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 a rozhodnutí Komise 2010/261/EU (Úř. věst. L 312, 7.12.2018, s. 56).

(***) Nařízení Evropského parlamentu a Rady (EU) 2019/816 ze dne 17. dubna 2019, kterým se zřizuje centralizovaný systém pro identifikaci členských států, jež mají informace o odsouzeních státních příslušníků třetích zemí a osob bez státní příslušnosti (ECRIS-TCN), na doplnění Evropského informačního systému rejstříků trestů a kterým se mění nařízení (EU) 2018/1726 (Úř. věst. L 135, 22.5.2019, s. 1).“;

c) písmeno hh) se nahrazuje tímto:

„hh) přijímá formální připomínky ke zprávám evropského inspektora ochrany údajů o auditech podle čl. 56 odst. 2 nařízení (EU) 2018/1861, čl. 42 odst. 2 nařízení (ES) č. 767/2008, čl. 31 odst. 2 nařízení (EU) č. 603/2013, čl. 56 odst. 2 nařízení (EU) 2017/2226, článku 67 nařízení (EU) 2018/1240, čl. 29 odst. 2 nařízení (EU) 2019/816 a článku 52 nařízení (EU) 2019/817 a (EU) 2019/818 a zajišťuje patřičná opatření v návaznosti na tyto audity;“

d) písmeno mm) se nahrazuje tímto:

„mm) zajišťuje každoroční zveřejnění seznamu příslušných orgánů, které jsou oprávněny přímo vyhledávat v údajích obsažených v SIS podle čl. 41 odst. 8 nařízení (EU) 2018/1861 a čl. 56 odst. 7 nařízení (EU) 2018/1862, spolu se seznamem úřadů vnitrostátních systémů SIS (N.SIS) a centrální SIRENE podle čl. 7 odst. 3 nařízení (EU) 2018/1861 a čl. 7 odst. 3 nařízení (EU) 2018/1862, seznamem příslušných orgánů podle čl. 65 odst. 2 nařízení (EU) 2017/2226, seznamem příslušných orgánů podle čl. 87 odst. 2 nařízení (EU) 2018/1240, seznamem ústředních orgánů podle čl. 34 odst. 2 nařízení (EU) 2019/816 a seznamem orgánů podle čl. 71 odst. 1 nařízení (EU) 2019/817 a čl. 67 odst. 1 nařízení (EU) 2019/818.“

3) V článku 22 se odstavce 4 nahrazuje tímto:

„4. Europol a Eurojust se mohou účastnit zasedání správní rady jako pozorovatelé, jsou-li na pořadu jednání otázky týkající se SIS II v souvislosti s uplatňováním rozhodnutí 2007/533/SVV.

Evropská agentura pro pohraniční a pobřežní stráž se může účastnit zasedání správní rady jako pozorovatelka, jsou-li na pořadu jednání otázky týkající se SIS v souvislosti s uplatňováním nařízení (EU) 2016/1624.

Europol se může účastnit zasedání správní rady jako pozorovatel, jsou-li na pořadu jednání otázky týkající se VIS v souvislosti s uplatňováním rozhodnutí 2008/633/SVV nebo otázky týkající se Eurodacu v souvislosti s uplatňováním nařízení (EU) č. 603/2013.

Europol se může účastnit zasedání správní rady jako pozorovatel, jsou-li na pořadu jednání otázky týkající se EES v souvislosti s uplatňováním nařízení (EU) 2017/2226 nebo otázky týkající se ETIAS související s nařízením (EU) 2018/1240.

Evropská agentura pro pohraniční a pobřežní stráž se může účastnit zasedání správní rady jako pozorovatelka, jsou-li na pořadu jednání otázky týkající se ETIAS v souvislosti s uplatňováním nařízení (EU) 2018/1240.

Eurojust, Europol a Úřad evropského veřejného žalobce se mohou účastnit zasedání správní rady jako pozorovatelé, jsou-li na pořadu jednání otázky týkající se nařízení (EU) 2019/816.

Europol, Eurojust a Evropská agentura pro pohraniční a pobřežní stráž se mohou účastnit zasedání správní rady jako pozorovatelé, jsou-li na pořadu jednání otázky týkající se nařízení (EU) 2019/817 a (EU) 2019/818.

Správní rada může na zasedání jako pozorovatele pozvat jakoukoli další osobu, jejíž stanovisko může být předmětem zájmu.“

4) V čl. 24 odst. 3 se písmeno p) nahrazuje tímto:

„p) aniž je dotčen článek 17 služebního řádu úředníků, stanovení požadavků na zachování důvěrnosti údajů k zajištění souladu s článkem 17 nařízení (ES) č. 1987/2006, článkem 17 rozhodnutí 2007/533/SVV, čl. 26 odst. 9 nařízení (ES) č. 767/2008, čl. 4 odst. 4 nařízení (EU) č. 603/2013, čl. 37 odst. 4 nařízení (EU) 2017/2226, čl. 74 odst. 2 nařízení (EU) 2018/1240, čl. 11 odst. 16 nařízení (EU) 2019/816 a čl. 55 odst. 2 nařízení (EU) 2019/817 a (EU) 2019/818;“.

5) Článek 27 se mění takto:

a) v odstavci 1 se vkládá nové písmeno, které zní:

„da) poradní skupina pro interoperabilitu;“

b) odstavec 3 se nahrazuje tímto:

„3. Europol, Eurojust a Evropská agentura pro pohraniční a pobřežní stráž mohou každý jmenovat svého zástupce do poradní skupiny pro SIS II.

Europol může také jmenovat svého zástupce do poradních skupin pro VIS a Eurodac a EES-ETIAS.

Evropská agentura pro pohraniční a pobřežní stráž může také jmenovat svého zástupce do poradní skupiny pro EES-ETIAS.

Eurojust, Europol a Úřad evropského veřejného žalobce mohou každý jmenovat svého zástupce do poradní skupiny pro ECRIS-TCN.

Europol, Eurojust a Evropská agentura pro pohraniční a pobřežní stráž mohou každý jmenovat svého zástupce do poradní skupiny pro interoperabilitu.“

Článek 60

Změny nařízení (EU) 2018/1862

Nařízení (EU) 2018/1862 se mění takto:

1) V článku 3 se doplňují nové body, které znějí:

- „18) „ESP“ Evropský vyhledávací portál zřízený čl. 6 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2019/818 (*);
- 19) „sdílenou BMS“ sdílená služba pro porovnávání biometrických údajů zřízená čl. 12 odst. 1 nařízení (EU) 2019/818;
- 20) „CIR“ společné úložiště údajů o totožnosti zřízené čl. 17 odst. 1 nařízení (EU) 2019/818;
- 21) „MID“ detektor vícenásobné totožnosti zřízený čl. 25 odst. 1 nařízení (EU) 2019/818.

(*) Nařízení Evropského parlamentu a Rady (EU) 2019/818 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti policejní a justiční spolupráce, azylu a migrace a kterým se mění nařízení (EU) 2018/1726, (EU) 2018/1862 a (EU) 2019/816. (Úř. věst. L 135, 22.5.2019, s. 85).“

2) Článek 4 se mění takto:

a) v odstavci 1 se písmena b) a c) nahrazují tímto:

- „b) vnitrostátního systému (dále jen „N.SIS“) v každém členském státě, sestávajícího z vnitrostátních datových systémů, které komunikují s centrálním SIS, včetně alespoň jednoho vnitrostátního nebo sdíleného záložního N.SIS;
- c) komunikační infrastruktury mezi CS-SIS, záložní CS-SIS a NI-SIS (dále jen „komunikační infrastruktura“), která poskytuje šifrovanou virtuální síť vyhrazenou pro údaje SIS a výměnu údajů mezi centrály SIRENE uvedenými v čl. 7 odst. 2, a
- d) zabezpečené komunikační infrastruktury mezi CS-SIS a centrálními infrastrukturami ESP, sdílené BMS a MID.“;

b) doplňují se nové odstavce, které znějí:

„8. Aniž jsou dotčeny odstavce 1 až 5, lze údaje SIS o osobách a dokladech totožnosti vyhledávat rovněž prostřednictvím ESP.

9. Aniž jsou dotčeny odstavce 1 až 5, lze údaje SIS o osobách a dokladech totožnosti předávat rovněž prostřednictvím zabezpečené komunikační infrastruktury uvedené v odst. 1 písm. d). Tato předávání se omezí na rozsah, v jakém jsou údaje nezbytné pro účely nařízení (EU) 2019/818.“

3) V článku 7 se vkládá nový odstavec, který zní:

„2a. Centrály SIRENE rovněž zajistí manuální ověření různých totožností v souladu s článkem 29 nařízení (EU) 2019/818. V rozsahu nezbytném pro plnění tohoto úkolu mají centrály SIRENE přístup k údajům uloženým v CIR a MID pro účely stanovené v člincích 21 a 26 nařízení (EU) 2019/818.“

4) V čl. 12 odst. 1 se doplňuje nový pododstavec, který zní:

„Členské státy zajistí, aby každý přístup k osobním údajům prostřednictvím ESP byl rovněž zaprotokolován za účelem kontroly, zda bylo vyhledávání zákonné, za účelem dohledu nad zákonností zpracovávání údajů, pro vlastní kontrolu a pro integritu údajů a jejich zabezpečení.“

5) V čl. 44 odst. 1 se doplňuje nové písmeno, které zní:

„f) ověření různých totožností a potírání podvodného zneužívání totožnosti v souladu s kapitolou V nařízení (EU) 2019/818.“

6) V článku 74 se odstavec 7 nahrazuje tímto:

„7. Pro účely čl. 15 odst. 4 a odstavců 3, 4 a 6 tohoto článku agentura eu-LISA ukládá údaje uvedené v čl. 15 odst. 4 a v odstavci 3 tohoto článku, které neumožňují individuální identifikaci, v centrálním úložišti pro účely podávání zpráv a statistiky uvedeném v článku 39 nařízení (EU) 2019/818.

Agentura eu-LISA umožní Komisi a subjektům uvedeným v odstavci 6 tohoto článku získat zmíněné zprávy a statistiky. Na žádost udělí členským státům, Komisi, Europolu a Evropské agentuře pro pohraniční a pobřežní stráž přístup do centrálního úložiště pro zprávy a statistiky v souladu s článkem 39 nařízení (EU) 2019/818.“

Článek 61

Změny nařízení (EU) 2019/816

Nařízení (EU) 2019/816 se mění takto:

1) V článku 1 se doplňuje nové písmeno, které zní:

„c) stanovují podmínky, za nichž ECRIS-TCN přispívá k usnadnění a podpoře správného zjištění totožnosti osob registrovaných v ECRIS-TCN za podmínek a pro účely článku 20 nařízení Evropského parlamentu a Rady (EU) 2019/818 (*) tím, že ukládá údaje o totožnosti, údaje o cestovních dokladech a biometrické údaje v CIR.

(*) Nařízení Evropského parlamentu a Rady (EU) 2019/818 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti policejní a justiční spolupráce, azylu a migrace a kterým se mění nařízení (EU) 2018/1726, (EU) 2018/1862 a (EU) 2019/816 (Úř. věst. L 135, 22.5.2019, s. 85).“

2) Článek 2 se nahrazuje tímto:

„Článek 2

Oblast působnosti

Toto nařízení se vztahuje na zpracovávání informací o totožnosti státních příslušníků třetích zemí, kteří byli odsouzeni v členských státech, za účelem zjištění členských států, v nichž byla taková odsouzení vydána. S výjimkou čl. 5 odst. 1 písm. b) bodu ii) se ustanovení tohoto nařízení, která se vztahují na státní příslušníky třetích zemí, vztahují rovněž na občany Unie, kteří jsou zároveň státními příslušníky třetí země a kteří byli odsouzeni v členských státech. Toto nařízení též usnadňuje a podporuje správné zjištění totožnosti osob v souladu s tímto nařízením a s nařízením (EU) 2019/818.“

3) Článek 3 se mění takto:

a) bod 8 se zrušuje;

b) doplňují se nové body, které zní:

„19) „CIR“ společné úložiště údajů o totožnosti zřízené čl. 17 odst. 1 nařízení (EU) 2019/818;

20) „údaji ECRIS-TCN“ všechny údaje uložené v centrálním systému a v CIR v souladu s článkem 5;

21) Evropský vyhledávací portál zřízený čl. 6 odst. 1 nařízení (EU) 2019/818;“.

4) V článku 4 se odstavec 1 mění takto:

a) písmeno a) se nahrazuje tímto:

„a) centrálního systému;“

b) vkládá se nový bod, který zní:

„aa) CIR;“

c) doplňuje se nový bod, který zní:

„e) komunikační infrastruktury mezi centrálním systémem a centrálními infrastrukturami ESP a CIR.“

5) Článek 5 se mění takto:

a) v článku 1 se návětí nahrazuje tímto:

„1. V případě každého odsouzeného státního příslušníka třetí země ústřední orgán odsuzujícího členského státu pořídí datový záznam v ECRIS-TCN. Datový záznam musí zahrnovat:“;

b) vkládá se nový odstavec, který zní:

„1a. CIR obsahuje údaje uvedené v odst. 1 písm. b) a následující údaje uvedené v odst. 1 písm. a): příjmení, jméno (jména); datum narození, místo narození (obec a země), státní příslušnost (příslušnosti), pohlaví, případné předchozí jméno (jména) nebo příjmení, pseudonymy nebo přezdívky, existují-li, a případně druh a číslo cestovního dokladu nebo dokladů dané osoby, jakož i název vydávajícího orgánu tohoto dokladu. CIR může rovněž obsahovat údaje uvedené v odstavci 3. Ostatní údaje ECRIS-TCN se uchovávají v centrálním systému.“

6) Článek 8 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. Každý datový záznam se uchovává v centrálním systému a CIR, dokud jsou údaje o odsouzeních dotyčné osoby uloženy v rejstříku trestů.“;

b) odstavec 2 se nahrazuje tímto:

„2. Po uplynutí doby uchovávání uvedené v odstavci 1 ústřední orgán odsuzujícího členského státu vymaže datový záznam z centrálního systému a CIR, včetně případných údajů o otiscích prstů nebo zobrazení obličeje. Výmaz se provádí pokud možno automaticky a v každém případě nejpozději jeden měsíc po uplynutí doby uchovávání.“

7) Článek 9 se mění takto:

a) v odstavci 1 se slova „do ECRIS-TCN“ nahrazují slovy „do centrálního systému a CIR“;

b) v odstavcích 2, 3 a 4 se slova „centrální systém“ v příslušném mluvnickém tvaru nahrazují výrazem „centrální systém a CIR“ v příslušném mluvnickém tvaru.

8) V čl. 10 odst. 1 se zrušuje písmeno j).

9) V čl. 12 odst. 2 se slova „v centrálním systému“ nahrazují slovy „v centrálním systému a CIR“.

10) V čl. 13 odst. 2 se slova „centrálního systému“ nahrazují slovy „centrálního systému a CIR“.

11) V čl. 23 odst. 2 se slova „do centrálního systému“ nahrazují slovy „do centrálního systému a CIR“.

12) Článek 24 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. Údaje vložené do centrálního systému a CIR se zpracovávají pouze za účelem identifikace členských států, jež mají informace z rejstříku trestů o státních příslušnících třetích zemí. Údaje vložené do CIR se rovněž zpracovávají v souladu s nařízením (EU) 2019/818 pro účely usnadňování a podpory správného zjištění totožnosti osob registrovaných v ECRIS-TCN v souladu s uvedeným nařízením.“;

b) doplňuje se nový odstavec, který zní:

„3. Aniž je dotčen odstavec 2, je přístup k údajům uloženým v CIR rovněž vyhrazen řádně zmocněným pracovníkům vnitrostátních orgánů každého členského státu a řádně zmocněným pracovníkům agentur Unie příslušných pro účely stanovené v článcích 20 a 21 nařízení (EU) 2019/818. Takový přístup je omezen na rozsah, ve kterém jsou tyto údaje potřebné pro plnění jejich úkolů za uvedenými účely a který je přiměřený sledovaným cílům.“

13) V článku 32 se odstavec 2 se nahrazuje tímto:

„2. Pro účely odstavce 1 tohoto článku uchovává agentura eu-LISA údaje uvedené v uvedeném odstavci v centrálním úložišti pro podávání zpráv a statistiky uvedeném v článku 39 nařízení (EU) 2019/818.“

14) V čl. 33 odst. 1 se slova „centrálního systému“ nahrazují slovy „centrálního systému, CIR“.

15) V článku 41 se odstavec 2 nahrazuje tímto:

„2. U odsouzení vydaných přede dnem zahájení vkládání údajů určeným podle čl. 35 odst. 1 pořídí ústřední orgány jednotlivé datové záznamy v centrálním systému takto:

- a) alfanumerické údaje vloží do centrálního systému a CIR do konce období uvedeného v čl. 35 odst. 2;
- b) údaje o otiscích prstů vloží do CIR do dvou let po zahájení provozu v souladu s čl. 35 odst. 4.“

KAPITOLA X

Závěrečná ustanovení

Článek 62

Podávání zpráv a statistiky

1. Výhradně pro účely podávání zpráv a statistiky mají řádně zmocnění pracovníci příslušných orgánů členských států, Komise a agentury eu-LISA přístup k těmto údajům souvisejícím s ESP: počet vyhledávání na uživatele profilu ESP.

Z těchto údajů nesmí být možné identifikovat jednotlivce.

2. Výhradně pro účely podávání zpráv a statistiky mají řádně zmocnění pracovníci příslušných orgánů členských států, Komise a agentury eu-LISA přístup k těmto údajům souvisejícím s CIR:

- a) počet vyhledávání pro účely článků 20, 21 a 22;
- b) státní příslušnost, pohlaví a rok narození osoby;
- c) druh cestovního dokladu a třípísmenný kód země, která jej vydala;
- d) počet vyhledávání provedených s biometrickými údaji a bez nich.

Z těchto údajů nesmí být možné identifikovat jednotlivce.

3. Výhradně pro účely podávání zpráv a statistiky mají řádně zmocnění pracovníci příslušných orgánů členských států, Komise a agentury eu-LISA přístup k těmto údajům souvisejícím s MID:

- a) počet vyhledávání provedených s biometrickými údaji a bez nich;
- b) počet jednotlivých typů propojení a informačních systémů EU obsahujících propojené údaje;
- c) doba, po kterou zůstalo žluté a červené propojení v systému.

Z těchto údajů nesmí být možné identifikovat jednotlivce.

4. Řádně zmocnění pracovníci Evropské agentury pro pohraniční a pobřežní stráž mají přístup k údajům uvedeným v odstavcích 1, 2 a 3 tohoto článku pro účely provádění analýz rizik a hodnocení zranitelnosti podle článků 11 a 13 Evropského parlamentu a Rady (EU) 2016/1624 ⁽³⁸⁾.

5. Řádně zmocnění pracovníci Europolu mají přístup k údajům uvedeným v odstavcích 2 a 3 tohoto článku pro účely provádění strategických, tematických a operačních analýz podle čl. 18 odst. 2 písm. b) a c) nařízení (EU) 2016/794.

6. Pro účely odstavců 1, 2 a 3 ukládá agentura eu-LISA údaje uvedené v těchto odstavcích v CRRS. Z údajů v CRRS nesmí být možné identifikovat jednotlivce, ale tyto údaje musí umožnit orgánům uvedeným v odstavcích 1, 2 a 3 získávat přizpůsobitelné zprávy a statistiky s cílem zvýšit účinnost hraničních kontrol, usnadnit orgánům zpracovávání žádostí o víza a podpořit vytváření fakticky podložených politik Unie v oblasti migrace a bezpečnosti.

7. Komise zpřístupní Agentuře Evropské unie pro základní práva na její žádost relevantní informace přiměřené shrnutí za účelem vyhodnocení dopadu tohoto nařízení na základní práva.

⁽³⁸⁾ Nařízení Evropského parlamentu a Rady (EU) 2016/1624 ze dne 14. září 2016 o Evropské pohraniční a pobřežní stráž a o změně nařízení Evropského parlamentu a Rady (EU) 2016/399 a zrušení nařízení Evropského parlamentu a Rady (ES) č. 863/2007, nařízení Rady (ES) č. 2007/2004 a rozhodnutí Rady 2005/267/ES (Úř. věst. L 251, 16.9.2016, s. 1).

Článek 63

Přechodné období pro používání Evropského vyhledávacího portálu

1. Po dobu dvou let ode dne zahájení provozu ESP se neuplatní povinnosti uvedené v čl. 7 odst. 2 a 4 a používání ESP je nepovinné.
2. Komisi je svěřena pravomoc přijmout akt v přenesené pravomoci v souladu s článkem 69, kterým změní toto nařízení tak, že se jednou prodlouží doba uvedená v odstavci 1 tohoto článku o nejvýše jeden rok, jestliže z posouzení uplatňování ESP vyplývá, že toto prodloužení je nezbytné, zejména s ohledem na dopad, který by mělo uvedení ESP do provozu na organizaci a délku hraničních kontrol.

Článek 64

Přechodné období pro přístup ke společnému úložišti údajů o totožnosti pro účely prevence, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů

Článek 22 se použije ode dne zahájení provozu CIR uvedeného v čl. 68 odst. 3.

Článek 65

Přechodné období pro odhalování vícenásobné totožnosti

1. Po dobu jednoho roku poté, co agentura eu-LISA oznámí dokončení testu MID uvedeného v čl. 68 odst. 4 písm. b), a před zahájením provozu MID odpovídá za zjišťování vícenásobné totožnosti s použitím údajů uložených v EES, VIS, Eurodacu a SIS ústřední jednotka ETIAS. Odhalování vícenásobné totožnosti se provádí pouze s použitím biometrických údajů.
 2. Pokud vyhledávání vykáže jednu či více shod a údaje o totožnosti v propojených souborech jsou stejné nebo podobné, vytvoří se v souladu s článkem 33 bílé propojení.
- Pokud vyhledávání vykáže jednu či více shod a údaje o totožnosti v propojených souborech nelze považovat za podobné, vytvoří se v souladu s článkem 30 žluté propojení a použije se postup uvedený v článku 29.
- Pokud je vykázáno výsledkem více shod, vytvoří se propojení mezi všemi údaji, které vedly ke shodě.
3. Pokud se vytvoří žluté propojení, MID udělí přístup k údajům o totožnosti vyskytujícím se v různých informačních systémech EU ústřední jednotce ETIAS.
 4. Pokud se vytvoří propojení se záznamem v SIS, který je jiný než záznam vytvořený podle článku 3 nařízení (EU) 2018/1860, článků 24 a 25 nařízení (EU) 2018/1861 a článku 38 nařízení (EU) 2018/1862, MID udělí přístup k údajům o totožnosti vyskytujícím se v různých informačních systémech centrále SIRENE členského státu, který záznam vytvořil.
 5. Ústřední jednotka ETIAS nebo v případech uvedených v odstavci 4 tohoto článku centrála SIRENE členského státu, který záznam vytvořil, má přístup k údajům obsaženým v souboru údajů souvisejících s potvrzením totožnosti, posuzuje různé totožnosti, aktualizuje propojení v souladu s články 31, 32 a 33 a doplní ho do souboru údajů souvisejících s potvrzením totožnosti.
 6. Ústřední jednotka ETIAS učiní oznámení Komisi v souladu s čl. 67 odst. 3 poté, co byla všechna žlutá propojení manuálně ověřena a jejich statut aktualizován na zelená, bílá nebo červená propojení.
 7. Při odhalování vícenásobné totožnosti podle tohoto článku jsou ústřední jednotce ETIAS podle potřeby nápomocny členské státy.
 8. Komisi je svěřena pravomoc přijmout akt v přenesené pravomoci v souladu s článkem 69, kterým změní toto nařízení tak, že se prodlouží doba uvedená v odstavci 1 tohoto článku o šest měsíců, přičemž ji lze prodloužit dvakrát, pokaždé o šest měsíců. Toto prodloužení smí být povoleno pouze na základě posouzení odhadované doby k dokončení odhalování vícenásobné totožnosti podle tohoto článku, které ukazuje, že odhalování vícenásobné totožnosti nebude možné dokončit před dobou zbývající podle odstavce 1 tohoto článku nebo během probíhajícího prodloužení z důvodu nezávislých na ústřední jednotce ETIAS a že nelze uplatnit žádná nápravná opatření. Posouzení se provede nejpozději tři měsíce před uplynutím této doby nebo probíhajícího prodloužení.

Článek 66

Náklady

1. Náklady vzniklé ve spojení se zřízením a provozem ESP, sdílené BMS, CIR a MID jsou hrazeny ze souhrnného rozpočtu Unie.
2. Náklady vzniklé v souvislosti s integrací stávajících vnitrostátních infrastruktur a jejich připojením k vnitrostátním jednotným rozhraním, jakož i náklady vzniklé v souvislosti s provozováním vnitrostátních jednotných rozhraní, jsou hrazeny ze souhrnného rozpočtu Unie.

Vyloučeny jsou tyto náklady:

- a) projektové řízení v členských státech (schůze, služební cesty, kanceláře);
- b) náklady na provozování vnitrostátních informačních systémů (prostory, instalace, elektřina, chlazení);
- c) provoz vnitrostátních informačních systémů (smlouvy s operátory a technickou podporou);
- d) návrh, vývoj, realizace, provoz a údržba vnitrostátních komunikačních sítí.

3. Aniž je dotčeno poskytnutí dalších finančních prostředků na tento účel z jiných zdrojů souhrnného rozpočtu Unie, uvolňuje se z krytí ve výši 791 000 000 EUR přiděleného podle čl. 5 odst. 5 písm. b) nařízení (EU) č. 515/2014 na pokrytí nákladů provádění tohoto nařízení podle odstavců 1 a 2 tohoto článku částka ve výši 32 077 000 EUR.

4. Z krytí uvedeného v odstavci 3 se přidělí 22 861 000 EUR agentuře eu-LISA, 9 072 000 EUR Europolu a 144 000 EUR Agentuře Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva (CEPOL) na podporu plnění úkolů těchto agentur podle tohoto nařízení. Toto financování je plněno v nepřímém řízení.

5. Náklady na určené orgány hradí jednotlivé určující členské státy. Náklady na připojení každého určeného orgánu k CIR hradí příslušný členský stát.

Europol hradí své vlastní náklady, včetně nákladů na připojení k CIR.

Článek 67

Oznámení

1. Členské státy oznámí agentuře eu-LISA orgány uvedené v člancích 7, 20, 21 a 26, které mohou využívat ESP, CIR a MID nebo k nim mít přístup.

Konsolidovaný seznam uvedených orgánů se zveřejní v Úředním věstníku Evropské unie do tří měsíců ode dne zahájení provozu jednotlivých složek interoperability v souladu s článkem 68. V případě změn v tomto seznamu zveřejní agentura eu-LISA jednou za rok aktualizovaný konsolidovaný seznam.

2. Agentura eu-LISA oznámí Komisi úspěšné dokončení testů uvedených v čl. 68 odst. 1 písm. b), odst. 2 písm. b), odst. 3 písm. b), odst. 4 písm. b), odst. 5 písm. b) a odst. 6 písm. b).
3. Ústřední jednotka ETIAS oznámí Komisi úspěšné dokončení přechodného období stanoveného v článku 65.
4. Komise zpřístupní členským státům a veřejnosti informace oznámené podle odstavce 1 na nepřetržitě aktualizované veřejné internetové stránce.

Článek 68

Zahájení provozu

1. Komise stanoví datum zahájení provozu ESP prostřednictvím prováděcího aktu, jakmile jsou splněny tyto podmínky:

- a) byla přijata opatření uvedená v čl. 8 odst. 2, čl. 9 odst. 7 a čl. 43 odst. 5;

- b) agentura eu-LISA oznámila úspěšné dokončení souhrnného testu ESP, který provedla ve spolupráci s orgány členských států a agenturami Unie, které mohou ESP používat;
- c) agentura eu-LISA potvrdila, že byla provedena nezbytná technická a právní opatření týkající se shromažďování a předávání údajů uvedených v čl. 8 odst. 1, a oznámila je Komisi.

ESP smí vyhledávat v databázích Interpolu, jakmile technická opatření umožňují soulad s čl. 9 odst. 5. Není-li možné dodržet čl. 9 odst. 5, má to za následek, že ESP nevyhledává v databázích Interpolu, ale zahájení provozu ESP tím není odloženo.

Komise stanoví datum uvedené v prvním pododstavci tak, aby spadalo do 30 dnů od přijetí prováděcího aktu.

2. Komise stanoví datum zahájení provozu sdílené BMS prostřednictvím prováděcího aktu, jakmile jsou splněny tyto podmínky:

- a) byla přijata opatření uvedená v čl. 13 odst. 5 a čl. 43 odst. 5;
- b) agentura eu-LISA oznámila úspěšné dokončení souhrnného testu sdílené BSM, který provedla ve spolupráci s orgány členských států;
- c) agentura eu-LISA potvrdila, že byla provedena nezbytná technická a právní opatření týkající se shromažďování a předávání údajů uvedených v článku 13, a oznámila je Komisi;
- d) agentura eu-LISA oznámila Komisi úspěšné dokončení testu uvedeného v odst. 5 písm. b).

Komise stanoví datum uvedené v prvním pododstavci tak, aby spadalo do 30 dnů od přijetí prováděcího aktu.

3. Komise stanoví datum zahájení provozu CIR prostřednictvím prováděcího aktu, jakmile jsou splněny tyto podmínky:

- a) byla přijata opatření uvedená v čl. 43 odst. 5 a čl. 74 odst. 10;
- b) agentura eu-LISA oznámila úspěšné dokončení souhrnného testu CIR, který provedla ve spolupráci s orgány členských států;
- c) agentura eu-LISA potvrdila, že byla provedena nezbytná technická a právní opatření týkající se shromažďování a předávání údajů uvedených v článku 18, a oznámila je Komisi;
- d) agentura eu-LISA oznámila Komisi úspěšné dokončení testu uvedeného v odst. 5 písm. b).

Komise stanoví datum uvedené v prvním pododstavci tak, aby spadalo do 30 dnů od přijetí prováděcího aktu.

4. Komise stanoví datum zahájení provozu CIR prostřednictvím prováděcího aktu, jakmile jsou splněny tyto podmínky:

- a) byla přijata opatření uvedená v čl. 28 odst. 5 a 7, čl. 32 odst. 5, čl. 33 odst. 6, čl. 43 odst. 5 a čl. 49 odst. 6;
- b) agentura eu-LISA oznámila úspěšné dokončení souhrnného testu MID, který provedla ve spolupráci s orgány členských států a ústřední jednotkou ETIAS;
- c) agentura eu-LISA potvrdila, že byla provedena nezbytná technická a právní opatření týkající se shromažďování a předávání údajů uvedených v článku 13, a oznámila je Komisi;
- d) ústřední jednotka ETIAS učinila oznámení Komisi v souladu s čl. 67 odst. 3;
- e) agentura eu-LISA oznámila Komisi úspěšné dokončení testu uvedeného v odst. 1 písm. b), odst. 2 písm. b), odst. 3 písm. b) a odst. 5 písm. b).

Komise stanoví datum uvedené v prvním pododstavci tak, aby spadalo do 30 dnů od přijetí prováděcího aktu.

5. Komise stanoví prostřednictvím prováděcích aktů datum, od něhož se použijí automatizované mechanismy a postup kontroly kvality údajů, společné ukazatele kvality údajů a minimální normy kvality údajů, jakmile jsou splněny tyto podmínky:

- a) byla přijata opatření uvedená v čl. 37 odst. 4;

- b) agentura eu-LISA oznámila úspěšné dokončení souhrnného testu mechanismů a postupů automatizované kontroly kvality údajů, společných ukazatelů kvality údajů a minimálních norem kvality údajů, který provedla ve spolupráci s orgány členských států.

Komise stanoví datum uvedené v prvním pododstavci tak, aby spadalo do 30 dnů od přijetí prováděcího aktu.

6. Komise stanoví datum zahájení provozu CRRS prostřednictvím prováděcího aktu, jakmile jsou splněny tyto podmínky:

- a) byla přijata opatření uvedená v čl. 39 odst. 5 a čl. 43 odst. 5;
- b) agentura eu-LISA oznámila úspěšné dokončení souhrnného testu CRRS, který provedla ve spolupráci s orgány členských států;
- c) agentura eu-LISA potvrdila, že byla provedena nezbytná technická a právní opatření týkající se shromažďování a předávání údajů uvedených v článku 39, a oznámila je Komisi.

Komise stanoví datum uvedené v prvním pododstavci tak, aby spadalo do 30 dnů od přijetí prováděcího aktu.

7. Komise sdělí Evropskému parlamentu a Radě výsledky testů provedených v souladu s odst. 1 písm. b), odst. 2 písm. b), odst. 3 písm. b), odst. 4 písm. b), odst. 5 písm. b) a odst. 6 písm. b).

8. Členské státy, ústřední jednotka ETIAS a Europol začnou používat každou ze složek interoperability ode dne stanoveného Komisí v souladu s odstavci 1, 2, 3 a 4.

Článek 69

Výkon přenesené pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.
2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 28 odst. 5, čl. 39 odst. 5, čl. 49 odst. 6, čl. 63 odst. 2 a čl. 65 odst. 8 je svěřena Komisi na dobu pěti let ode 11. června 2019. Komise vypracuje zprávu o výkonu přenesené pravomoci nejpozději devět měsíců před koncem tohoto pětiletého období. Přenesení pravomoci se automaticky prodlužuje o stejně dlouhá období, pokud Evropský parlament nebo Rada nevysloví proti tomuto prodloužení námitku nejpozději tři měsíce před koncem každého z těchto období.
3. Evropský parlament nebo Rada mohou přenesení pravomocí uvedené v čl. 28 odst. 5, čl. 39 odst. 5, čl. 49 odst. 6, čl. 63 odst. 2 a čl. 65 odst. 8 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm blíže určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v Úředním věstníku Evropské unie nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.
4. Před přijetím aktu v přenesené pravomoci Komise vede konzultace s odborníky jmenovanými jednotlivými členskými státy v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů.
5. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.
6. Akt v přenesené pravomoci přijatý podle v čl. 28 odst. 5, čl. 39 odst. 5, čl. 49 odst. 6, čl. 63 odst. 2 a čl. 65 odst. 8 vstoupí v platnost pouze tehdy, pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

Článek 70

Postup projednávání ve výboru

1. Komisi je nápomocen výbor. Tento výbor je výborem ve smyslu nařízení (EU) č. 182/2011.
2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

Pokud výbor nevydá žádné stanovisko, Komise navrhaný prováděcí akt nepřijme a použije se čl. 5 odst. 4 třetí pododstavec nařízení (EU) č. 182/2011.

Článek 71

Poradní skupina

Agentura eu-LISA zřídí Poradní skupinu pro interoperabilitu. Během fáze návrhu a vývoje složek interoperability se použije čl. 54 odst. 4, 5 a 6.

Článek 72

Odborná příprava

Agentura eu-LISA plní úkoly související s poskytováním odborné přípravy zaměřené na technické aspekty používání složek interoperability podle nařízení (EU) 2018/1762.

Orgány členských států a agentury Unie organizují pro své pracovníky zmocněné ke zpracovávání údajů za použití složek interoperability vhodné vzdělávací programy v oblasti bezpečnosti údajů, kvality údajů, pravidel pro ochranu údajů, postupů použitelných pro zpracovávání údajů a povinností poskytovat informace podle čl. 32 odst. 4, čl. 33 odst. 4 a článku 47.

Ve vhodných případech jsou na úrovni Unie pořádány společné vzdělávací kurzy věnované těmto tématům s cílem prohloubit spolupráci a výměnu osvědčených postupů mezi pracovníky orgánů členských států a agentur Unie, kteří jsou zmocněni ke zpracovávání údajů za použití složek interoperability. Zvláštní pozornost je věnována procesu odhalování vícenásobné totožnosti včetně manuálního ověření různých totožností a s tím související nutnost zachovat vhodné záruky základních práv.

Článek 73

Praktická příručka

Komise v úzké spolupráci s členskými státy, agenturou eu-LISA a dalšími příslušnými agenturami Unie vypracuje praktickou příručku pro provádění a řízení složek interoperability. Praktická příručka poskytne technické a operativní pokyny, doporučení a osvědčené postupy. Komise ji přijme formou doporučení.

Článek 74

Sledování a hodnocení

1. Agentura eu-LISA zajistí zavedení postupů ke sledování vývoje složek interoperability a jejich připojení k vnitrostátnímu jednotnému rozhraní vzhledem k cílům v oblasti plánování a nákladů a ke sledování fungování složek interoperability, pokud jde o porovnání jejich technických výstupů, nákladové efektivnosti, bezpečnosti a kvality služeb se stanovenými cíli.
2. Do 12. prosince 2019 a poté každých šest měsíců během fáze vývoje složek interoperability předloží agentura eu-LISA Evropskému parlamentu a Radě zprávu o stavu vývoje složek interoperability a jejich připojení k vnitrostátnímu jednotnému rozhraní. Po ukončení vývoje předloží Evropskému parlamentu a Radě zprávu, ve které podrobně vysvětlí, jak byly splněny cíle týkající se zejména plánování a nákladů, a odůvodní případné odchylky.
3. Čtyři roky po zahájení provozu jednotlivých složek interoperability v souladu s článkem 68 a poté každé čtyři roky předloží agentura eu-LISA Evropskému parlamentu, Radě a Komisi zprávu o technickém fungování složek interoperability, včetně jejich zabezpečení.
4. Dále pak po uplynutí jednoho roku od jednotlivých zpráv agentury eu-LISA vytvoří Komise celkové hodnocení složek interoperability, které obsahují:
 - a) posouzení uplatňování tohoto nařízení;
 - b) posouzení dosažených výsledků ve vztahu k cílům tohoto nařízení a jeho dopadu na základní práva, včetně zejména posouzení dopadu složek interoperability na právo na nediskriminaci;
 - c) posouzení fungování internetového portálu včetně údajů o jeho používání a počet žádostí, které byly vyřízeny;
 - d) posouzení trvajících platností důvodu pro vznik složek interoperability;

- e) posouzení zabezpečení složek interoperability;
- f) posouzení využívání CIR ke zjišťování totožnosti;
- g) posouzení využívání CIR k prevenci, odhalování a vyšetřování teroristických trestných činů a jiných závažných trestných činů;
- h) posouzení všech důsledků, včetně případných nepřiměřených dopadů na plynulost provozu na hraničních přechodech a faktorů majících dopady na souhrnný rozpočet Unie.
- i) hodnocení vyhledávání v databázích Interpolu prostřednictvím ESP, včetně informací o počtu shod v databázích Interpolu a informací o veškerých problémech, které se vyskytly.

Celkové hodnocení podle prvního pododstavce tohoto odstavce zahrnuje případná nezbytná doporučení. Komise předloží tuto hodnotící zprávu Evropskému parlamentu, Radě, evropskému inspektorovi ochrany údajů a Agentuře Evropské unie pro základní práva.

5. Do dne 12. června 2020 a poté každý rok až do přijetí prováděcích aktů Komise uvedených v článku 68 předkládá Komise Evropskému parlamentu a Radě zprávu o aktuálním stavu příprav na provedení tohoto nařízení v plném rozsahu. Tato zpráva obsahuje rovněž podrobné informace o vzniklých nákladech a informace o rizicích, která mohou mít dopad na celkové náklady.

6. Do dvou let ode dne zahájení provozu MID v souladu s čl. 68 odst. 4 vypracuje Komise posouzení dopadu MID na právo na nediskriminaci. Po první zprávě se posouzení dopadu MID na právo na nediskriminaci stává součástí posouzení uvedeného v odst. 4 písm. b) tohoto článku.

7. Členské státy a Europol poskytnou agentuře eu-LISA a Komisi informace nezbytné k vypracování zpráv uvedených v odstavcích 3 až 6. Tyto informace nesmějí ohrozit pracovní metody ani obsahovat informace, které prozrazují zdroje, pracovníky nebo informace o vyšetřování určených orgánů.

8. Agentura eu-LISA poskytne Komisi informace nezbytné k vypracování celkového hodnocení uvedených v odstavci 4.

9. Každý členský stát a Europol vypracují – při dodržení vnitrostátních právních předpisů o zveřejňování citlivých informací a aniž jsou dotčena omezení nutná z důvodu ochrany bezpečnosti a veřejného pořádku, prevence trestné činnosti a zaručení řádného průběhu vnitrostátních vyšetřování – výroční zprávu o účinnosti přístupu k údajům uloženým v CIR pro účely prevence, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů; tato zpráva obsahuje informace a statistiky o:

- a) přesných účelech nahlížení do údajů, včetně typů teroristických trestných činů nebo jiných závažných trestných činů;
- b) oprávněných důvodech pro důvodné podezření, že se na podezřelou osobu, pachatele nebo oběť vztahuje nařízení (EU) č. 603/2013;
- c) počtu žádostí o přístup do CIR pro účely prevence, odhalování a vyšetřování teroristických trestných činů nebo jiných závažných trestných činů;
- d) počtu a typech případů, které byly završeny úspěšným zjištěním totožnosti;
- e) potřebě a využití postupů pro výjimečně naléhavé případy včetně případů, kdy ústřední přístupový bod při následném ověření výjimečnou naléhavost neuznal.

Výroční zprávy vypracované členskými státy a Eupolem se předají Komisi do 30. června následujícího roku.

10. Členským státům je poskytnuto technické řešení k řízení žádostí uživatelů o přístup podle článku 22 a k usnadnění shromažďování informací podle odstavců 7 a 9 tohoto článku pro účely vytváření zpráv a statistik uvedených ve zmíněných odstavcích. Komise přijme prováděcí akty, jimiž stanoví specifikace tohoto technického řešení. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 70 odst. 2.

Článek 75

Vstup v platnost a použitelnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Ustanovení tohoto nařízení týkající se ESP se použijí ode dne stanoveného Komisí v souladu s čl. 68 odst. 1.

Ustanovení tohoto nařízení týkající se sdílené BMS se použijí ode dne stanoveného Komisí v souladu s čl. 68 odst. 2.

Ustanovení tohoto nařízení týkající se CIR se použijí ode dne stanoveného Komisí v souladu s čl. 68 odst. 3.

Ustanovení tohoto nařízení týkající se MID se použijí ode dne stanoveného Komisí v souladu s čl. 68 odst. 4.

Ustanovení tohoto nařízení týkající se automatizovaných mechanismů a postupů kontroly kvality údajů, společných ukazatelů kvality údajů a minimálních norem kvality údajů se použijí ode dnů stanovených Komisí v souladu s čl. 68 odst. 5.

Ustanovení tohoto nařízení týkající se CRRS se použijí ode dne stanoveného Komisí v souladu s čl. 68 odst. 6.

Články 6, 12, 17, 25, 38, 42, 54, 56, 58, 66, 67, 69, 70, 71 a 73 a čl. 74 odst. 1 se použijí ode dne 11. června 2019.

Toto nařízení se použije na Eurodac ode dne použitelnosti přepracovaného znění nařízení (EU) č. 603/2013.

Toto nařízení je závazné v celém rozsahu a přímo použitelné v členských státech v souladu se Smlouvami.

V Bruselu dne 20. května 2019.

Za Evropský parlament

předseda

A. TAJANI

Za Radu

předseda

G. CIAMBA