EVROPSKÁ
KOMISE

Ve Štrasburku dne 12.12.2017
COM(2017) 794 final

2017/0352 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU (policejní a justiční spolupráce, azyl a migrace)

{SWD(2017) 473} - {SWD(2017) 474}

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Okolnosti

V uplynulých třech letech pocítila EU nárůst nedovolených překročení hranic do EU, stejně jako rostoucí a přetrvávající hrozbu pro vnitřní bezpečnost, což se projevilo řadou teroristických útoků. Obyvatelé EU očekávají, že kontroly osob na vnějších hranicích i kontroly v rámci schengenského prostoru budou účinné, zajistí účinné řízení migrace a přispějí k vnitřní bezpečnosti. Tyto výzvy vynesly do popředí naléhavou potřebu propojit a komplexně posílit informační nástroje EU pro správu hranic, řízení migrace a bezpečnost.

Správu informací v EU lze a musí se provádět efektivnější a účelnější tak, aby se při plném dodržování základních práv, mimo jiné zejména práva na ochranu osobních údajů, zajistila lepší ochrana vnějších hranic EU, zlepšilo řízení migrace a posílila se vnitřní bezpečnost ku prospěchu všech občanů. Na úrovni EU již existuje řada informačních systémů, jejichž cílem je poskytovat příslušníkům pohraniční stráže, imigračním úředníkům a pracovníkům donucovacích orgánů důležité informace o osobách, a na vývoji dalších takových systémů se pracuje. Aby tato podpora byla účinná, musejí být informace poskytované informačními systémy EU úplné, přesné a spolehlivé. V architektuře správy informací EU se však projevují strukturální nedostatky. Vnitrostátní orgány se musejí vypořádat se složitým prostředím různě řízených informačních systémů. Architektura správy údajů pro ochranu hranic a bezpečnost je roztříštěná a informace jsou uchovávány odděleně v nepropojených systémech. Vznikají tak mezery. Z tohoto důvodu **nejsou různé informační systémy na úrovni EU v současnosti interoperabilní** – tj. neprobíhá mezi nimi výměna a sdílení informací tak, aby orgány a příslušní úředníci mohli získat potřebné informace, kdykoli a kdekoli je to nutné. Interoperabilita informačních systémů na úrovni EU může významně pomoci odstranit současná bílá místa, kdy může docházet k tomu, že osoby včetně těch, které mohou být zapojeny do teroristických činností, jsou vedené v jednotlivých, navzájem nepropojených databázích, kde figurují pod různými jmény.

V dubnu 2016 předložila Komise **Sdělení *o silnějších a inteligentnějších informačních systémech pro ochranu hranic a bezpečnost***[1], ve kterém se zabývá řadou strukturálních nedostatků v informačních systémech[2]. Cílem sdělení z dubna 2016 bylo zahájit diskusi o tom, jak mohou informační systémy v Evropské unii zlepšit správu hranic, řízení migrace a vnitřní bezpečnost. Naléhavou potřebu kroků v této oblasti uznala také **Rada**. V červnu 2016 podpořila **plán na posílení výměny informací a správy informací** včetně řešení interoperability v oblasti spravedlnosti a vnitřních věcí[3]. Účelem tohoto plánu byla podpora operativních vyšetřování a rychlé zajištění ucelených, tematických a aktuálních informací vysoké kvality pro pracovníky v předních liniích, jako jsou policisté, příslušníci pohraniční stráže, státní zástupci, imigrační úředníci a další, a umožnit jim tak efektivně spolupracovat a jednat. K přijetí opatření v této oblasti vyzval také **Evropský parlament**. Ve svém usnesení z

[1] COM(2016) 205 ze dne 6. dubna 2016.

[2] 1) Neoptimální fungování stávajících informačních systémů; 2) mezery v informacích v architektuře správy údajů v EU; 3) složité prostředí různě řízených informačních systémů; 4) roztříštěná architektura správy údajů pro ochranu hranic a bezpečnost – informace jsou uchovávány odděleně v nepropojených systémech, takže vznikají bílá místa.

[3] Plán ze dne 6. června 2016 na posílení výměny informací a správy informací včetně řešení interoperability v oblasti spravedlnosti a vnitřních věcí – 9368/1/16 REV 1.

července 2016[4], které se týkalo pracovního programu Komise na rok 2017, požadoval Evropský parlament „*návrhy na zdokonalení a rozvoj stávajících informačních systémů, vyřešení mezer v informacích a pokrok směrem k interoperabilitě a také návrhy na závazné sdílení informací na úrovni EU doprovázené nezbytnými zárukami v oblasti ochrany údajů*“. Projev předsedy Evropské komise Junckera o stavu Unie ze září 2016[5] a závěry Evropské rady z prosince 2016[6] zdůraznily, jak důležité je překonat současné nedostatky v oblasti správy údajů a zlepšit interoperabilitu stávajících informačních systémů.

V červnu 2016, v návaznosti na sdělení z dubna 2016, Komise zřídila **expertní skupinu na vysoké úrovni pro informační systémy a interoperabilitu**[7] s cílem zaměřit se na právní, technické a provozní problémy při posilování interoperability mezi ústředními systémy EU pro ochranu hranic a bezpečnost, včetně jejich nezbytnosti, technické proveditelnosti, přiměřenosti a jejich důsledků pro ochranu údajů. **Závěrečná zpráva** expertní skupiny na vysoké úrovni byla zveřejněna v květnu 2017[8]. Přinesla řadu doporučení pro posílení a rozvoj informačních systémů EU a jejich interoperability. Do práce skupiny odborníků se zapojila také Evropská agentura pro základní práva, evropský inspektor ochrany údajů a protiteroristický koordinátor EU. Každý z nich předložil podpůrné prohlášení a současně konstatoval, že je nutné pokročit v řešení širších otázek základních práv a ochrany údajů. Zástupci sekretariátu Výboru pro občanské svobody, spravedlnost a vnitřní věci Evropského parlamentu a generálního sekretariátu Rady se zúčastnili jako pozorovatelé. Expertní skupina na vysoké úrovni dospěla k závěru, že **je nezbytné a technicky proveditelné pracovat na praktických řešeních interoperability**, která v zásadě mohou mít operativní přínosy a zároveň je lze realizovat v souladu s požadavky na ochranu údajů.

Na základě zprávy a doporučení expertní skupiny Komise ve své *sedmé zprávě o pokroku na cestě k účinné a skutečné bezpečnostní unii*[9] stanovila **nový přístup ke správě údajů** pro bezpečnost, správu hranic a řízení migrace, kde jsou všechny centralizované informační systémy pro bezpečnost, správu hranic a řízení migrace interoperabilní při plném dodržování základních práv. Komise oznámila svůj záměr pokračovat v práci na vytvoření Evropského vyhledávacího portálu, který dokáže souběžně prohledávat všechny příslušné systémy EU v oblasti bezpečnosti, správy hranic a řízení migrace, přičemž se pravděpodobně uplatní jednodušší pravidla pro přístup pro účely prosazování práva, a vytvořit pro tyto systémy sdílenou službu pro porovnávání biometrických údajů (případně schopnou označit shodu[10]) a společné úložiště údajů o totožnosti. Oznámila svůj záměr co nejdříve předložit legislativní návrh týkající se interoperability.

Závěry Evropské rady z června 2017[11] zopakovaly potřebu jednat. Na základě závěrů Rady pro spravedlnost a vnitřní věci z června 2017[12] vyzvala Evropská rada Komisi, aby za účelem

---

4 Usnesení Evropského parlamentu ze dne 6. července 2016 o strategických prioritách pracovního programu Komise na rok 2017 (2016/2773(RSP)).

5 Stav Unie 2016 (14. 9. 2016), https://ec.europa.eu/commission/state-union-2016_cs.

6 Závěry Evropské rady (15. 12. 2016), http://www.consilium.europa.eu/media/21909/15-euco-conclusions-final-cs.pdf.

7 Rozhodnutí Komise ze dne 17. června 2016 o zřízení expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu – 2016/C 257/03.

8 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

9 COM(2017) 261 final.

10 Nová koncepce ochrany soukromí již od návrhu, která omezuje přístup ke všem údajům pouze na oznámení o nalezení/nenalezení shody upozorňující na přítomnost (či nepřítomnost) údajů.

11 Závěry Evropské rady ze zasedání ve dnech 22.–23. června 2017.

12 Výsledky 3546. zasedání Rady pro spravedlnost a vnitřní věci ze dne 8. a 9. června 2017, 10136/17.

realizace doporučení expertní skupiny na vysoké úrovni co nejdříve připravila návrh právního aktu. Tato iniciativa také reaguje na výzvu Rady k vytvoření uceleného rámce pro přístup pro účely prosazování práva do různých databází v oblasti spravedlnosti a vnitřních věcí s cílem dosáhnout vyšší míry zjednodušení, soudržnosti a účinnosti a věnovat větší pozornost operativním potřebám[13]. Pro posílení snah učinit z Evropské unie bezpečnější společnost, v plném souladu se základními právy, Komise ve svém pracovním programu na rok 2018[14] oznámila, že návrh týkající se interoperability informačních systémů bude představen do konce roku 2017.

- **Cíle návrhu**

Obecné cíle této iniciativy vyplývají z cílů uvedených ve Smlouvě v oblasti zlepšování správy vnějších hranic schengenského prostoru a posilování vnitřní bezpečnosti Evropské unie. Odvozují se také od politických rozhodnutí Komise a příslušných závěrů (Evropské) Rady. Tyto cíle jsou dále zpracovány v Evropském programu pro migraci a následných sděleních, včetně sdělení o ochraně a posílení Schengenu,[15] Evropského programu pro bezpečnost[16] a zpráv Komise o činnosti a pokroku na cestě k účinné a skutečné bezpečnostní unii[17].

Cíle tohoto návrhu jsou neoddělitelně spjaty s výše uvedenými skutečnostmi, přičemž se opírají zejména o sdělení z dubna 2016 a o zjištění expertní skupiny na vysoké rovni.

Návrh má tyto specifické cíle:

1) zajistit, aby koncoví uživatelé, zejména příslušníci pohraniční stráže, pracovníci donucovacích orgánů, imigrační úředníci a justiční orgány, získali **rychlý, plynulý, bezproblémový a řízený přístup** k informacím, které potřebují k plnění svých úkolů;

2) zajistit řešení pro **odhalování vícenásobných totožností** spojených s totožnými soubory biometrických údajů, a to s dvojím účelem, kterým je zajištění správného zjištění totožnosti osob jednajících v dobré víře a **potírání podvodného zneužití totožnosti**;

3) usnadnit **kontroly totožnosti státních příslušníků třetích zemí** na území členského státu ze strany policejních orgánů a

4) usnadnit a **zjednodušit přístup donucovacích orgánů** k informačním systémům, jež neslouží k prosazování práva, na úrovni EU, pokud to je nezbytné pro předcházení, vyšetřování, odhalování nebo stíhání závažné trestné činnosti a terorismu.

Kromě těchto základních operativních cílů tento návrh také pomůže:

[13] Výbor stálých zástupců Rady (Coreper) dne 2. března 2017 při udělování mandátu předsednictví Rady k zahájení interinstitucionálního jednání o Systému vstupu/výstupu EU schválil návrh prohlášení Rady vyzývající Komisi, aby navrhla komplexní rámec pro přístup do různých databází v oblasti spravedlnosti a vnitřních věcí pro účely vymáhání práva za účelem dosažení většího zjednodušení, soudržnosti, účinnosti a zohlednění operačních potřeb (Souhrnný zápis 7177/17, 21. 3. 2017).

[14] COM(2017) 650 final.

[15] COM(2017) 570 final.

[16] COM(2015) 185 final.

[17] COM(2016) 230 final.

- usnadnit technické a operační provádění stávajících a budoucích nových informačních systémů **ze strany členských států**;
- posílit a zjednodušit podmínky pro **bezpečnost a ochranu údajů**, kterými se řídí příslušné systémy, a
- zlepšit a sladit požadavky na **kvalitu údajů** jednotlivých systémů.

Návrh pak také obsahuje ustanovení pro zavedení a řízení univerzálního formátu pro zprávy (UMF) jako normy EU pro vývoj informačních systémů v oblasti spravedlnosti a vnitřních věcí a zřízení centrálního úložiště pro účely podávání zpráv a statistiky.

- **Oblast působnosti návrhu**

Společně se souvisejícím návrhem předkládaným v tentýž den se návrh týkající se interoperability zaměřuje na informační systémy EU pro bezpečnost, správu hranic a řízení migrace, které jsou provozovány na centrální úrovni a z nichž tři již existují, jeden stojí na počátku vývoje a další dva jsou ve fázi návrhů, o nichž nyní jednají spolunormotvůrci. Každý systém má vlastní cíle, účely, právní základ, pravidla, uživatelské skupiny a institucionální kontext.

V současné době existující tyto tři centralizované informační systémy:

- **Schengenský informační systém (SIS)** se širokou škálou záznamů o osobách (odepření vstupu nebo pobytu, evropský zatýkací rozkaz, pohřešované osoby, zajištění spolupráce v soudním řízení, skryté a zvláštní kontroly) a věcech (včetně ztracených, odcizených a neplatných dokladů totožnosti nebo cestovních dokladů)[18];
- systém **Eurodac** s údaji o otiscích prstů žadatelů o azyl a státních příslušníků třetích zemí, kteří nedovoleně překročili vnější hranice nebo kteří nelegálně pobývají v některém členském státě, a
- **Vízový informační systém (VIS)** s údaji o krátkodobých vízech.

Kromě těchto stávajících systémů Komise v letech 2016–2017 navrhla tři nové centralizované informační systémy EU:

- **Systém vstupu/výstupu (EES)**, jehož právní základ byl nyní schválen, nahradí současný systém ručního razítkování cestovních pasů a bude elektronicky zaznamenávat jméno, druh cestovního dokladu, biometrické údaje a datum a místo vstupu a výstupu státních příslušníků třetích zemí, kteří vstupují do schengenského prostoru za účelem krátkodobého pobytu;
- navrhovaný **evropský systém pro cestovní informace a povolení (ETIAS)**, bude-li přijat, bude z velké části automatizovaným systémem, který bude shromažďovat a ověřovat informace poskytnuté státními příslušníky třetích zemí s bezvízovým režimem před jejich cestou do schengenského prostoru, a
- navrhovaný **Evropský informační systém rejstříků trestů pro státní příslušníky třetích zemí (systém ECRIS-TCN)**, který by byl elektronickým systémem pro

[18] Návrhy nařízení Komise z prosince 2016 o SIS navrhují, aby byla zahrnuta také rozhodnutí o navrácení a vyšetřovací kontroly.

výměnu informací o předchozích odsouzeních státních příslušníků třetích zemí trestními soudy v EU.

Těchto šest systémů se vzájemně doplňuje – s výjimkou Schengenského informačního systému (SIS) – a jsou zaměřeny výlučně na státní příslušníky třetích zemí. Tyto systémy pomáhají vnitrostátním orgánům v oblasti správy hranic, řízení migrace, zpracovávání víz a otázek azylu a v boji proti trestné činnosti a terorismu. Toto platí zejména pro SIS, který je dnes nejrozšířenějším nástrojem pro sdílení informací v oblasti prosazování práva.

Kromě těchto informačních systémů spravovaných centrálně na úrovni EU zahrnuje oblast působnosti tohoto návrhu také databázi odcizených a ztracených cestovních dokladů (SLTD) Interpolu, která je v souladu s ustanoveními Schengenského hraničního kodexu systematicky požívána na vnějších hranicích EU, a databázi Interpolu TDAWN (cestovní doklady s údaji uvedenými v oběžnících). Týká se rovněž údajů **Europolu**, a to v míře nutné pro fungování navrhovaného systému ETIAS a pro zajištění pomoci členským státům při dotazování na údaje o závažné trestné činnosti a terorismu.

Vnitrostátní informační systémy a decentralizované informační systémy EU jsou mimo oblast působnosti této iniciativy. Pokud bude prokázána taková nezbytnost, mohou být decentralizované systémy, jako jsou systémy provozované v prümském rámci,[19] směrnice o jmenné evidenci cestujících (PNR)[20] a směrnice o předběžných informacích o cestujících[21], připojeny v pozdější fázi k jedné či více složkám navrhovaným v rámci této iniciativy[22].

Aby se dodržoval rozdíl mezi záležitostmi, které představují rozvoj schengenského *acquis*, pokud jde o hranice a víza, na jedné straně, a na druhé straně dalšími systémy, které se týkají schengenského *acquis* v oblasti policejní spolupráce nebo s schengenským *acquis* nesouvisejí, zabývá se tento návrh přístupem k Schengenskému informačnímu systému, jak jej v současnosti upravuje rozhodnutí 2007/533/SVV, a systémem Eurodac a [ECRIS-TCN].

- **Nezbytné technické složky pro dosažení interoperability**

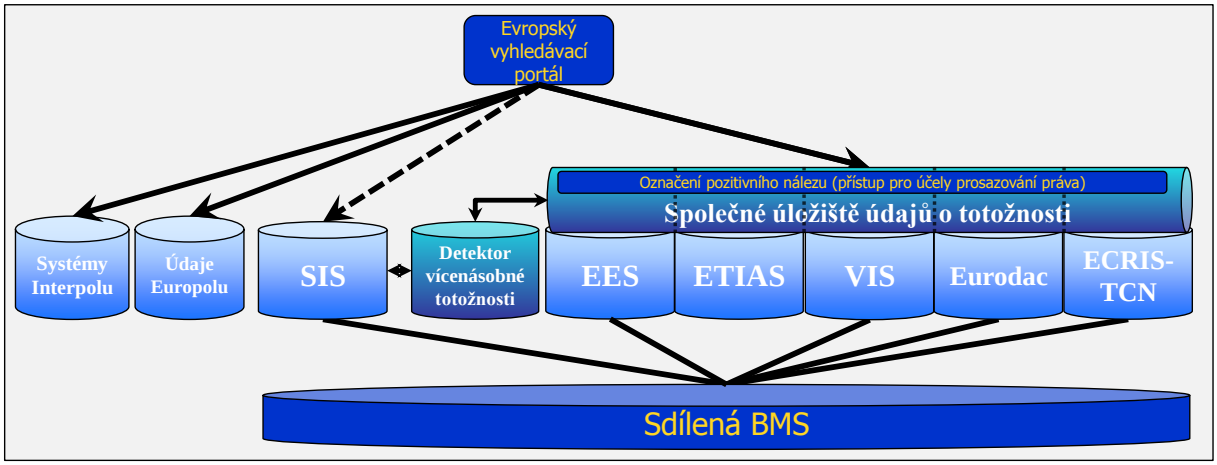
K dosažení cílů tohoto návrhu je nutné zřídit tyto čtyři složky interoperability:

- Evropský vyhledávací portál – ESP
- sdílená služba pro porovnávání biometrických údajů – sdílená BMS
- společné úložiště údajů o totožnosti – CIR
- detektor vícenásobné totožnosti – MID

Každá z těchto složek je podrobně popsána v pracovním dokumentu útvarů Komise o posouzení dopadů, který doprovází tento návrh.

Kombinace těchto čtyř složek vede k následujícímu řešení interoperability:

[19] http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1508936184412&uri=CELEX:32008D06 15
[20] http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1508936384641&uri=CELEX:32016L06 81
[21] Směrnice Rady 2004/82/ES ze dne 29. dubna 2004 o povinnosti dopravců předávat údaje o cestujících.
[22] Obdobně s ohledem na celní systémy Rada ve svých závěrech z června 2017 vyzvala Komisi, aby vypracovala studii proveditelnosti s cílem podrobněji prozkoumat technické, provozní a právní aspekty interoperability systémů pro bezpečnost a správu hranic s celními systémy, a aby svá zjištění předložila do konce roku 2018 Radě k projednání.



Cíle a fungování těchto čtyř složek lze shrnout takto:

1) **Evropský vyhledávací portál (ESP)** je složkou, která by umožnila souběžné vyhledávání ve více systémech (v centrálním SIS, Eurodacu, VIS, budoucím EES a navrhovaných systémech ETIAS a ECRIS-TCN i příslušných systémech Interpolu a údajích Europolu) s použitím údajů o totožnosti (biografických i biometrických). Tento portál by zajistil, aby uživatelé evropských informačních systémů měli rychlý, bezproblémový, účinný, systematický a řízený přístup ke všem informacím, které potřebují k plnění svých úkolů.

   Vyhledávání v Evropském vyhledávacím portálu by okamžitě, v řádu sekund, zajistilo informace z různých systémů, k nimž má uživatel oprávněný přístup. V závislosti na účelu vyhledávání a příslušných přístupových právech by měl ESP různé konfigurace.

   ESP nezpracovává žádné nové údaje a žádné údaje neukládá; fungoval by jako jednotný portál nebo „zprostředkovatel zpráv“ pro vyhledávání v různých ústředních systémech a plynule by získával nezbytné informace, a to při plném dodržování požadavků na kontrolu přístupu a ochranu údajů základních systémů. ESP by usnadnil správné a oprávněné používání všech stávajících evropských informačních systémů a zjednodušil by a zlevnil jejich prohlížení a používání pro členské státy, v souladu se právními nástroji, kterými se tyto systémy řídí.

2) **Sdílená služba pro porovnávání biometrických údajů (sdílená BMS)** by umožnila vyhledávání a porovnávání biometrických údajů (otisky prstů a zobrazení obličeje) z několika ústředních systémů (zejména ze systémů SIS, Eurodac, VIS, budoucího EES a navrhovaného systému ECRIS-TCN). Navrhovaný systém ETIAS nebude obsahovat biometrické údaje a nebude tedy propojen se sdílenou BMS.

   Tam, kde stávající ústřední systém (SIS, Eurodac, VIS) v současnosti používá vyhrazený, vlastní nástroj pro vyhledávání biometrických údajů[23], poskytne sdílená služba pro porovnávání biometrických údajů společnou platformu, v níž jsou údaje vyhledávány a porovnávány souběžně. Sdílená BMS by přinesla podstatné výhody, pokud jde o bezpečnost, náklad, údržbu a provoz, neboť by využívala jedinou technologickou složku namísto pěti různých. Biometrické údaje (otisky prstů a zobrazení obličeje) jsou výhradně

[23] Tyto biometrické vyhledávače se technicky označují jako systém automatizované identifikace otisků prstů (AFIS) nebo systém automatizované biometrické identifikace (ABIS).

uchovávány v základních systémech. Sdílená BMS by vytvořila a zachovala matematické vyjádření biometrických vzorků (šablonu), ale skutečné údaje by se odstranily a zůstaly by tedy uložené jen jednou, na jednom místě.

Sdílená BMS by byla klíčovou složkou umožňující snazší zjišťování propojení mezi soubory údajů a různými totožnostmi, kterými se prokazuje tatáž osoba v různých ústředních systémech. Bez sdílené BMS nebude žádná z ostatních tří složek moci fungovat.

3) **Společné úložiště údajů o totožnosti (CIR)** by bylo sdílenou složkou pro ukládání biografických[24] a biometrických údajů o totožnosti státních příslušníků třetích zemí zaznamenaných v systému Eurodac, VIS, budoucím EES, navrhovaném ETIAS a navrhovaném systému ECRIS-TCN. Každý z těchto pěti ústředních systémů ukládá nebo bude ukládat biografické údaje o konkrétních osobách pro konkrétní účely. To by se nezměnilo. Příslušné údaje o totožnosti by se ukládaly v CIR, ale i nadále by „patřily“ do příslušných základních systémů, které tyto údaje zaznamenaly.

CIR by neobsahoval údaje ze SIS. Komplexní technická architektura SIS obsahující vnitrostátní kopie, částečné vnitrostátní kopie a možné vnitrostátní systémy pro porovnávání biometrických údajů by učinila systém CIR tak složitým, že by již nebyl technicky ani finančně realizovatelný.

Klíčovým cílem CIR je usnadnit biografickou identifikaci státního příslušníka třetí země. Díky CIR by se zvýšila rychlost operací, zlepšila účinnost a dosáhlo by se úspor z rozsahu. Zřízení CIR je nezbytné, aby se umožnily účinné kontroly totožnosti státních příslušníků třetích zemí včetně kontrol na území členského státu. Dále pak přidáním funkce „označení pozitivního nálezu“ by CIR mohl pomoci při kontrole přítomnosti (nebo neexistence) údajů v kterémkoli ze systémů, které CIR pokrývá, a to pomocí jednoduchého oznámení o pozitivním nálezu / bez pozitivního nálezu. CIR by tak rovněž pomohl zjednodušit přístup donucovacích orgánů k informačním systémům, jež neslouží k prosazování práva, zatímco by se zachovala vysoká míra ochrany údajů (viz oddíl týkající se dvoufázového postupu pro přístup pro účely prosazování práva).

Z uvedených pěti systémů, na které má CIR vztahovat, představují budoucí EES, navrhovaný ETIAS a navrhovaný systém ECRIS-TCN nové systémy, které je ještě nutné vyvinout. Stávající systém Eurodac zatím neobsahuje biografické údaje; k jeho rozšíření dojde, jakmile bude pro Eurodac schválen nový právní základ. Stávající systém VIS neobsahuje biografické údaje, avšak s ohledem na jeho nezbytnou interakci s budoucím EES jej bude třeba modernizovat. Vytvoření CIR by tedy přišlo ve správný okamžik. V žádném případě by to neznamenalo zdvojování existujících údajů. Systém CIR by byl technicky vzato vyvinut na bázi platformy EES/ETIAS.

4) **Detektor vícenásobné totožnosti (MID)** by kontroloval, zda vyhledávané údaje o totožnosti existují ve více než jednom ze systémů, které by k němu byly připojeny. MID zahrnuje systémy, které ukládají údaje o totožnosti do CIR (Eurodac, VIS, budoucí systém EES, navrhovaný systém ETIAS a navrhovaný systém ECRIS-TCN), jakož i do systému SIS. MID by umožnil odhalit vícenásobné totožnosti propojené se stejnými

[24] Mezi biografické údaje, které lze najít na cestovním dokladu, patří: příjmení, jméno, pohlaví, datum narození, číslo cestovního dokladu. Nepatří mezi ně adresy, předchozí jména, biometrické údaje atd.

soubory biometrických údajů, a to s dvojím účelem, kterým je usnadnění kontrol totožnosti osob jednajících v dobré víře a potírání podvodného zneužití totožnosti.

MID by umožnil stanovit, zda odlišná jména patří k téže totožnosti. Jde o nezbytnou inovaci pro účinné řešení podvodného používání totožností, což je velmi vážným narušením bezpečnosti. MID by zobrazil pouze ty biografické záznamy o totožnosti, u nichž existuje propojení v různých ústředních systémech. Tato propojení by byla zjišťována prostřednictvím sdílené služby pro porovnávání biometrických údajů a bylo by nutné, aby je potvrdil nebo zamítl orgán, který údaje, jež vedly k vytvoření propojení, zaznamenal do informačního systému. Aby se oprávněným uživatelům MID usnadnilo plnění této povinnosti, systém by označoval zjištěná propojení podle čtyř kategorií:

- žluté propojení – potenciálně odlišné biografické totožnosti téže osoby,
- bílé propojení – potvrzení, že různé biografické totožnosti náležejí stejné osobě jednající v dobré víře,
- zelené propojení – potvrzení, že různé osoby jednající v dobré víře mají stejnou biografickou totožnost,
- červené propojení – podezření, že různé biografické totožnosti zákonně používá tatáž osoba.

Tento návrh popisuje postupy, které by byly zavedeny, aby bylo možné s těmito různými kategoriemi pracovat. Totožnost dotčených osob jednajících v dobré víře by se měla co nejdříve jednoznačně vyjasnit tak, že se žluté propojení změní na potvrzené zelené nebo bílé propojení, aby se zajistilo, že nedojde ke zbytečným potížím. Oproti tomu, pokud by posouzení vedlo k potvrzení červeného propojení nebo ke změně ze žlutého propojení na červené, bylo by nutné přijmout příslušné kroky.

- **Dvoufázový postup pro přístup pro účely prosazování práva zajištěný společným úložištěm údajů o totožnosti**

Prosazování práva se definuje jako druhotný nebo vedlejší cíl systémů Eurodac, VIS, budoucího systému EES a navrhovaného systému ETIAS. V důsledku toho jsou možnosti přístupu k údajům uloženým v těchto systémech pro účely prosazování práva omezené. Donucovací orgány mohou mít k těmto informačním systémům, jež neslouží k prosazování práva, přímý přístup pouze pro účely prevence, vyšetřování, odhalování či stíhání teroristických a jiných závažných trestných činů. Pro příslušné systémy navíc platí různé podmínky pro přístup a záruky a některá z těchto stávajících pravidel_by mohla brzdit zákonné využívání těchto systémů ze strany uvedených orgánů. V obecnější rovině lze říci, že zásada předchozího vyhledávání omezuje možnost orgánů členských států nahlížet do systémů pro odůvodněné účely prosazování práva, a mohla by tedy být příčinou promarněné příležitosti ke zjištění nezbytných informací.

Ve svém sdělení z dubna 2016 Komise uznala nutnost optimalizovat stávající nástroje pro účely prosazování práva při současném dodržení požadavků na ochranu údajů. Tuto nezbytnost potvrdily a zopakovaly členské státy a příslušné agentury v rámci expertní skupiny na vysoké úrovni.

Vzhledem k výše uvedenému by vytvoření systému CIR s tzv. „funkcí označení pozitivního nálezu“ zavedlo možnost získat přístup do systému EES, VIS, ETIAS a Eurodac pomocí **dvoufázového postupu pro nahlížení do údajů**. Tento dvoufázový postup by nezměnil skutečnost, že prosazování práva představuje pro tyto systémy striktně vedlejší cíl, a že se tudíž na něj vztahují přísná pravidla upravující přístup.

V první fázi by pracovník donucovacího orgánu zahájil vyhledávání týkající se určité osoby na základě údajů o totožnosti této osoby, cestovního dokladu nebo biometrických údajů, aby zkontroloval, zda informace o hledané osobě jsou uloženy v systému CIR. Pokud takové údaje existují, pracovník obdrží **odpověď, v níž je uvedeno, který informační systém (systémy) obsahuje (obsahují) údaje** o této osobě (**označení pozitivního nálezu**). Pracovník by neměl skutečný přístup k žádným údajům v žádném ze základních systémů.

Ve druhé fázi by pracovník mohl jednotlivě požádat o přístup do každého systému, který byl uveden jako systém obsahující dané údaje, aby získal kompletní složku o vyhledávané osobě, **v souladu se stávajícími pravidly a postupy stanovenými jednotlivými dotčenými systémy. Přístup** v rámci této druhé fáze by i nadále podléhal předchozímu povolení ze strany určeného orgánu a vyžadoval by i nadále zadání konkrétního uživatelského jména a přihlášení.

Tento nový přístup by také znamenal přidanou hodnotu pro donucovací orgány vzhledem k **existenci možných propojení** v systému MID. Systém MID by pomohl CIR s identifikací stávajících propojení, čímž by se ještě více zpřesnilo vyhledávání. Systém MID by byl schopen uvést, zda je daná osoba v různých informačních systémech **známá pod různými totožnostmi.**

Tento dvoufázový postup pro nahlížení do údajů je zvláště cenný v případech, kdy podezřelý z teroristického trestného činu nebo jiného závažného trestného činu, pachatel nebo údajná oběť takového trestného činu **nejsou známi**. V těchto případech by systém CIR umožnil identifikovat informační systém, který danou osobu zná, během jediného vyhledávání. Stávající podmínky předchozího vyhledávání ve vnitrostátních databázích a předchozího vyhledávání v systému automatizované identifikace otisků prstů jiných členských států podle rozhodnutí 2008/615/SVV („ověření podle Prümské smlouvy“) by tak byly nadbytečné.

Nový dvoufázový postup pro nahlížení do údajů by vstoupil v platnost tehdy, až by byly **složky** interoperability **plně funkční.**

- **Další prvky tohoto návrhu na podporu složek interoperability**

1) Kromě výše uvedených složek obsahuje tento návrh nařízení také návrh na zřízení **centrálního úložiště pro účely podávání zpráv a statistiky (CRRS)**. Toto úložiště je nezbytné, aby mohly být vytvářeny a sdíleny zprávy s (anonymními) statistickými údaji pro politické a provozní účely a pro účely kvality údajů. Současná praxe shromažďování statistických údajů pouze v jednotlivých informačních systémech ohrožuje bezpečnost údajů a výkonnost a neumožňuje korelaci údajů mezi systémy.

   CRRS by poskytlo vyhrazené, samostatné úložiště pro anonymní statistické údaje získané ze systémů SIS, VIS, Eurodac, budoucího EES, navrhovaného ETIAS, navrhovaného ECRIS-TCN, společného úložiště údajů o totožnosti, detektoru vícenásobné totožnosti a ze sdílené služby pro porovnávání biometrických údajů. Úložiště by zajistilo možnost

zabezpečeného sdílení zpráv (v souladu s příslušnými právními nástroji) pro členské státy, Komisi (včetně Eurostatu) a agentury EU.

Vyvinutí jednoho ústředního úložiště namísto několika oddělených úložišť pro každý systém by znamenalo nižší náklady a snížení úsilí zaměřeného na jeho zřízení, provoz i údržbu. Zvýšilo by se rovněž úroveň zabezpečení údajů, jelikož ukládání údajů a kontrola přístupu by byly prováděny v jediném úložišti.

2) Tento návrh nařízení také navrhuje zavedení **univerzálního formátu pro zprávy (UMF)** jako normy na úrovni EU, aby se interoperabilním způsobem umožnila interakce mezi více systémy, včetně systémů vyvinutých a spravovaných agenturou eu-LISA. K používání této normy by byl rovněž pobízen Europol a Interpol.

Norma UMF zavádí společný a jednotný technický jazyk pro účely popsání a propojení datových prvků, zejména těch prvků, které týkají osob a (cestovních) dokladů. Používání UMF při vývoji nových informačních systémů zaručuje snadnější začlenění a interoperabilitu s dalšími systémy, zejména pro členské státy, které potřebují pro komunikaci s těmito novými systémy vytvořit rozhraní. V této souvislosti lze považovat povinné používání UMF při vývoji nových systémů za nezbytný předpoklad pro zavádění složek interoperability navrhovaných v tomto nařízení.

Aby se zajistilo úplné zavedení normy UMF po celé EU, je navrhována odpovídající struktura řízení. Komise by odpovídala za zavedení a vývoj normy UMF v rámci přezkumného postupu s členskými státy. Zapojeny budou i státy přidružené k Schengenské úmluvě, agentury EU a mezinárodní subjekty zúčastněné v projektech UMF (například agentura eu-LISA, Europol a Interpol). Navrhovaná struktura řízení má pro UMF zásadní význam, aby se zajistilo rozšíření této normy a současně se zajistila její co největší použitelnost a uplatnitelnost.

3) Tento návrh nařízení dále zavádí **mechanismy automatizované kontroly kvality a** společné ukazatele kvality, jakož i nutnost, aby členské státy zajistily co nejvyšší úroveň kvality údajů při jejich vkládání do systémů a při používání těchto systémů. Pokud nebude zajištěna nejvyšší kvalita údajů, může tím být negativně ovlivněna schopnost identifikovat hledané osoby a rovněž může dojít k narušení základních práv nevinných osob. Problémy, jejichž příčinou může být zadávání údajů lidskou obsluhou, řeší pravidla pro automatickou validaci, jež mohou chybám ze strany obsluhy zabránit. Cílem by bylo automaticky identifikovat zjevně nesprávné nebo nekonzistentní vložené údaje tak, aby členský stát původu mohl údaje ověřit a provést veškeré nezbytné kroky k nápravě. Agentura eu-LISA by navíc vypracovávala a předkládala pravidelné zprávy o kvalitě údajů.

- **Dopady na další právní nástroje**

Společně se souvisejícím návrhem zavádí tento návrh nařízení inovace, které budou vyžadovat změny jiných právních nástrojů:

- nařízení (EU) č. 2016/399 (Schengenský hraniční kodex)
- nařízení (EU) č. 2017/2226 (nařízení o EES)
- nařízení (ES) č. 767/2008 (nařízení o VIS)
- rozhodnutí Rady 2004/512/ES (rozhodnutí o VIS)

- rozhodnutí Rady 2008/633/SVV (rozhodnutí o VIS / přístupu donucovacích orgánů)
- [nařízení o ETIAS]
- [nařízení o Eurodacu]
- [nařízení o SIS]
- [nařízení o ECRIS-TCN včetně příslušných ustanovení nařízení (EU) 2016/1624 (nařízení o Evropské pohraniční a pobřežní stráži)]
- [nařízení o agentuře eu-LISA]

Stávající návrh a jeho související návrh zahrnují podrobná ustanovení týkající se nezbytných změn právních nástrojů, které jsou v současnosti stabilními texty v podobě přijaté spolunormotvůrci: Schengenský hraniční kodex, nařízení o EES, nařízení o VIS, rozhodnutí Rady 2008/633/SVV a rozhodnutí Rady 2004/512/ES.

Ostatní uvedené nástroje (nařízení o ETIAS, Eurodacu, SIS, ECRIS-TCN, eu-LISA) se momentálně projednávají v Evropském parlamentu a Radě. U těchto nástrojů proto v této fázi není možné stanovit nezbytné změny. Komise předloží tyto změny pro každý z těchto nástrojů do dvou týdnů po dosažení politické shody o každém z příslušných návrhů nařízení.

- **Soulad s platnými předpisy v této oblasti politiky**

Tento návrh spadá do rámce širšího procesu, který byl zahájen sdělením z dubna 2016 nazvaným *Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost* a následnou činností expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu. Cíle návrhu jsou tři:

a) posílit a maximalizovat přínosy **stávajících informačních systémů**;

b) vyřešit informační mezery zřízením nových informačních systémů;

c) posílit interoperabilitu mezi těmito systémy.

V souvislosti s prvním cílem přijala Komise v prosinci 2016 návrhy na další posílení stávajícího Schengenského informačního systému (SIS)[25]. V případě systému Eurodac došlo k urychlení jednání o revidovaném právním základě v návaznosti na návrh Komise z května 2016[26]. Rovněž se připravuje návrh nového právního základu pro vízový informační systém (VIS), který bude předložen ve druhém čtvrtletí roku 2018.

Co se týče druhého cíle, jednání o návrhu Komise z dubna 2016 týkajícího se zřízení Systému vstupu/výstupu (EES)[27] byla uzavřena již v červenci 2017, kdy spolunormotvůrci dosáhli politické shody, kterou Evropský parlament potvrdil v říjnu 2017 a Rada ji formálně přijala v listopadu 2017. Právní základ nabude účinnosti v prosinci 2017. Jednání o návrhu z listopadu 2016 o zřízení evropského systému pro cestovní informace a povolení (ETIAS)[28] již byla zahájena a jejich uzavření se očekává v nadcházejících měsících. V červnu 2017 Komise navrhla právní základ pro vyřešení další informační mezery: Evropský informační systém

[25] COM(2016) 883 final.
[26] COM(2016) 272 final.
[27] COM(2016) 194 final.
[28] COM(2016) 731 final.

rejstříků trestů pro státní příslušníky třetích zemí (systém ECRIS-TCN)[29]. I v tomto případě spolunormotvůrci uvedli, že cílem je včasné přijetí tohoto právního základu.

Stávající návrh se zaměřuje na třetí cíl uvedený ve sdělení z dubna 2016.

- **Soulad s ostatními politikami Unie v oblasti spravedlnosti a vnitřních věcí**

Tento návrh společně se souvisejícím návrhem vychází z Evropského programu pro migraci a následných sdělení, včetně sdělení o ochraně a posílení Schengenu,[30] Evropského programu pro bezpečnost[31] a činnosti Komise a jejích zpráv o pokroku s ohledem na vytváření účinné a skutečné bezpečnostní unie, a je s nimi v souladu[32]. Je v souladu s ostatními politikami Unie, zejména pokud jde o oblast:

- Vnitřní bezpečnost: Evropský program pro bezpečnost uvádí, že zásadní význam pro předcházení přeshraniční trestné činnosti a terorismu mají společné vysoké normy správy hranic. Tento návrh dále přispívá k dosahování vysoké úrovně vnitřní bezpečnosti tím, že orgánům nabízí způsob jak získat rychlý, bezproblémový, systematický a řízený přístup k informacím, které požadují.
- Azyl: návrh zahrnuje systém Eurodac jako jeden z ústředních systémů EU, na které se má vztahovat interoperabilita.
- Správa vnějších hranic a bezpečnost: tento návrh posiluje systémy SIS a VIS, které přispívají k účinné kontrole vnějších hranic Unie, jakož i budoucí systém EES a navrhovaný systém ETIAS a ECRIS-TCN.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

- **Právní základ**

Hlavním právním základem budou následující články Smlouvy o fungování Evropské unie: 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).

Podle čl. 16 odst. 2 má Unie pravomoc přijímat opatření související s ochranou fyzických osob při zpracovávání osobních údajů orgány, institucemi a jinými subjekty Unie a členskými státy, pokud vykonávají činnosti spadající do oblasti působnosti práva Unie, a pravidla o volném pohybu těchto údajů. Podle článku 74 může Rada přijímat opatření, kterými zajistí správní spolupráci mezi příslušnými útvary členských států v oblasti spravedlnosti, svobody a bezpečnosti. Podle článku 78 má Unie pravomoc přijímat opatření týkající se společného evropského azylového systému. Podle čl. 79 odst. 2 písm. c) má Unie pravomoc přijímat opatření v oblasti nedovoleného přistěhovalectví a nedovoleného pobytu. Podle čl. 82 odst. 1 písm. d) a čl. 87 odst. 2 písm. a) má Unie rovněž pravomoc přijímat opatření k posílení policejní a justiční spolupráce týkající se shromažďování, uchovávání, zpracovávání, analýzy a výměny příslušných informací. Podle čl. 85 odst. 1 a čl. 88 odst. 2 má Unie pravomoc vymezit úkoly Eurojustu a Europolu.

[29] COM(2017) 344 final.
[30] COM(2017) 570 final.
[31] COM(2015) 185 final.
[32] COM(2016) 230 final.

- **Subsidiarita**

Svoboda pohybu v rámci EU vyžaduje účinnou správu vnějších hranic Unie, aby byla zajištěna bezpečnost. Členské státy se tedy dohodly na společném řešení těchto výzev, které spočívá zejména ve sdílení informací prostřednictvím centralizovaných systémů EU v oblasti spravedlnosti a vnitřních věcí. To potvrzuje řada závěrů, které přijala Evropská rada a Rada, především po roce 2015.

Neprovádění kontrol na vnitřních hranicích vyžaduje účinnou správu vnějších hranic schengenského prostoru, kde každý členský stát nebo země přidružená k Schengenu musí kontrolovat vnější hranici v zájmu ostatních států Schengenu. Žádný členský stát tedy nedokáže samostatně bojovat proti nelegální migraci a přeshraniční trestné činnosti. Státní příslušníci třetích zemí, kteří vstupují do prostoru bez kontrol na vnitřních hranicích, se v tomto prostoru mohou volně pohybovat. V prostoru bez vnitřních hranic je třeba při potírání nelegální migrace a mezinárodní trestné činnosti a terorismu, což zahrnuje odhalování podvodného zneužití totožnosti, jednat společně, přičemž řešení tohoto problému je možné pouze na úrovni EU.

Klíčové společné informační systémy na úrovni EU jsou již v provozu nebo se zavádějí. Aby se zlepšila interoperabilita mezi těmito informačními systémy, je nutné opatření na úrovni EU. Jádrem tohoto návrhu je lepší účinnost a používání centralizovaných systémů spravovaných agenturou eu-LISA. Z důvodu rozsahu, účinků a dopadu plánovaných kroků lze základních cílů účinně a systematicky dosáhnout pouze na úrovni EU.

- **Proporcionalita**

Jak je podrobně uvedeno v posouzení dopadů, které je přiloženo k tomuto návrhu nařízení, politická rozhodnutí přijatá v tomto návrhu se považují za přiměřená. Nepřekračují rámec toho, co je nezbytné k dosažení dohodnutých cílů.

Evropský vyhledávací portál (ESP) je nezbytným nástrojem pro posílení oprávněného používání stávajících a budoucích informačních systémů EU. Dopad ESP v oblasti zpracování údajů je velmi omezený. Nebude ukládat žádné údaje vyjma informací, které se týkají různých uživatelských profilů ESP a údajů a informačních systémů, k nimž mají uživatelé přístup, a sledování jejich využívání prostřednictvím protokolů. Úloha ESP jako zprostředkovatele zpráv, pomocníka a facilitátora je přiměřená, nezbytná a omezená, pokud jde o vyhledávání a přístupová práva podle právních základů týkajících se informačních systémů a podle navrhovaného nařízení o interoperabilitě.

Sdílená služba pro porovnávání biometrických údajů (sdílená BMS) je nezbytná pro fungování ESP, společného úložiště údajů o totožnosti a detektoru vícenásobné totožnosti a usnadňuje používání a údržbu stávajících a budoucích příslušných informačních systémů EU. Její funkce umožňuje účinné, plynulé a systematické vyhledávání biometrických údajů z různých zdrojů. Biometrické údaje se ukládají a uchovávají v základních systémech. Sdílená BMS vytváří šablony, ale skutečná zobrazení se vymažou. Údaje se tedy ukládají jen na jednom místě, pouze jednou.

Společné úložiště údajů o totožnosti (CIR) je nezbytné pro dosažení účelu správného zjištění totožnosti státních příslušníků třetí země, např. během kontroly totožnosti v schengenském prostoru. CIR také podporuje fungování detektoru vícenásobné totožnosti, a je tedy nezbytnou složkou pro dosažení dvojího cíle, a sice usnadnění kontrol totožnosti cestujících v dobré víře a potírání podvodného zneužívání totožnosti. Přístup do CIR pro tento

účel je omezený na ty uživatele, kteří dané informace potřebují k plnění svých úkolů (což vyžaduje, aby se tyto kontroly staly novým vedlejším účelem systémů Eurodac, VIS, budoucího systému EES, navrhovaného systému ETIAS a navrhovaného systému ECRIS-TCN). Zpracování údajů je přísně omezeno na to, co je nezbytné k dosažení tohoto cíle, budou zavedeny příslušné záruky, které zajistí, že budou dodržována přístupová práva a že v CIR budou ukládány jen nezbytně nutné údaje. Aby bylo možné zajistit minimalizaci údajů a předcházet jejich neodůvodněnému zdvojování, CIR uchovává požadované biografické údaje z každého ze základních systémů – ty jsou ukládány, doplňovány, pozměňovány a vymazávány v souladu s příslušným právním základem –, aniž by je kopíroval. Podmínky uchovávání údajů jsou v plné shodě s ustanoveními o uchovávání údajů základních informačních systémů, které údaje o totožnosti poskytují.

Detektor vícenásobné totožnosti (MID) je nezbytný nástroj pro odhalování vícenásobných totožností s dvojím účelem, kterým je usnadnění kontrol totožnosti cestujících v dobré víře a potírání podvodného zneužití totožnosti. MID bude obsahovat propojení mezi jednotlivci, kteří se vyskytují ve více než jednom ústředním informačním systému s přísným omezením na údaje nezbytné k ověření, zda daná osoba je registrována pod různými biografickými totožnostmi v různých systémech zákonně či nezákonně, ale také k vyjasnění, zda dvě osoby s podobnými biografickými údaji nemohou být tatáž osoba. Zpracování údajů v rámci MID a sdílené BMS za účelem propojení individuálních souborů mezi jednotlivými systémy se udržuje na absolutním minimu. MID bude obsahovat záruky proti možné diskriminaci nebo nepříznivým rozhodnutím ve vztahu k osobám s více zákonnými totožnostmi.

- **Volba nástroje**

Navrhuje se nařízení Evropského parlamentu a Rady. Navrhovaný právní předpis řeší přímo provoz ústředních informačních systémů EU pro ochranu hranic a bezpečnost, přičemž všechny tyto systémy byly zřízeny, nebo se jejich zřízení navrhuje, na základě nařízení. Agentura eu-LISA, která bude odpovědná za návrh a vývoj a později také za technickou správu uvedených složek, je rovněž zřízena na základě nařízení. Nařízení je tedy vhodným nástrojem.

3. VÝSLEDKY KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

- **Veřejné konzultace**

Při přípravě tohoto návrhu Komise v červenci 2017 zahájila veřejnou konzultaci s cílem získat stanoviska zúčastněných stran na téma interoperability. V rámci konzultace bylo obdrženo 18 odpovědí od různých zúčastněných stran, včetně vlád členských států, organizací ze soukromého sektoru, dalších organizací, jako jsou nevládní organizace a skupiny odborníků (think tank), jakož i od soukromých občanů[33]. Odpovědi obecně vyjadřovaly podporu základním principům tohoto návrhu týkajícího se interoperability. Velká většina respondentů se shodla na tom, že problémy identifikované v rámci veřejné konzultace byly správně určeny a že cíle, které si balíček týkající se interoperability stanoví, jsou správné. Respondenti se zejména domnívali, že by možnosti nastíněné v konzultačním dokumentu:

- pomohly zaměstnancům v terénu získat přístup k informacím, které potřebují;
- předešly zdvojování údajů, snížily překrývání a odhalily nesrovnalosti v údajích;

[33] Další podrobnosti jsou obsaženy v souhrnné zprávě přiložené k posouzení dopadu.

- pomohly spolehlivěji identifikovat osoby – včetně osob s vícenásobnými totožnostmi – a omezily podvodné zneužívání totožnosti.

Jednoznačná většina respondentů podpořila každou z navrhovaných možností a označila je za nezbytné pro dosažení cílů této iniciativy, přičemž ve svých odpovědích respondenti zdůrazňovali potřebu důrazných a jasných opatření na ochranu údajů, zejména pokud jde o přístup k informacím uloženým v systémech a uchovávání údajů, jakož i potřebu aktuálních, vysoce kvalitních údajů v systémech a opatření, která toto zaručí.

Všechny tyto záležitosti byly při přípravě tohoto návrhu zohledněny.

- **Průzkum Eurobarometr**

V červnu 2017 se uspořádal zvláštní průzkum Eurobarometr[34], který ukázal, že strategie EU zaměřená na sdílení informací na úrovni EU za účelem boje proti trestné činnosti a terorismu má širokou podporu veřejnosti: takřka všichni respondenti (92 %) se shodují na tom, že vnitrostátní orgány by měly sdílet informace s orgány jiných členských států s cílem lépe bojovat proti trestné činnosti a terorismu.

Jednoznačná většina (69 %) respondentů vyjádřila názor, že policie a jiné vnitrostátní donucovací orgány by měly systematicky sdílet informace s dalšími zeměmi EU. Ve všech členských státech se většina respondentů domnívá, že informace by měly být sdíleny v každém případě.

- **Expertní skupina na vysoké úrovni pro informační systémy a interoperabilitu**

Jak již bylo zmíněno v úvodu, tento návrh vychází z doporučení **expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu**[35]. Tato skupina byla zřízena v červnu 2016 s cílem řešit právní, technické a provozní otázky dostupných možností pro dosažení interoperability mezi ústředními systémy EU pro ochranu hranic a bezpečnost. Skupina obecně a komplexně posoudila architekturu správy údajů pro účely správy hranic a prosazování práva, přičemž rovněž zohlednila příslušné úlohy celních orgánů, jejich povinnosti a systémy.

Skupinu tvořili odborníci z členských států a zemí přidružených k Schengenu, jakož i z agentur EU (eu-LISA, Europol, Evropský podpůrný úřad pro otázky azylu, Evropská agentura pro pohraniční a pobřežní stráž a Agentura EU pro základní práva). Protiteroristický koordinátor EU a evropský inspektor ochrany údajů se skupiny zúčastnili jako řádní členové. Kromě toho se jako pozorovatelé zúčastnili zástupci sekretariátu výboru Evropského parlamentu pro občanské svobody, spravedlnost a vnitřní věci a generálního sekretariátu Rady.

Závěrečná zpráva expertní skupiny na vysoké úrovni byla zveřejněna v květnu 2017[36]. Zdůraznila potřebu jednat s cílem řešit strukturální nedostatky zjištěné ve sdělení z dubna 2016. Přinesla řadu doporučení pro posílení a vývoj informačních systémů EU a interoperability. Došla k závěru, že **pro dosažení interoperability je nezbytné a technicky**

[34] *Zpráva o postojích Evropanů k otázkám bezpečnosti* analyzuje výsledky zvláštního průzkumu veřejného mínění Eurobarometr (464b) ohledně celkového povědomí, zkušeností a vnímání občanů, pokud jde o bezpečnost. Tento průzkum provedla síť TNS Political & Social v 28 členských státech v období 13. až 26. června 2017. Dotázáno bylo 28 093 občanů EU z různých sociálních a demografických kategorií.

[35] Rozhodnutí Komise ze dne 17. června 2016 o zřízení expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu – 2016/C 257/03.

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

možné pracovat na vytvoření Evropského vyhledávacího portálu, sdílené služby pro porovnávání biometrických údajů a společného úložiště údajů o totožnosti, které v zásadě mohou mít jak operativní přínosy, tak být vytvořeny v souladu s požadavky na ochranu údajů. Skupina také doporučila zvážit dodatečnou možnost dvoufázového postupu pro přístup pro účely prosazování práva na základě funkce označení pozitivního nálezu.

Tento návrh nařízení také reaguje na doporučení expertní skupiny na vysoké úrovni týkajících se kvality údajů, univerzálního formátu pro zprávy (UMF) a zřízení datového skladu [zde uváděného jako centrální úložiště pro účely podávání zpráv a statistiky (CRRS)].

Čtvrtá složka pro interoperabilitu navrhovaná v tomto návrhu nařízení (detektor vícenásobné totožnosti) nebyla určena expertní skupinou na vysoké úrovni, ale je výsledkem dodatečné technické analýzy a posouzení proporcionality, které provedla Komise.

- **Technické studie**

Na podporu přípravy návrhu byly zadány tři studie. Společnost Unisys na základě smlouvy s Komisí předložila zprávu o studii proveditelnosti týkající se Evropského vyhledávacího portálu. Agentura eu-LISA nechala vypracovat technickou zprávu u společnosti Gartner (společně se společností Unisys) na podporu vývoje sdílené služby pro porovnávání biometrických údajů. Společnost PWC dodala Komisi technickou zprávu o společném úložišti údajů o totožnosti.

- **Posouzení dopadů**

Tento návrh je podložen posouzením dopadů, které uvedeno v doprovodném pracovním dokumentu útvarů Komise SWD(2017) XXX.

Výbor pro kontrolu regulace přezkoumal návrh posouzení dopadů na svém zasedání dne 6. prosince 2017 a dne 8. prosince k němu vydal stanovisko (kladné s výhradami) s tím, že posouzení dopadů je nutno upravit tak, aby byla zapracována doporučení výboru ke konkrétním otázkám. Tato doporučení se týkala především dodatečných opatření v rámci upřednostňované možnosti, a sice zefektivnění stávajících přístupových práv koncových uživatelů v informačních systémech EU, a dále objasnění souvisejících záruk pro ochranu údajů a základní práva. Druhá hlavní připomínka se týkala vyjasnění integrace Schengenského informačního systému v rámci druhé možnosti, včetně účinnosti a nákladů na usnadnění jejího porovnání se třetí upřednostňovanou možností. Komise v reakci na tyto hlavní připomínky a rovněž s cílem řešit další poznámky výboru své posouzení dopadů aktualizovala.

Posouzení dopadů se zabývalo otázkou, zda a jak lze dosáhnout jednotlivých vymezených cílů s využitím jedné či více technických složek určených expertní skupinou na vysoké úrovni a prostřednictvím následné analýzy. Podle potřeby se posouzení dopadů zaměřilo i na dílčí možnosti nezbytné pro splnění těchto cílů při současném dodržení rámce ochrany údajů. Z posouzení dopadů vyplynulo, že:

- Má-li být splněn cíl poskytnout oprávněným uživatelům rychlý, bezproblémový, systematický a řízený přístup k příslušným informačním systémům, je třeba vytvořit Evropský vyhledávací portál (ESP) opírající se o sdílenou službu pro porovnávání biometrických údajů (sdílená BMS), aby bylo možné pokrýt všechny databáze.

- Má-li být splněn cíl usnadnit kontroly totožnosti státních příslušníků třetích zemí na území členského státu ze strany oprávněných pracovníků, je třeba zřídit společné úložiště údajů o totožnosti (CIR) obsahující minimální soubor údajů o totožnosti a opírající se o tutéž sdílenou BMS.
- Má-li být splněn cíl spočívající v odhalování vícenásobných totožností propojených se stejným souborem biometrických údajů, a to s dvojím účelem, kterým je usnadnění kontrol totožnosti cestujících v dobré víře a potírání podvodného zneužití totožnosti, je třeba vytvořit detektor vícenásobné totožnosti (MID), který bude obsahovat propojení mezi různými totožnostmi mezi systémy.
- Má-li být splněn cíl usnadnit a zefektivnit přístup donucovacích orgánů k informačním systémům, jež neslouží k prosazování práva, pro účely prevence, vyšetřování, odhalování nebo stíhání závažné trestné činnosti a terorismu, je třeba, aby společné úložiště údajů o totožnosti (CIR) obsahovalo funkci označení pozitivního nálezu.

Jelikož musí být splněny všechny cíle, **úplným řešením je kombinace ESP, CIR (s funkcí označení pozitivního nálezu) a MID, přičemž všechny tyto systémy se budou opírat o sdílenou BMS**.

Významným pozitivním dopadem bude zlepšení správy hranic a zvýšení vnitřní bezpečnosti v rámci Evropské unie. Nové složky zefektivní a urychlí přístup vnitrostátních orgánů k nezbytným informacím, jakož i zjištění totožnosti státních příslušníků třetích zemí. Umožní orgánům vytvářet vzájemná propojení s již existujícími důležitými informacemi o fyzických osobách během hraničních kontrol, při posuzování žádostí o víza nebo azyl a při práci policie. Umožní se tím přístup k informacím, které mohou podpořit přijímání spolehlivých rozhodnutí, ať už se týkají vyšetřování závažné trestné činnosti a terorismu, nebo migrace a azylu. Ačkoli se návrhy přímo nedotýkají státních příslušníků EU (navrhovaná opatření se primárně zaměřují na státní příslušníky třetích zemí, jejichž údaje jsou registrovány v některém centralizovaném informačním systému EU), očekává se, že posílí důvěru veřejnosti tím, že zajistí, aby vyhotovení a používání systémů zvýšilo bezpečnost občanů EU.

Bezprostřední finanční a hospodářské dopady návrhu budou omezeny na návrh, vývoj a provoz nových zařízení. Náklady budou hrazeny z rozpočtu EU a orgánů členských států, které budou systémy provozovat. Dopad na cestovní ruch bude pozitivní, jelikož navrhovaná opatření zvýší bezpečnost Evropské unie a měla by také urychlit hraniční kontroly. Obdobně se očekává pozitivní dopad na letiště, námořní přístavy a dopravce, a to zejména z důvodu urychlení hraničních kontrol.

- **Základní práva**

Posouzení dopadů se zaměřilo zejména na dopady navrhovaných opatření na základní práva, zvláště pak na právo na ochranu údajů.

V souladu s Listinou základních práv EU, kterou jsou orgány EU a členské státy při provádění práva EU vázány (čl. 51 odst. 1 Listiny), musejí být příležitosti, které interoperabilita nabízí jako opatření pro posílení bezpečnosti a ochranu vnějších hranic, v rovnováze s povinností zajistit, aby zásahy do základních práv, k nimž může dojít v souvislosti s novým prostředím využívajícím interoperabilitu, byly omezené na přísně nezbytné minimum, aby se podařilo splnit sledované cíle obecného zájmu, a to v souladu se zásadou proporcionality (čl. 52 odst. 1 Listiny).

Navrhovaná řešení interoperability jsou doplňkovými složkami pro stávající systémy. Jako takové tedy nezmění rovnováhu, kterou již zaručuje každý ze stávajících ústředních systémů ve vazbě na jejich kladný dopad na základní práva.

Interoperabilita nicméně může mít další, nepřímý dopad na řadu základních práv. Správné zjištění totožnosti osoby má pozitivní dopad na právo na respektování soukromého života a zejména na právo na totožnost (článek 7 Listiny), jelikož může pomoci zabránit záměně totožností. Na druhé straně lze považovat provádění kontrol na základě biometrických údajů za narušování práva na lidskou důstojnost (zejména tehdy, pokud je vnímáno jako ponižující) (článek 1). V rámci průzkumu[37] realizovaném Agenturou EU pro základní práva byli respondenti dotazováni, zda si myslí, že poskytování biometrických údajů v kontextu hraničních kontrol je pro ně ponižující. Podle většiny respondentů tomu tak není.

Navrhované složky interoperability nabízejí příležitost přijímat cílená preventivní opatření na posílení bezpečnosti. Jako takové mohou přispět k ochraně práva na život (článek 2 Listiny), což zahrnuje pozitivní povinnost orgánů přijímat preventivní operativní opatření za účelem ochrany osob, jejichž život je v ohrožení, pokud vědí nebo by měly vědět o existenci bezprostředního ohrožení[38], jakož dodržování zákaz otroctví a nucené práce (článek 5). Díky spolehlivému, přístupnějšímu a jednoduššímu zjišťování totožnosti může interoperabilita usnadnit hledání pohřešovaných dětí nebo dětí, které jsou oběťmi obchodování s lidmi, a usnadnit rychlou a cílenou reakci.

Spolehlivé, přístupnější a jednodušší zjišťování totožnosti může také přispět k účinnému zajištění práva na azyl (článek 18 Listiny) a zákazu navracení (článek 19 Listiny). Interoperabilita by ve skutečnosti mohla zabránit tomu, aby žadatelé o azyl byli nezákonně zadrženi, zajištěni a nezákonně vyhoštěni. Prostřednictvím interoperability by se také usnadnilo zjištění podvodných zneužití totožnosti. Snížila by se také nutnost sdílet údaje a informace o žadatelích o azyl se třetími zeměmi (zvláště se zeměmi původu) pro účely stanovení totožnosti osoby a získání cestovních dokladů, což by mohlo potenciálně dotčenou osobu ohrozit.

- **Ochrana osobních údajů**

Vzhledem k tomu, že se interoperabilita týká osobních údajů, bude mít zejména dopad na právo na ochranu osobních údajů. Toto právo zaručuje článek 8 Listiny a článek 16 Smlouvy o fungování Evropské unie a dále pak článek 8 Evropské úmluvy o lidských právech. Jak zdůraznil Soudní dvůr EU[39], právo na ochranu osobních údajů není právem absolutním, avšak musí být posuzováno v souvislosti se svou funkcí ve společnosti[40]. Ochrana údajů je úzce spjata s respektováním soukromého a rodinného života, které je zakotveno v článku 7 Listiny.

---

[37] *FRA survey in the framework of the eu-LISA pilot on smart borders — travellers' views on and experiences of smart borders* (Průzkum FRA v rámci pilotního projektu agentury eu-LISA o inteligentních hranicích – názory cestujících na inteligentní hranice a zkušenosti s nimi), zpráva Agentury EU pro základní práva: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

[38] Evropský soud pro lidská práva, Osman v. Spojenému království, stížnost č. 87/1997/871/1083, 28. října 1998, bod 116.

[39] Rozsudek Soudního dvora ze dne 9. listopadu 2010, spojené věci C-92/09 a C-93/09, Volker a Markus Schecke a Eifert, Sb. rozh. 2010, s. I 0000.

[40] V souladu s čl. 52 odst. 1 Listiny mohou být omezení výkonu práva na ochranu údajů zavedena tehdy, pokud jsou tato omezení stanovena zákonem a respektují podstatu těchto práv a svobod. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Evropské unie, nebo potřebě ochrany práv a svobod druhých.

V souladu s obecným nařízením o ochraně osobních údajů[41] nesmí být volný pohyb údajů v rámci EU omezován z důvodů ochrany osobních údajů. Je nicméně nutné dodržet několik zásad. Má-li být jakékoli omezení výkonu základních práv chráněných Listinou zákonné, musí splňovat následující kritéria stanovená v jejím článku 52 odst. 1:

- musí být stanoveno zákonem;
- musí respektovat podstatu práv;
- musí skutečně vyhovovat cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého;
- musí být nezbytné; a
- musí dodržovat zásadu proporcionality.

Stávající návrh zapracovává všechna tato pravidla na ochranu osobních údajů, jak je podrobně uvedeno v přiloženém posouzení dopadů. Návrh vychází ze zásad záměrné a standardní ochrany osobních údajů. Zahrnuje veškerá příslušná ustanovení týkající se omezení zpracování údajů na míru nezbytně nutnou pro navrhovaný účel a poskytování přístupu k údajům pouze takovým subjektům, které je „musí znát“. Lhůty pro uchovávání údajů (v příslušných případech) jsou přiměřené a omezené. Přístup k údajům je vyhrazen výhradně řádně oprávněným pracovníkům orgánů členských států nebo subjektů EU, které jsou příslušné pro konkrétní účely každého informačního systému, v rozsahu potřebném ke splnění jejich úkolů v souladu s těmito účely.

4. ROZPOČTOVÉ DŮSLEDKY

Rozpočtové důsledky jsou uvedeny v přiloženém finančním výkazu. Ten pokrývá zbývající období stávajícího víceletého finančního rámce (do roku 2020) a sedm let následujícího období (2021–2027). Navrhovaný rozpočet na roky 2021 a dále je přiložen pro ilustraci a nepředjímá příští víceletý finanční rámec.

Zavedení tohoto návrhu bude vyžadovat přidělení rozpočtových prostředků na:

1) **vývoj** a integraci uvedených čtyř složek interoperability a centrálního úložiště pro účely podávání zpráv a statistiky agenturou eu-LISA a jejich následnou **údržbu a provoz**;

2) **migraci údajů** do sdílené služby pro porovnávání biometrických údajů (sdílená BMS) a společného úložiště údajů o totožnosti (CIR). V případě sdílené BMS bude nutné znovu vytvořit biometrické šablony odpovídajících údajů ze všech tří systémů, které biometrické údaje v současnosti používají (SIS, VIS a Eurodac). V případě CIR bude nutné migrovat prvky osobních údajů z VIS do CIR a možná propojení zjištěná mezi totožnostmi v SIS, VIS a Eurodacu bude nutné potvrdit. Zejména tento poslední proces je náročný na zdroje;

3) aktualizaci **vnitrostátního jednotného rozhraní** (NUI) ze strany agentury eu-LISA, které je již součástí nařízení o EES a má se stát obecnou složkou, jež umožní výměnu zpráv mezi členskými státy a ústředními systémy;

[41] 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).

4) **začlenění vnitrostátních systémů členských států** do NUI, které umožní předávání zpráv vyměňovaných se systémem CIR / detektorem vícenásobné totožnosti prostřednictvím Evropského vyhledávacího portálu;

5) **odbornou přípravu** zaměřenou na využívání složek interoperability koncovými uživateli, rovněž prostřednictvím Agentury Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva (CEPOL).

Složky interoperability jsou vytvářeny a udržovány jako program. Zatímco Evropský vyhledávací portál (ESP) a detektor vícenásobné totožnosti jsou zcela nové složky, sdílená BMS a CIR jsou společně s centrálním úložištěm pro účely podávání zpráv a statistiky (CRRS) sdílené složky, které spojují existující uložené údaje (nebo ty, které budou uloženy) ve stávajících nebo nových systémech, s příslušnými aktuálními rozpočtovými odhady.

ESP bude zavádět stávající známá rozhraní ve vztahu k systémům SIS, VIS a Eurodac a ve vhodné době se rozšíří na nové systémy.

ESP budou členské státy a agentury využívat pomocí rozhraní vycházejícího z univerzálního formátu pro zprávy (UMF). Toto nové rozhraní bude vyžadovat vývoj, úpravy, integraci a testování ze strany členských států, eu-LISA, Europolu a Evropské agentury pro pohraniční a pobřežní stráž. ESP by využíval koncepce vnitrostátního jednotného rozhraní (NUI) zavedeného pro systém EES, což by snížilo úsilí o integraci.

ESP bude znamenat další náklady pro Europol, aby bylo možné zpřístupnit rozhraní QUEST pro používání zahrnující údaje se základním stupněm ochrany (BPL).

Základ **sdílené BMS** bude *de facto* zřízen tím, že se vytvoří nový systém EES, jelikož ten zahrne zdaleka největší objem nových biometrických údajů. Požadovaný rozpočet byl vyhrazen v rámci právního nástroje EES. Přidávání dalších biometrických údajů ze systémů VIS, SIS a Eurodac do sdílené BMS představuje další náklady spojené zejména s migrací stávajících údajů. Rozpočet na všechny tři systémy se v této souvislosti odhaduje na 10 milionů EUR. Přidávání nových biometrických údajů z navrhovaného systému ECRIS-TCN představuje omezené dodatečné náklady, které lze pokrýt z fondů vyhrazených v rámci navrhovaného právního nástroje ECRIS-TCN na zřízení systému automatizované identifikace otisků prstů ECRIS-TCN.

Společné úložiště údajů o totožnosti bude zřízeno při vytvoření budoucího systému EES a bude dále rozšířeno při vývoji navrhovaného systému ETIAS. Prostředky spojené s uchováváním a vyhledáváním těchto údajů byly zařazeny do rozpočtu vyhrazeného v rámci právních nástrojů budoucího systému EES a navrhovaného systému ETIAS. Přidávání nových biografických údajů ze systému Eurodac a z navrhovaného systému ECRIS-TCN představuje drobné další náklady, které již byly vyhrazeny v rámci právních nástrojů systému Eurodac a navrhovaného systému ECRIS-TCN.

Celkový rozpočet požadovaný pro období devíti let (2019–2027) dosahuje výše 424,7 milionu EUR a pokrývá následující položky:

1) rozpočet 225 milionů EUR pro agenturu eu-LISA, který pokrývá celkové náklady na vývoj programu, jenž zajistí všech pět složek interoperability (68,3 milionu EUR), náklady na údržbu od okamžiku, kdy budou složky k dispozici, až do roku 2027 (56,1 milionu EUR), zvláštní rozpočet 25 milionů EUR pro migraci údajů ze stávajících systémů do sdílené BMS a další náklady na aktualizaci NUI, síť,

odbornou přípravu a zasedání. Zvláštní rozpočet 18,7 milionu EUR pokrývá náklady na modernizaci a provoz ECRIS-TCN v režimu vysoké dostupnosti od roku 2022.

2) Rozpočet 136,3 milionu EUR na pokrytí změn, které musí členské státy učinit ve svých vnitrostátních systémech, aby mohly používat složky interoperability, jednotné vnitrostátní rozhraní realizované agenturou eu-LISA, a rozpočet na odbornou přípravu významného počtu koncových uživatelů.

3) Rozpočet 48,9 milionu EUR pro Europol na pokrytí modernizace IT systémů Europolu tak, aby se přizpůsobily objemu zpráv, které budou zpracovávány, a vyšší výkonnostní úrovni[42]. Složky interoperability budou využívány systémem ETIAS pro účely nahlížení do údajů Europolu.

4) Rozpočet 4,8 milionu EUR pro Evropskou agenturu pro pohraniční a pobřežní stráž na hostování týmu specialistů, kteří budou během jednoho roku potvrzovat propojení mezi totožnostmi od okamžiku spuštění detektoru vícenásobné totožnosti.

5) Rozpočet 2,0 milionu EUR pro Agenturu Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva (CEPOL) na pokrytí příprav a průběhu vzdělávání pro provozní zaměstnance.

6) Zajištění 7,7 milionu EUR pro GŘ HOME na pokrytí omezeného navýšení počtu zaměstnanců a souvisejících nákladů ve fázi vývoje jednotlivých složek, jelikož během tohoto období bude muset Komise plnit rovněž další úkoly a převezme odpovědnost za výbor zabývající se univerzálním formátem zpráv.

Nařízení o Fondu pro vnitřní bezpečnost (ISF) – hranice je finanční nástroj, do nějž byl začleněn rozpočet na provedení iniciativy týkající se interoperability. V článku 5 písm. b) se stanoví, že 791 milionů EUR je nutno čerpat v rámci programu na vývoj systémů informačních technologií založených na stávajících a/nebo nových systémech na podporu řízení migračních toků přes vnější hranice Unie, s výhradou přijetí příslušných právních předpisů Unie a v souladu s podmínkami stanovenými v článku 15 odst. 5. Z těchto 791 milionů EUR je vyhrazeno 480,2 milionu EUR na vývoj systému EES, 210 milionů EUR na systém ETIAS a 67,9 milionu EUR na revizi systému SIS. Zbývající částka (32,9 milionu EUR) má být znovu přerozdělena prostřednictvím mechanismů ISF-hranice. Současný návrh požaduje na stávající období víceletého finančního rámce (2019/20) částku 32,1 milionu EUR, kterou lze pokrýt ze zbývajícího rozpočtu.

5. DOPLŇUJÍCÍ INFORMACE

- **Plány provádění a monitorování, hodnocení a podávání zpráv**

Agentura eu-LISA odpovídá za provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva. V rámci této funkce je pověřena provozem a technickým a operativním zlepšováním stávajících systémů a vývojem již naplánovaných budoucích systémů. Podle navrhovaného nařízení vymezí agentura eu-LISA návrh fyzické architektury složek interoperability, tyto složky vyvine, realizuje a konečně zajistí jejich tzv. hosting. Příslušné složky budou zaváděny postupně ve spojení s rozvojem základních systémů.

[42] Současná kapacita Europolu, pokud jde o zpracování informací, není v souladu se značným objemem (průměrně 100 000 vyhledávání za den) a se zkrácenou dobou odezvy, které bude vyžadovat systém ETIAS.

Komise zajistí, aby byly zavedeny systémy pro monitorování vývoje a fungování všech čtyř složek (Evropského vyhledávacího portálu, sdílené služby pro porovnávání biometrických údajů, společného úložiště údajů o totožnosti, detektoru vícenásobné totožnosti) a centrálního úložiště pro účely podávání zpráv a statistiky, a bude provádět jejich hodnocení vzhledem k hlavním politickým cílům. Čtyři roky po zavedení a zprovoznění uvedených funkčních prvků a poté každé čtyři roky by měla agentura eu-LISA Evropskému parlamentu, Radě a Komisi předložit zprávu o technickém fungování složek interoperability. Kromě toho pět let po zavedení a zprovoznění uvedených funkčních prvků a poté každé čtyři roky by měla Komise vypracovat celkové zhodnocení příslušných složek, které zahrne přímý nebo nepřímý dopad těchto složek a jejich praktického provádění na základní práva. Agentura eu-LISA by měla prozkoumat dosažené výsledky s ohledem na cíle a zhodnotit trvající platnost výchozího principu a případné důsledky pro budoucí možnosti. Komise by měla předkládat hodnotící zprávy Evropskému parlamentu a Radě.

- **Podrobné vysvětlení konkrétních ustanovení návrhu**

Kapitola I obsahuje obecná ustanovení tohoto nařízení. Vysvětluje: zásady, z nichž nařízení vychází; složky jím zřizované; cíle, které interoperabilita sleduje; oblast působnosti tohoto nařízení; definice pojmů použitých v tomto nařízení a zásadu zákazu diskriminace v souvislosti se zpracováním údajů podle tohoto nařízení.

Kapitola II obsahuje ustanovení týkající se Evropského vyhledávacího portálu (ESP). Tato kapitola se týká zřízení ESP a jeho technické architektury, které má vyvinout agentura eu-LISA. Vymezuje cíl ESP a určuje osoby, které jej mohou používat, jakož i způsob, jak mají tento systém používat v souladu se stávajícími přístupovými právy pro každý z ústředních systémů. Kapitola obsahuje ustanovení, podle kterého má eu-LISA vytvořit uživatelské profily pro jednotlivé kategorie uživatelů. Tato kapitola stanoví postup, jak bude ESP vyhledávat v ústředních systémech, a stanoví obsah a formát odpovědí uživatelům. Kapitola II rovněž stanoví, že agentura eu-LISA bude vést protokoly o všech operacích zpracovávání údajů, a stanoví nouzový postup v případě, že ESP nebude mít přístup k jednomu či více ústředních systémům.

Kapitola III obsahuje ustanovení o sdílené službě pro porovnávání biometrických údajů (sdílená BMS). Tato kapitola se týká zřízení sdílené BMS a její technické architektury, které má vyvinout agentura eu-LISA. Vymezuje cíl sdílené BMS a stanoví, jaké údaje se ukládají. Objasňuje vztah mezi sdílenou BMS a ostatními složkami. Kapitola III rovněž stanoví, že údaje budou ve sdílené BMS uchovávány jen po dobu, kdy jsou uloženy v příslušném ústředním systému, a stanoví, že agentura eu-LISA bude vést protokoly o všech zpracovatelských operacích.

Kapitola IV obsahuje ustanovení o společném úložišti údajů o totožnosti (CIR). Tato kapitola se týká zřízení CIR a jeho technické architektury, které má vyvinout agentura eu-LISA. Vymezuje cíl CIR a objasňuje, jaké údaje se mají uchovávat a jak, včetně ustanovení o zajištění kvality uchovávaných údajů. Tato kapitola stanoví, že CIR vytvoří na základě údajů v ústředních systémech individuální soubory a že tyto soubory se budou aktualizovat v souladu se změnami v jednotlivých ústředních systémech. Kapitola IV rovněž upřesňuje, jak bude CIR fungovat ve vztahu k detektoru vícenásobné totožnosti. Tato kapitola určuje osoby, které mohou mít přístup do CIR, a jak mohou nahlížet do údajů v souladu s přístupovými právy, a obsahuje další konkrétní ustanovení v případě, že se jedná o přístup pro účely zjištění totožnosti nebo o přístup – jakožto první krok dvoufázového postupu – do systému EES, VIS, ETIAS a Eurodac prostřednictvím CIR pro účely prosazování práva. Kapitola IV také stanoví, že agentura eu-LISA bude vést protokoly o všech zpracovatelských operacích, které se CIR týkají.

Kapitola V obsahuje ustanovení o detektoru vícenásobné totožnosti (MID). Tato kapitola se týká zřízení MID a jeho technické architektury, které má vyvinout agentura eu-LISA. Objasňuje cíl MID a upravuje použití MID v souladu s právy na přístup do jednotlivých ústředních systémů. Kapitola V stanoví, kdy a jak bude MID spouštět vyhledávání za účelem odhalení vícenásobných totožností, jaké jsou možné výsledky a jaká následná opatření je třeba přijmout, včetně využití manuálního ověřování. Je zde uvedena klasifikace typů propojení, které mohou vyplynout z vyhledávání v závislosti na tom, zda výsledek ukazuje jedinou totožnost, vícenásobnou totožnost nebo údaje sdílené totožnosti. Tato kapitola stanoví, že MID bude ukládat propojené údaje uchovávané v ústředních systémech, zatímco data zůstanou ve dvou či více jednotlivých ústředních systémech. Kapitola V také stanoví, že agentura eu-LISA bude vést záznamy o všech zpracovatelských operacích, které se MID týkají.

Kapitola VI obsahuje ustanovení o opatřeních na podporu interoperability. Stanoví zlepšení kvalitu údajů, zřízení univerzálního formátu zpráv jako společné normy pro výměnu informací na podporu interoperability a vytvoření centrálního úložiště pro účely podávání zpráv a statistiky.

Kapitola VII souvisí s ochranou údajů. Tato kapitola obsahuje ustanovení, která zaručují, že zpracování údajů podle tohoto nařízení bude zákonné a řádné v souladu s ustanoveními nařízení č. 45/2001. Vysvětluje, kdo bude zpracovatelem údajů pro jednotlivá opatření interoperability navrhovaná v tomto nařízení, stanoví opatření, která má přijmout agentura eu-LISA a orgány členských států s cílem zajistit bezpečnost zpracování údajů, důvěrnost údajů, náležité řešení bezpečnostních incidentů a správné monitorování souladu s opatřeními uvedenými v tomto nařízení. Tato kapitola rovněž obsahuje ustanovení o právech subjektů údajů, včetně práva být informován o tom, že údaje, které se jich týkají, byly uloženy a zpracovány podle tohoto nařízení, a práva na přístup, opravu a vymazání osobních údajů, které byly uloženy a zpracovány podle tohoto nařízení. Tato kapitola dále stanoví zásadu, že údaje zpracované podle tohoto nařízení nesmějí být přenášeny ani zpřístupňovány žádné třetí zemi, mezinárodní organizaci ani soukromé straně, a to s výjimkou Interpolu pro některé konkrétní účely, a údajů obdržených od Europolu přes Evropský vyhledávací portál, kde platí pravidla nařízení 2016/794 o následném zpracování údajů. Na závěr tato kapitola obsahuje ustanovení týkající se dohledu a auditů v souvislosti s ochranou údajů.

Kapitola VIII stanoví oblasti odpovědnosti agentury eu-LISA před zahájením navrhovaných opatření a po zavedení navrhovaných opatření, jakož i povinnosti členských států, Europolu a ústřední jednotky ETIAS.

Kapitola IX stanoví podrobnosti týkající se: požadavků na statistiku a podávání zpráv v souvislosti s údaji zpracovávanými podle tohoto nařízení; nutných přechodných opatření; ujednání ohledně nákladů plynoucích z tohoto nařízení; požadavků na oznámení; postupu pro zavedení opatření navrhovaných v tomto nařízení; ujednání ohledně správy a řízení včetně zřízení výboru a poradní skupiny, odpovědnosti agentury eu-LISA za odbornou přípravu a praktických pokynů na podporu zavádění a správy složek interoperability; postupů pro monitorování a hodnocení opatření navrhovaných v tomto nařízení; a ustanovení o vstupu tohoto nařízení v platnost.

2017/0352 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU (policejní a justiční spolupráce, azyl a migrace)

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 a 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,

po konzultaci s evropským inspektorem ochrany údajů,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru,[43]

s ohledem na stanovisko Výboru regionů,[44]

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Ve svém sdělení ze dne 6. dubna 2016 nazvaném *Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost*[45] Komise zdůraznila potřebu zlepšit unijní architekturu správy údajů pro správu hranic a bezpečnost. Toto sdělení zahájilo proces směřující k dosažení interoperability informačních systémů 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[46] 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 pracovního programu Komise na rok 2017[47] požadoval Evropský parlament návrhy na zdokonalení a rozvoj stávajících informačních systémů, vyřešení mezer v informacích a pokrok směrem k interoperabilitě a také návrhy na závazné sdílení informací na úrovni EU doprovázené nezbytnými zárukami v oblasti ochrany údajů.

---

[43] Úř. věst. C, , s. .

[44]

[45] COM(2016) 205, 6.4.2016.

[46] Plán ze dne 6. června 2016 na posílení výměny informací a správy informací včetně řešení interoperability v oblasti spravedlnosti a vnitřních věcí – 9368/1/16 REV 1.

[47] Usnesení Evropského parlamentu ze dne 6. července 2016 o strategických prioritách pracovního programu Komise na rok 2017 (2016/2773(RSP)).

(4) Evropská rada dne 15. prosince 2016[48] vyzvala k dalšímu zlepšování interoperability informačních systémů a databází EU.

(5) Ve své závěrečné zprávě ze dne 11. května 2017[49] 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 v zásadě obě řešení mohou 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, kterého bylo dosaženo v úsilí o vytvoření účinné a skutečně bezpečnostní Unie*[50], 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.

(7) Ve svých závěrech ze dne 9. června 2017[51] o dalším postupu s cílem zlepšit výměnu informací a zajistit interoperabilitu informačních systémů EU Rada vyzvala Komisi, aby usilovala o řešení interoperability tak, jak je navrhla expertní skupina na vysoké úrovni.

(8) Evropská rada dne 23. června 2017[52] zdůraznila potřebu zlepšovat interoperabilitu databází a vyzvala Komisi, aby za účelem přijetí návrhů předložených expertní skupinou na vysoké úrovni pro interoperabilitu co nejdříve připravila návrh právního aktu.

(9) Aby bylo možné zlepšit správu vnějších hranic, přispět k prevenci a potírání nelegální migrace 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, je třeba zajistit interoperabilitu informačních systémů EU, zejména [Systému vstupu/výstupu (EES)], Vízového informačního systému (VIS), [evropského systému pro cestovní informace a povolení (ETIAS)], systému Eurodac, Schengenského informačního systému (SIS) a [Evropského informačního systému rejstříků trestů pro státní příslušníky třetích zemí (ECRIS-TCN)], aby se tyto informační systémy EU a jejich data navzájem doplňovaly. 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, přispět k boji proti podvodnému zneužití totožnosti, zlepšit a harmonizovat požadavky na kvalitu údajů příslušných informačních systémů EU, usnadnit technické a provozní provádění stávajících i budoucích informačních systémů EU ze strany členských států, posílit a zjednodušit záruky pro zabezpečení a ochranu údajů vztahující se na příslušné informační systémy EU, zefektivnit přístup pro účely prosazování práva k systémům

---

48 http://www.consilium.europa.eu/cs/press/press-releases/2016/12/15/euco-conclusions-final/.
49 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.
50 COM(2017) 261 final, 16.5.2017.
51 http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf.
52 Závěry Evropské rady ze zasedání ve dnech 22.–23. června 2017.

EES, VIS, [ETIAS] a Eurodac a podpořit účely systémů EES, VIS, [ETIAS], Eurodac, SIS a [systému ECRIS-TCN].

(11) Složky interoperability by měly pokrývat systém EES, VIS, [ETIAS], Eurodac, SIS a [systém ECRIS-TCN]. Rovněž by měly zahrnovat údaje Europolu v takovém rozsahu, aby se umožnilo souběžné vyhledávání v těchto údajích a v uvedených informačních systémech EU.

(12) Složky interoperability by se měly týkat osob, ve vztahu k nimž mohou být osobní údaje zpracovávány v informačních systémech EU a Europolem, zejména jde o státní příslušníky třetích zemí, jejichž osobní údaje jsou zpracovávány v informačních systémech EU a Europolem, a o občany EU, jejichž osobní údaje zpracovává systém SIS a Europol.

(13) Evropský vyhledávací portál (ESP) by měl být zřízen s cílem technicky usnadnit rychlý, bezproblémový, účinný, systematický a řízený přístup k informačním systémům EU, k údajům Europolu a k databázím Interpolu, který orgány členských států a subjekty EU potřebují v souladu se svými přístupovými právy a pro účely plnění svých úkolů, a rovněž s cílem podpořit účely systémů EES, VIS, [ETIAS], Eurodac, SIS, [systému ECRIS-TCN] a údajů Europolu. ESP by měl umožnit souběžné vyhledávání ve všech příslušných informačních systémech EU, jakož i v údajích Europolu a databázích Interpolu a měl by fungovat jako jednotný portál nebo „zprostředkovatel zpráv“ pro vyhledávání v různých ústředních systémech, přičemž by plynule při plném dodržování požadavků na kontrolu přístupu a ochranu údajů základních systémů získával nezbytné informace.

(14) Koncoví uživatelé evropského vyhledávacího portálu (ESP), kteří mají práva na přístup k údajům Europolu na základě nařízení Evropského parlamentu a Rady (EU) 2016/794[53], by měli mít možnost vyhledávat v údajích Europolu souběžně s údaji v informačních systémech EU, k nimž mají přístup. Jakékoli další zpracovávání údajů následně po 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.

(15) Evropský vyhledávací portál (ESP) by měl být vyvinut a nastaven tak, aby neumožňoval používat pro vyhledávání datová pole, která se netýkají osob nebo cestovních dokladů nebo která se nevyskytují v některém informačním systému EU, v údajích Europolu nebo v databázi Interpolu.

(16) Aby se zajistilo rychlé a systematické využívání všech informačních systémů EU, měl by se Evropský vyhledávací portál (ESP) používat pro vyhledávání ve společném úložišti údajů o totožnosti, v systémech EES, VIS, [ETIAS], Eurodac a [systému 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 orgány 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 systémech Interpolu, čímž doplní stávající vyhrazená rozhraní.

(17) Biometrické údaje, jako jsou otisky prstů a zobrazení obličeje, jsou jedinečné, a pro zjištění totožnosti osob tedy mnohem spolehlivější než alfanumerické údaje. Sdílená

[53] 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).

služba pro porovnávání biometrických údajů (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 mohou být registrovány v různých databázích, a to porovnáním jejich biometrických údajů z různých systémů a s využitím jedinečné technické složky namísto pěti různých složek v každém ze základních systémů. Tím, že bude využívat jedinou technologickou složku namísto jednotlivých složek v každém ze základních systémů, měla by sdílená BMS přispět k bezpečnosti a znamenat rovněž přínos z hlediska financí, údržby a provozu. Všechny systémy automatizované identifikace otisků prstů včetně těch, které se v současnosti používají pro systémy Eurodac, VIS a SIS, využívají biometrické šablony složené z údajů odvozených extrakcí rysů ze skutečných biometrických vzorků. Sdílená BMS by měla všechny tyto biometrické šablony seskupit a uložit na jediném místě, čímž se usnadní porovnávání mezi systémy na základě biometrických údajů a umožní značné úspory z rozsahu při vývoji a údržbě ústředních systémů EU.

(18) Biometrické údaje představují citlivé osobní údaje. Toto nařízení by mělo rovněž stanovit základy a záruky pro zpracování takových údajů pro účely zjištění jediné totožnosti dotčených osob.

(19) Aby byly systémy zřízené nařízením Evropského parlamentu a Rady (EU) 2017/2226[54], nařízením Evropského parlamentu a Rady (ES) č. 767/2008[55], [nařízením o ETIAS] pro správu hranic Unie, systém zřízený [nařízením o Eurodacu] pro účely zjištění totožnosti žadatelů o mezinárodní ochranu a boje proti nelegální migraci a systém zřízený [nařízením o systému ECRIS-TCN] účinné, musí se opírat o přesné zjištění totožnosti státních příslušníků třetích zemí, jejichž osobní údaje jsou v nich uloženy.

(20) Společné úložiště údajů o totožnosti (CIR) by tedy mělo usnadnit a pomáhat při správném zjištění totožnosti osob registrovaných v systémech EES, VIS, [ETIAS], Eurodac a [v systému ECRIS-TCN].

(21) Osobní údaje uložené v těchto informačních systémech EU se mohou vztahovat k různým nebo neúplně uvedeným totožnostem téže osoby. Členské státy mají k dispozici účinné možnosti ke zjištění totožnosti svých obyvatel nebo registrovaných osob s trvalým povolením k pobytu na jejich území, to však neplatí pro státní příslušníky třetích zemí. Interoperabilita mezi informačními systémy EU by měla přispět ke správnému zjištění totožnosti státních příslušníků třetích zemí. Společné úložiště údajů o totožnosti (CIR) by mělo uchovávat osobní údaje státních příslušníků třetích zemí, které se vyskytují v systémech a které jsou nezbytné pro umožnění přesnějšího zjištění totožnosti těchto jednotlivců, a obsahovat tedy údaje o jejich totožnosti, cestovních dokladech a biometrické údaje, bez ohledu na to, v jakém systému byly údaje původně shromážděny. V CIR by se měly uchovávat pouze ty osobní údaje, které jsou k provedení přesné kontroly totožnosti nezbytně nutné. Osobní údaje zaznamenané v systému CIR by neměly být uchovávány déle, než je

[54] 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 (nařízení o EES) (Úř. věst. L 327, 9.12.2017, s. 20–82).

[55] 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).

nezbytně nutné pro účely základních systémů, a měly by se automaticky vymazat, když se údaj vymaže v základním systému, a to v souladu s jejich logickým oddělením.

(22) Tento nový postup zpracování spočívající v ukládání takových údajů do společného úložiště údajů o totožnosti (CIR), namísto jejich ukládání v jednotlivých oddělených systémech, je nezbytný, má-li se zvýšit přesnost zjišťování totožnosti, kterou umožňuje automatizované porovnávání a zjišťování shod těchto údajů. Skutečnost, že údaje o totožnosti a biometrické údaje státních příslušníků třetích zemí jsou ukládány do CIR, by nijak neměla zpomalit zpracování údajů pro účely nařízení o EES, o VIS, o ETIAS, o Eurodacu nebo o systému ECRIS-TCN, jelikož CIR by měl být novou sdílenou složkou těchto základních systémů.

(23) V této souvislosti je nutné ve společném úložišti údajů o totožnosti (CIR) vytvořit pro každou osobu, která je zaznamenána v systému EES, VIS, ETIAS, Eurodac nebo ECRIS-TCN, individuální soubor, aby bylo možné splnit účel správné zjištění totožnosti státních příslušníků třetích zemí v schengenském prostoru a podpořit detektor vícenásobné totožnosti s dvojím cílem, kterým je usnadnění kontrol totožnosti cestujících v dobré víře a potírání podvodného zneužití totožnosti. Individuální soubor by měl všechny možné totožnosti spojené s určitou osobou uložit na jednom místě a zpřístupnit je řádně oprávněným koncovým uživatelům.

(24) Společné úložiště údajů o totožnosti (CIR) by tedy mělo podpořit fungování detektoru vícenásobné totožnosti a usnadnit a urychlit přístup donucovacích orgánů k informačním systémům EU, které nejsou zřízeny výlučně pro účely prevence, vyšetřování, odhalování či stíhání závažné trestné činnosti.

(25) Společné úložiště údajů o totožnosti (CIR) by mělo zahrnovat sdílenou schránku pro údaje o totožnosti a biometrické údaje státních příslušníků třetích zemí registrovaných v systémech EES, VIS, [ETIAS], Eurodac a [ECRIS-TCN], která by fungovala jako sdílená složka mezi uvedenými systémy pro účely ukládání těchto údajů a umožňovala by jejich vyhledávání.

(26) Všechny záznamy ve společném úložišti údajů o totožnosti (CIR) by měly být logicky odděleny prostřednictvím automatizovaného označování každého záznamu uvádějícího základní systém, který je jeho vlastníkem. Toto označení by se mělo používat při kontrole přístupu do CIR a na jeho základě by se měl přístup k danému záznamu buď umožnit, nebo zamítnout.

(27) Orgány členských států příslušné pro prevenci a potírání nelegální migrace a příslušné orgány ve smyslu čl. 3 bodu 7 směrnice 2016/680 by měly být pro účely správného zjištění totožnosti osob oprávněny vyhledávat ve společném úložišti údajů o totožnosti (CIR) na základě biometrických údajů, které o dané osobě získaly během kontroly totožnosti.

(28) 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 uložené ve společném úložišti údajů o totožnosti (CIR), měly by mít orgány členského státu umožněno nahlížet do údajů o totožnosti této osoby uložených v CIR, aniž by bylo jakkoli uvedeno, kterému informačnímu systému EU tyto údaje patří.

(29) Členské státy by měly přijmout vnitrostátní legislativní opatření, kterými určí orgány příslušné pro provádění kontrol totožnosti s využitím společného úložiště údajů o

totožnosti (CIR) a stanoví postupy, podmínky a kritéria těchto kontrol v souladu se zásadou proporcionality. Vnitrostátní legislativní opatření by měla zejména stanovit pravomoc, která členům těchto orgánů umožní shromažďovat biometrické údaje při kontrole totožnosti osoby za její přítomnosti.

(30) Toto nařízení by mělo také zavést novou možnost jednoduššího přístupu určených donucovacích orgánů členských států a Europolu k jiným údajům, než jsou údaje o totožnosti, uloženým v systémech EES, VIS, [ETIAS] nebo Eurodac. Údaje, a to včetně údajů jiných než údaje o totožnosti obsažených v těchto systémech, mohou být v konkrétních případech nezbytné pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů nebo závažných trestných činů.

(31) Plný přístup, který je nezbytný pro účely prevence, odhalování a vyšetřování teroristických trestných činů nebo jiných závažných trestných činů, k potřebným údajům obsaženým v informačních systémech EU, jiným než příslušné údaje o totožnosti zahrnuté do společného úložiště údajů o totožnosti (CIR) a získané na základě biometrických údajů dané osoby shromážděných při kontrole totožnosti, by se měl i nadále řídit ustanoveními příslušných právních nástrojů. Určené donucovací orgány 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 oprávněný určeným orgánem by tedy měl mít právo vidět, ve kterém z informačních systémů EU jsou údaje odpovídající zadanému dotazu zaznamenány. Dotčený systém by se tak označil na základě automatizovaného ověření výskytu pozitivního nálezu v systému (tzv. funkce označení pozitivního nálezu).

(32) Z protokolů o vyhledávání ve společném úložišti údajů o totožnosti by měl vyplynout účel tohoto 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 takové vyhledávání bylo zahájeno pro účely prevence, odhalování a vyšetřování teroristických trestných činů nebo jiných závažných trestných činů.

(33) Vyhledávání ve společném úložišti údajů o totožnosti (CIR) prováděné určenými orgány členských států a Europolem s cílem obdržet odpověď s označením pozitivního nálezu a uvedením informace, že údaj je zaznamenán v systému EES, VIS, [ETIAS] nebo Eurodac, vyžaduje automatizované zpracovávání osobních údajů. Funkce označení pozitivního nálezu by neodhalila osobní údaje dotčené osoby, pouze by ukázala, že některé z jejích údajů jsou uložené v jednom ze systémů. Oprávněný koncový uživatel by neměl přijmout žádné nepříznivé rozhodnutí v souvislosti s dotčenou osobou pouze na základě prostého výskytu označení pozitivního nálezu. Přístup koncového uživatele funkce označení shody by tedy znamenal velmi omezené narušení práva na ochranu osobních údajů dotčené osoby, nicméně by bylo nutné umožnit určenému orgánu a Europolu, aby se s žádostí o přístup k osobním údajům mohly účinněji obracet přímo na systém, který byl označen jako systém, jenž takové údaje obsahuje.

(34) Tento dvoufázový postup pro nahlížení do údajů je zvláště cenný v případech, kdy podezřelý z teroristického trestného činu nebo jiného závažného trestného činu, pachatel nebo údajná oběť takového trestného činu nejsou známi. V těchto případech by společné úložiště údajů o totožnosti (CIR) mělo umožnit identifikovat informační systém, kterému je dotčená osoba známa, během jediného vyhledávání. Tím, že se v uvedených případech uloží povinnost používat tento nový postup při přístupu k systémům pro účely prosazování práva, neměly by se již na přístup k osobním údajům

uloženým v systémech EES, VIS, [ETIAS] a Eurodac vztahovat požadavky předchozího vyhledávání ve vnitrostátních databázích nebo spouštění předchozího vyhledávání v systému automatizované identifikace otisků prstů jiných členských států podle rozhodnutí 2008/615/SVV. Zásada předchozího vyhledávání účinně omezuje možnost orgánů členských států nahlížet do systémů pro odůvodněné účely prosazování práva, a mohla by tedy být příčinou promarněné příležitosti ke zjištění nezbytných informací. Požadavky na předchozí vyhledávání ve vnitrostátních databázích a spuštění předchozího vyhledávání v systému automatizované identifikace otisků prstů jiných členských států podle rozhodnutí 2008/615/SVV by měly přestat platit až poté, co bude zprovozněna alternativní záruka dvoufázového postupu pro přístup k systémům pro účely prosazování práva prostřednictvím CIR.

(35) Detektor vícenásobné totožnosti (MID) by měl být zřízen s cílem podpořit fungování společného úložiště údajů o totožnosti a účely systémů EES, VIS, [ETIAS], Eurodac, SIS a [systém 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.

(36) Dosažení cílů informačních systémů EU v současné době ztěžuje skutečnost, že orgány využívající tyto systémy nemají možnost dostatečně spolehlivě ověřit totožnost státních příslušníků třetích zemí, jejichž údaje jsou uloženy v různých systémech. Důvodem je to, že soubor údajů o totožnosti uložený v jednom konkrétním systému může být podvodný, nesprávný či neúplný, přičemž tyto podvodné, nesprávné nebo neúplné údaje o totožnosti 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 státních příslušníků třetích zemí pro tyto účely.

(37) Detektor vícenásobné totožnosti (MID) by měl vytvářet a uchovávat propojení mezi údaji v různých informačních systémech EU pro účely odhalování více totožností, a to s dvojím účelem, kterým je usnadnění kontrol totožnosti cestujících v dobré víře a potírání podvodného zneužití totožnosti. MID by měl obsahovat pouze propojení mezi jednotlivci, kteří se vyskytují ve více než jednom informačním systému EU, s přísným omezením na údaje nutné k ověření, zda je daná osoba registrována pod různými biografickými totožnostmi v různých systémech zákonně či nezákonně, nebo k určení, zda dvě osoby s podobnými biografickými údaji nemohou být tatáž osoba. Zpracování údajů prostřednictvím Evropského vyhledávacího portálu (ESP) a sdílené služby pro porovnávání biometrických údajů (sdílená BMS) za účelem propojení individuálních souborů v jednotlivých systémech by mělo zůstat naprosto minimální, a omezí se tedy na zjištění vícenásobných totožností v okamžiku, kdy se do jednoho z informačních systémů, které jsou zapojené do společného úložiště údajů o totožnosti a do SIS, doplní nové údaje. MID by měl obsahovat záruky proti možné diskriminaci nebo nepříznivým rozhodnutím pro osoby s vícenásobnými zákonnými totožnostmi.

(38) 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. 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, účinným prováděním azylové a vízové politiky Unie a bojem proti nelegální migraci.

(39) Evropský vyhledávací portál (ESP) a sdílená služba pro porovnávání biometrických údajů (sdílená BMS) by měly porovnávat údaje o osobách ve společném úložišti údajů o totožnosti (CIR) a SIS, jestliže dojde k vytvoření nových záznamů ze strany vnitrostátního orgánu nebo orgánu EU. 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 dokázat identifikovat stejné nebo podobné údaje o státním příslušníkovi třetí země 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 vznikaly nepříznivé důsledky pro dotčeného státního příslušníka třetí země.

(40) Vnitrostátní orgán nebo subjekt EU, který údaj zaznamenal do příslušného informačního systému EU, by měl tato propojení potvrdit nebo změnit. Takový orgán by měl mít přístup k údajům uloženým ve společném úložišti údajů o totožnosti (CIR) nebo SIS a v detektoru vícenásobné totožnosti (MID) pro účely manuálního ověření totožnosti.

(41) Přístup k detektoru vícenásobné totožnosti (MID) ze strany orgánů členských států a subjektů EU, které mají přístup alespoň do jednoho informačního systému EU zapojeného do společného úložiště údajů o totožnosti (CIR) nebo do SIS, by měl být omezen na tzv. červená propojení, kde propojené údaje sdílejí totožné biometrické údaje, ale údaje o totožnosti se liší, a orgán odpovědný za ověření různých totožností dospěl k závěru, že odkazují nezákonně na tutéž osobu, nebo pokud propojené údaje obsahují podobné údaje o totožnosti a orgán odpovědný za ověření různých totožností dospěl k závěru, že odkazují nezákonně na tutéž osobu. Pokud propojené údaje o totožnosti nejsou podobné, mělo by se vytvořit žluté propojení a na základě manuálního ověření následně toto propojení potvrdit, nebo příslušným způsobem změnit jeho barvu.

(42) Manuální ověření vícenásobných totožností by mělo být zajištěno orgánem, který vytváří nebo aktualizuje údaje, jež vedly k pozitivnímu nálezu a následně k propojení s údaji, které jsou již uloženy v jiném informačním systému EU. Orgán odpovědný za ověření vícenásobných totožností by měl posoudit, zda jde o zákonné či nezákonné vícenásobné totožnosti. Takové posouzení by mělo proběhnout pokud možno za přítomnosti daného státního příslušníka třetí země a, je-li to nutné, mělo by se požadovat další vysvětlení nebo doplňující informace. Takové posouzení by mělo proběhnout neprodleně, v souladu s právními požadavky na přesnost informací podle unijního a vnitrostátního práva.

(43) U propojení získaných v souvislosti s Schengenským informačním systémem (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, záznamů o osobách pořízených pro účely skrytých nebo zvláštních kontrol nebo záznamů o neznámých hledaných osobách, by měla být orgánem odpovědným za ověření vícenásobných 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 v jednom z ostatních informačních systémů EU. Vytvoření propojení s údaji SIS by mělo proběhnout bez ohledu na činnosti, které je nutno vykonat v souladu s [nařízením o SIS].

(44) Agentura eu-LISA by měla zavést automatizované mechanismy kontroly kvality údajů a společné ukazatele kvality údajů. Měla by odpovídat za vývoj ústřední monitorovací kapacity kvality údajů a vypracovávat zprávy o kvalitě údajů a o analýze údajů s cílem zlepšit kontrolu nad prováděním a uplatňováním informačních systémů EU ze strany členských států. Společné ukazatele kvality 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.

(45) 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.

(46) Univerzální formát pro zprávy (UMF) by měl nastavit normu strukturované přeshraniční výměny informací mezi informačními systémy, orgány a/nebo organizacemi v oblasti spravedlnosti 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.

(47) Mělo by být zřízeno centrální úložiště pro účely podávání zpráv a statistiky (CRRS) s cílem vytvářet mezisystémové statistické údaje a analytické zprávy pro politické, provozní účely a pro účely kvality údajů. Agentura eu-LISA by měla zřídit, zavést a ve svých technických zařízeních umístit CRRS, v němž by byly zahrnuty anonymní statistické údaje z výše uvedených systémů, společného úložiště údajů o totožnosti, detektoru vícenásobné totožnosti a sdílené služby pro porovnávání biometrických údajů (sdílená BMS). Údaje obsažené v CRRS by neměly umožnit zjištění totožnosti jednotlivců. Agentura eu-LISA by měla zajistit anonymizaci údajů a anonymizované údaje zaznamenat do CRRS. Anonymizace údajů by měla probíhat automatizovaně a zaměstnancům agentury eu-LISA by neměl být udělen přímý přístup k žádným osobním údajům uloženým v informačních systémech EU nebo ve složkách interoperability.

(48) Na zpracování osobních údajů podle tohoto nařízení ze strany vnitrostátních orgánů by se mělo vztahovat nařízení (EU) 2016/679, pokud takové zpracování neprovádějí určené orgány nebo ústřední přístupové body členských států pro účely prevence, odhalování nebo vyšetřování teroristických trestných činů nebo jiných závažných trestných činů, kdy by měla platit směrnice Evropského parlamentu a Rady (EU) 2016/680.

(49) Zvláštní ustanovení o ochraně údajů [nařízení o Eurodacu], [nařízení o SIS v oblasti prosazování práva], [nařízení o SIS v oblasti navracení neoprávněně pobývajících osob] a [nařízení o systému ECRIS-TCN] by měla platit pro zpracování osobních údajů v těchto příslušných systémech.

(50) Nařízení Evropského parlamentu a Rady (ES) č. 45/2001[56] by se mělo vztahovat na zpracování osobních údajů agenturou eu-LISA a dalšími orgány a subjekty Unie při plnění jejich povinností podle tohoto nařízení, aniž je tím dotčeno ustanovení nařízení (EU) 2016/794, na které by se mělo vztahovat na zpracování osobních údajů Europolem.

(51) Vnitrostátní dozorové úřady zřízené v souladu s [nařízením (EU) 2016/679] by měly sledovat zákonnost zpracování osobních údajů členskými státy, zatímco evropský inspektor ochrany údajů, ustavený nařízením (ES) č. 45/2001, by měl sledovat činnost orgánů a institucí Unie související se zpracováním osobních údajů. Evropský inspektor ochrany údajů a dozorové úřady by měly při sledování zpracovávání osobních údajů složkami interoperability vzájemně spolupracovat.

(52) „(...) V souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001 byl konzultován evropský inspektor ochrany údajů, který své stanovisko předložil dne …“

(53) Pokud jde o důvěrnost, měla by se na úředníky a ostatní zaměstnance Evropské unie zaměstnané a pracující v souvislosti se SIS vztahovat příslušná ustanovení služebního řádu úředníků Evropské unie a pracovního řádu ostatních zaměstnanců Unie.

(54) Členské státy i agentura eu-LISA by měly udržovat 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 neporušenosti údajů, pokud jde o vývoj, návrh a správu složek interoperability.

(55) Na podporu účelů statistik a podávání zpráv je nutné udělit přístup oprávněným pracovníkům příslušných orgánů institucí a subjektů Unie určených v tomto nařízení k vyhledávání určitých údajů v souvislosti s určitými složkami interoperability bez umožnění zjištění totožnosti osob.

(56) Aby se příslušné orgány a subjekty EU mohly přizpůsobit novým požadavkům kladeným na používání Evropského vyhledávacího portálu (ESP), je nutné stanovit přechodné období. Obdobně pak, aby se zajistilo soudržné a optimální fungování detektoru vícenásobné totožnosti (MID), je nutné stanovit přechodná opatření pro spuštění jeho provozu.

(57) Náklady na vývoj složek interoperability plánované v rámci současného víceletého finančního rámce jsou nižší než zbývající částka v rozpočtu vyčleněná pro inteligentní hranice v nařízení Evropského parlamentu a Rady (EU) č. 515/2014[57]. Proto by toto nařízení mělo v souladu s čl. 5 odst. 5 písm. b) nařízení (EU) č. 515/2014 přerozdělit částku, která je v současnosti přidělena na vývoj systémů informačních technologií podporujících řízení migračních toků přes vnější hranice.

(58) Za účelem doplnění určitých podrobných technických aspektů tohoto nařízení by měla být Komisi svěřena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování Evropské unie, pokud jde o profily uživatelů Evropského vyhledávacího portálu (ESP) a obsah a formát jeho odpovědí. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni,

[56] 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).

[57] 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).

a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů[58]. Aby se zajistila rovná účast na vypracovávání aktů v přenesené pravomoci, měly by Evropský parlament a Rada obdržet všechny dokumenty současně s odborníky členských států a jejich odborníci by měli mít systematicky přístup na zasedání odborných skupin Komise, které se přípravou aktů v přenesené pravomoci zabývají.

(59) Za účelem zajištění jednotných podmínek k provedení tohoto nařízení by měly být Komisi svěřeny prováděcí pravomoci, aby mohla přijímat podrobná pravidla pro: mechanismy a postupy automatizované kontroly kvality a ukazatele kontroly kvality; vývoj normy UMF; postupy pro určení případů podobných totožností; provoz centrálního úložiště pro účely podávání zpráv a statistiky; a postup spolupráce v případě bezpečnostních incidentů. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011[59].

(60) Na zpracování údajů Europolu prováděné pro účely tohoto nařízení se vztahuje nařízení 2016/794.

(61) Tímto nařízením není dotčeno použití směrnice 2004/38/ES.

(62) V souladu s článkem 3 Dohody mezi Evropským společenstvím a Dánským královstvím o kritériích a mechanismech pro určení státu příslušného pro posuzování žádosti o azyl podané v Dánsku nebo jiném členském státě Evropské unie a o systému „Eurodac“ pro porovnávání otisků prstů za účelem účinného uplatňování Dublinské úmluvy[60] má Dánsko Komisi oznámit, zda provede obsah tohoto nařízení v rozsahu, v jakém se týká Eurodacu [sítě DubliNet, automatizovaného systému pro registraci a sledování a přidělovacího mechanismu pro žádosti o mezinárodní ochranu uvedeného v článku 44 nařízení (EU) XX/20XX, 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 (přepracované znění)].

(63) V rozsahu, v jakém se ustanovení tohoto nařízení týkají SIS ve smyslu úpravy obsažené v rozhodnutí 2007/533/SVV, 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 (dále jen „Protokol o schengenském *acquis*“), a v souladu s čl. 8 odst. 2 rozhodnutí Rady 2000/365/ES ze dne 29. května 2000 o žádosti Spojeného království Velké Británie a Severního Irska, aby se na ně vztahovala některá ustanovení schengenského *acquis*[61]. Dále pak v rozsahu, v jakém se ustanovení tohoto nařízení týkají Eurodacu [a automatizovaného systému pro registraci a sledování a přidělovacího mechanismu pro žádosti o mezinárodní ochranu uvedeného v článku 44 nařízení (EU) XX/XX, 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 (přepracované znění)], Spojené království může oznámit předsedovi Rady, že se chce

---

58 http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.L_.2016.123.01.0001.01.ENG.

59 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).

60

61

účastnit přijímání a uplatňování tohoto nařízení v souladu s článkem 3 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 (Protokol o postavení Spojeného království a Irska). V rozsahu, v jakém se ustanovení nařízení týkají systému ECRIS-TCN, v souladu s články 1 a 2 a čl. 4a odst. 1 Protokolu č. 21 o postavení Spojeného království a Irska s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o EU a Smlouvě o fungování EU, se Spojené království neúčastní přijímání tohoto nařízení a není pro ně závazné ani použitelné. V souladu s článkem 3 a čl. 4a odst. 1 Protokolu č. 21 může Spojené království oznámit, že se chce zúčastnit přijímání tohoto nařízení.

(64) V rozsahu, v jakém se ustanovení nařízení týkají SIS ve smyslu úpravy obsažené v rozhodnutí 2007/533/SVV, se Irsko účastní 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 (dále jen „Protokol o schengenském *acquis*“), a v souladu s čl. 6 odst. 2 rozhodnutí Rady 2002/192/ES ze dne 28. února 2002 o žádosti Irska, aby se na ně vztahovala některá ustanovení schengenského *acquis*[62]. Dále pak v rozsahu, v jakém se ustanovení tohoto nařízení týkají Eurodacu [a automatizovaného systému pro registraci a sledování a přidělovací mechanismus pro žádosti o mezinárodní ochranu uvedeného v článku 44 nařízení (EU) XX/XX, 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 (přepracované znění)], může Irsko oznámit předsedovi Rady, že se chce účastnit přijímání a uplatňování tohoto nařízení v souladu s článkem 3 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 (dále jen „Protokol o postavení Spojeného království a Irska“). V rozsahu, v jakém se ustanovení nařízení týkají systému ECRIS-TCN, v souladu s články 1 a 2 a čl. 4a odst. 1 Protokolu č. 21 o postavení Spojeného království a Irska s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o EU a Smlouvě o fungování EU, se Irsko neúčastní přijímání tohoto nařízení a není pro ně závazné ani použitelné. V souladu s článkem 3 a čl. 4a odst. 1 Protokolu č. 21 může Irsko oznámit, že se chce účastnit přijímání tohoto nařízení.

(65) Co se týče Islandu a Norska, pokud jde o Eurodac [a automatizovaný systém pro registraci a sledování a přidělovací mechanismus pro žádosti o mezinárodní ochranu uvedený v článku 44 nařízení (EU) XX/XX, 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 (přepracované znění)], toto nařízení představuje nové opatření ve smyslu Dohody mezi Evropským společenstvím a Islandskou republikou a Norským královstvím o kritériích a mechanismech určení státu příslušného pro posuzování žádosti o azyl podané v některém z členských států nebo na Islandu nebo v Norsku.

(66) Co se týče Švýcarska, pokud jde o Eurodac [a automatizovaný systém pro registraci a sledování a přidělovací mechanismus pro žádosti o mezinárodní ochranu uvedený v článku 44 nařízení (EU) XX/XX, kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o mezinárodní ochranu podané

62

státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států (přepracované znění)], toto nařízení představuje nové opatření týkající se Eurodacu ve smyslu Dohody mezi Evropským společenstvím a Švýcarskou konfederací o kritériích a mechanismech určení státu příslušného pro posuzování žádosti o azyl podané v některém z členských států nebo ve Švýcarsku.

(67) Co se týče Lichtenštejnska, pokud jde o Eurodac [a automatizovaný systém pro registraci a sledování a přidělovací mechanismus pro žádosti o mezinárodní ochranu uvedený v článku 44 nařízení (EU) XX/XX, 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 (přepracované znění)], toto nařízení představuje nové opatření ve smyslu Protokolu mezi Evropským společenstvím, Švýcarskou konfederací a Lichtenštejnským knížectvím o přistoupení Lichtenštejnského knížectví k Dohodě mezi Evropským společenstvím a Švýcarskou konfederací o kritériích a mechanismech určení státu příslušného pro posuzování žádosti o azyl podané v některém z členských států nebo ve Švýcarsku.

(68) Toto nařízení ctí základní práva a dodržuje zásady uznávané zejména Listinou základních práv Evropské unie a použije se v souladu s těmito právy a zásadami,

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I
Obecná ustanovení

Článek 1
Předmět

1. Toto nařízení společně s [nařízením 2018/xx o interoperabilitě v oblast hranic a víz] stanoví rámec, který má zajistit interoperabilitu mezi Systémem vstupu/výstupu (EES), Vízovým informačním systémem (VIS), [evropským systémem pro cestovní informace a povolení (ETIAS)], systémem Eurodac, Schengenským informačním systémem (SIS) a [Evropským informačním systémem rejstříků trestů pro státní příslušníky třetích zemí (ECRIS-TCN)] tak, aby se tyto systémy a údaje navzájem doplňovaly.

2. Tento rámec bude zahrnovat následující 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 obsahuje ustanovení týkajíc se požadavků na kvalitu údajů, univerzálního formátu pro zprávy (UMF), centrálního úložiště pro účely podávání zpráv a statistiky (CRRS) a stanoví povinnosti členských států a Evropské agentury pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (eu-LISA) s ohledem na návrh a provoz složek interoperability.

4. Toto nařízení rovněž upravuje postupy a podmínky pro přístup donucovacích orgánů členských států a Agentury Evropské unie pro spolupráci v oblasti prosazování práva (Europol) k Systému vstupu/výstupu (EES), Vízovému informačnímu systému (VIS), [evropskému systému pro cestovní informace a povolení (ETIAS)] a systému Eurodac pro účely prevence, odhalování a vyšetřování teroristických trestných činů nebo jiných závažných trestných činů, které spadají do jejich pravomoci.

Článek 2
Cíle interoperability

1. Zajištěním interoperability sleduje nařízení tyto cíle:
   a) zlepšit správu vnějších hranic;
   b) přispět k prevenci nelegální migrace a boji proti ní;
   c) 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;
   d) zlepšit provádění společné vízové politiky a
   e) pomáhat při posuzování žádostí o mezinárodní ochranu.
2. Cílů zajištění interoperability se dosáhne:
   a) správným zjištěním totožnosti osob;
   b) přispěním k boji proti podvodnému zneužívání totožnosti;
   c) zlepšením a slaďováním požadavků na kvalitu údajů jednotlivých informačních systémů EU;
   d) usnadněním technického a provozního provádění stávajících a budoucích informačních systémů ze strany členských států;
   e) posílením, zjednodušováním a zajištěním jednotnějších podmínek pro bezpečnost a ochranu údajů, kterými se řídí příslušné informační systémy EU;
   f) zjednodušením podmínek pro přístup k systémům EES, VIS, [ETIAS] a Eurodac pro účely prosazování práva;
   g) podporou účelů systémů EES, VIS, [ETIAS], Eurodac, SIS a [systému ECRIS-TCN].

Článek 3
Oblast působnosti

1. Toto nařízení se použije na Eurodac, Schengenský informační systém (SIS) a Evropský informační systém rejstříků trestů pro státní příslušníky třetích zemí (ECRIS-TCN)].
2. Toto nařízení se rovněž použije na údaje Europolu v rozsahu, který umožňuje jejich vyhledávání souběžně v informačních systémech EU uvedenými v odstavci 1 v souladu s unijním právem.
3. Toto nařízení se vztahuje na osoby, jejichž osobní údaje mohou být zpracovávány v informačních systémech EU uvedených v odstavci 1.

Článek 4
Definice

Pro účely tohoto nařízení se rozumí:

1) „vnějšími hranicemi“ vnější hranice definované v čl. 2 bodě 2 nařízení (EU) 2016/399;

2) „hraničními kontrolami“ hraniční kontroly definované v čl. 2 bodě 11 nařízení (EU) 2016/399;

3) „pohraničním orgánem“ příslušník pohraniční stráže, který je v souladu s vnitrostátním právem pověřen prováděním hraničních kontrol;

4) „dozorovými úřady“ dozorový úřad zřízený v souladu s čl. 51 odst. 1 nařízení (EU) 2016/679 a dozorový úřad zřízený v souladu s 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) „státním příslušníkem třetí země“ osoba, která není občanem Unie ve smyslu čl. 20 odst. 1 Smlouvy, nebo osoba bez státní příslušnosti nebo osoba, jejíž státní příslušnost není známa;

8) „alfanumerickými údaji“ údaje vyjádřené písmeny, číslicemi, zvláštními znaky, mezerami a interpunkčními znaménky;

9) „údaji o totožnosti“ údaje uvedené v čl. 27 odst. 3 písm. a) až h);

10) „údaji o otiscích prstů“ údaje týkající se otisků prstů jednotlivce;

11) „zobrazením obličeje“ digitální zobrazení obličeje;

12) „biometrickými údaji“ údaje o otiscích prstů a zobrazení obličeje;

13) „biometrickou šablonou“ matematické vyjádření získané extrakcí rysů z biometrických údajů omezených na charakteristiky, které jsou nezbytné pro zjištění totožnosti a ověření;

14) „cestovním dokladem“ pas nebo jiný rovnocenný doklad, který držitele opravňuje překračovat vnější hranice a do něhož lze vyznačit vízum;

15) „údaji o cestovním dokladu“ druh, číslo a země vydání cestovního dokladu, datum ukončení platnosti cestovního dokladu a trojmístný kód země, která cestovní doklad vydala;

16) „cestovním povolením“ cestovní povolení definované v článku 3 [nařízení o ETIAS];

17) „krátkodobým vízem“ vízum definované v čl. 2 bodě 2 písm. a) nařízení (ES) č. 810/2009;

18) „informačními systémy EU“ rozsáhlé informační systémy, které spravuje agentura eu-LISA;

19) „údaji Europolu“ osobní údaje, které byly poskytnuty Europolu pro účely uvedené v čl. 18 odst. 2 písm. a) nařízení (EU) 2016/794;

20) „databázemi Interpolu“ databáze odcizených a ztracených cestovních dokladů (SLTD) Interpolu a databáze Interpolu TDAWN (cestovní doklady s údaji uvedenými v oběžnících);

21) „shodou“ existence odpovídajícího údaje zjištěná porovnáváním dvou či více výskytů osobních údajů zaznamenaných nebo zaznamenávaných v informačním systému či databázi;

22) „pozitivním nálezem“ potvrzení jedné či více shod;

23) „policejním orgánem“ „příslušný orgán“ definovaný v čl. 3 bodě 7 směrnice 2016/680;

24) „určenými orgány“ určené orgány členského státu uvedené v čl. 29 odst. 1 nařízení (EU) 2017/2226, čl. 3 odst. 1 rozhodnutí Rady 2008/633/SVV, [článku 43 nařízení o systému ETIAS] a [článku 6 nařízení o Eurodacu];

25) „teroristickým trestným činem“ trestný čin podle vnitrostátního práva, který odpovídá nebo je rovnocenný jednomu z trestných činů uvedených ve směrnici (EU) 2017/541;

26) „závažným trestným činem“ trestný čin, který odpovídá nebo je rovnocenný jednomu z trestných činů uvedených v čl. 2 odst. 2 rámcového rozhodnutí 2002/584/SVV, pokud jej lze podle vnitrostátního práva potrestat odnětím svobody s horní hranicí sazby v délce nejméně tři roky nebo ochranným opatřením spojeným s omezením svobody ve stejné délce;

27) „EES“ Systém vstupu/výstupu uvedený v nařízení (EU) 2017/2226;

28) „VIS“ Vízový informační systém uvedený v nařízení (ES) č. 767/2008;

29) [„ETIAS“ evropský systém pro cestovní informace a povolení uvedený v nařízení o systému ETIAS];

30) „Eurodac“ systém Eurodac uvedený v [nařízení o Eurodacu];

31) „SIS“ Schengenský informační systém uvedený v [nařízení o SIS v oblasti hraničních kontrol, nařízení o SIS v oblasti prosazování práva a nařízení o SIS v oblasti navracení neoprávněně pobývajících osob];

32) [„systémem ECRIS-TCN“ Evropský informační systém rejstříků trestů obsahující informace o odsouzení státních příslušníků třetích zemí a osob bez státní příslušnost uvedený v nařízení o ECRIS-TCN];

33) „ESP“ Evropský vyhledávací portál uvedený v článku 6;

34) „sdílenou BMS“ sdílená služba pro porovnávání biometrických údajů uvedená v článku 15;

35) „CIR“ společné úložiště údajů o totožnosti uvedené v článku 17;

36) „MID“ detektor vícenásobné totožnosti uvedený v článku 25;

37) „CRRS“ centrální úložiště pro účely podávání zpráv a statistiky uvedené v článku 39.

Článek 5
Zákaz diskriminace

Zpracovávání osobních údajů pro účely tohoto nařízení nesmí vést k diskriminaci osob na základě pohlaví, rasového či etnického původu, náboženského vyznání nebo přesvědčení, zdravotního postižení, věku nebo sexuální orientace. Musí plně respektovat lidskou důstojnost a integritu. Zvláštní pozornost se musí věnovat dětem, starším osobám a osobám se zdravotním postižením.

KAPITOLA II
Evropský vyhledávací portál

Článek 6
Evropský vyhledávací portál

1. Zřizuje se Evropský vyhledávací portál (ESP), jehož účelem je zajistit, aby orgány členských států a subjekty EU získaly – v souladu se svými přístupovými právy – rychlý, bezproblémový, účinný, systematický a řízený přístup k informačním systémům EU, k údajům Europolu a k databázím Interpolu, který potřebují k plnění svých úkolů, a podpořit cíle systémů EES, VIS, [ETIAS], Eurodac, SIS, [systému ECRIS-TCN] a údajů Europolu.

2. Systém ESP se skládá:

   a) z ústřední infrastruktury včetně vyhledávacího portálu, který umožňuje souběžné vyhledávání v systémech EES, VIS, [ETIAS], Eurodac, SIS, [systému ECRIS-TCN] a rovněž v údajích Europolu a databázích Interpolu;

   b) ze zabezpečeného komunikačního kanálu mezi systémem ESP, členskými státy a subjekty EU, které jsou oprávněné používat ESP v souladu s unijním právem;

   c) ze zabezpečené komunikační infrastruktury mezi systémy ESP a EES, VIS, [ETIAS], Eurodac, centrálním SIS, [systémem ECRIS-TCN], údaji Europolu a databázemi Interpolu, jakož i mezi systémem ESP a ústředními infrastrukturami společného úložiště údajů o totožnosti (CIR) a detektorem vícenásobné totožnosti.

3. Agentura eu-LISA vyvine ESP a zajistí jeho technickou správu.

Článek 7
Používání Evropského vyhledávacího portálu

1. Používání ESP je vyhrazeno orgánům členských států a subjektům EU s přístupem do systémů EES, [ETIAS], VIS, SIS, Eurodac a [systému ECRIS-TCN], do CIR a k detektoru vícenásobné totožnosti, jakož i k údajům Europolu a databázím Interpolu v souladu s unijním či vnitrostátním právem upravujícím takový přístup.

2. Orgány uvedené v odstavci 1 mohou využívat ESP k vyhledávání údajů souvisejících s osobami nebo jejich cestovními doklady v ústředních systémech Eurodacu a [systému ECRIS-TCN] v souladu s jejich přístupovými právy podle unijního a vnitrostátního práva. ESP mohou také používat k vyhledávání v CIR v souladu s jejich přístupovými právy ve smyslu 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 ve smyslu [nařízení o SIS v oblasti hraničních kontrol a nařízení o SIS v oblasti prosazování práva]. Přístup do centrálního systému SIS přes ESP bude zajištěn prostřednictvím vnitrostátního systému (N.SIS) každého členského státu v souladu s [čl. 4 odst. 2 nařízení o SIS v oblasti hraničních kontrol a nařízení o SIS v oblasti prosazování práva].

4. Subjekty EU používají ESP k vyhledávání údajů týkajících se osob nebo jejich cestovních dokladů v centrálním SIS.

5. Orgány uvedené v odstavci 1 mohou využívat ESP k vyhledávání údajů týkajících se osob nebo jejich cestovních dokladů v údajích Europolu v souladu s jejich přístupovými právy podle unijního a vnitrostátního práva.

Článek 8
Profily uživatelů Evropského vyhledávacího portálu

1. Aby umožnila používání ESP, vytvoří agentura eu-LISA v souladu s unijním a vnitrostátním právem profil pro každou kategorii uživatelů ESP v souladu s technickými podrobnostmi a přístupovými právy uvedenými v odstavci 2, včetně:

   a) datových polí, která budou používána pro vyhledávání;

   b) informačních systémů EU, údajů Europolu a databází Interpolu, v nichž lze vyhledávat a které uživateli poskytnou odpověď a

   c) údajů uvedených v každé odpovědi.

2. Komise přijme akty v přenesené pravomoci v souladu s článkem 63 a stanoví technické podrobnosti profilů uvedených v odstavci 1 pro uživatele ESP zmíněné v čl. 7 odst. 1 v souladu s jejich přístupovými právy.

Článek 9
Vyhledávání

1. Uživatelé ESP zahájí vyhledávání tak, že zadají údaje do ESP v souladu s jejich uživatelským profilem a přístupovými právy. Po zahájení vyhledávání začne ESP na základě údajů zadaných uživatelem ESP prohledávat souběžně systémy EES, [ETIAS], VIS, SIS, Eurodac, [systém ECRIS-TCN] a CIR, jakož i údaje Europolu a databáze Interpolu.

2. Datová pole použitá k zahájení vyhledávání prostřednictvím ESP musejí odpovídat datovým polím týkajícím se osob nebo cestovních dokladů, která lze používat pro vyhledávání v různých informačních systémech EU, údajích Europolu a databázích Interpolu v souladu s právními nástroji, kterými se tyto systémy řídí.

3. Agentura eu-LISA zavede pro účely ESP dokument pro ovládání rozhraní (ICD), a to na základě UMF uvedeného v článku 38.

4. Systémy EES, [ETIAS], VIS, SIS, Eurodac, [systém ECRIS-TCN], CIR a detektor vícenásobné totožnosti i údaje Europolu a databáze Interpolu poskytnou na základě dotazu z ESP údaje, které obsahují.

5. Při vyhledávání v databázích Interpolu musí architektura ESP zaručit, že údaje používané uživatelem ESP k zahájení vyhledávání nejsou sdíleny s vlastníky údajů Interpolu.

6. Odpověď uživateli ESP musí být jedinečná a musí obsahovat všechny údaje, k nimž má uživatel přístup podle práva Unie. Pokud je to nezbytné, v odpovědi poskytnuté ESP je uvedeno, do kterého informačního systému nebo databáze daný údaj patří.

7. Komise přijme v souladu s článkem 63 akt v přenesené pravomoci, kterým stanoví obsah a formát odpovědí ESP.

Článek 10
Vedení protokolů

1. Aniž je dotčen [článek 39 nařízení o Eurodacu], [články 12 a 18 nařízení o SIS v oblasti prosazování práva], [článek 29 nařízení o ECRIS-TCN] a článek 40 nařízení (EU) 2016/794, vede agentura eu-LISA protokoly o všech operacích zpracování údajů v rámci ESP. V těchto protokolech se uvedou zejména tyto údaje:

   a) orgán členského státu a jednotlivý uživatel ESP, včetně použitého profilu ESP uvedený v článku 8;

   b) datum a čas vyhledávání;

   c) informační systémy EU a údaje Europolu, v nichž vyhledávání proběhlo;

   d) v souladu s vnitrostátními pravidly nebo nařízením (EU) 2016/794, případně nařízením (EU) 45/2001 identifikační značka osoby, která vyhledávání provedla.

2. Protokoly lze použít pouze pro účely dohledu nad ochranou údajů, včetně kontroly přípustnosti vyhledávání a zákonnosti zpracování údajů, a pro zabezpečení údajů podle článku 42. Tyto protokoly musí být chráněny vhodnými opatřeními proti neoprávněnému přístupu a vymazány po uplynutí jednoho roku od svého vytvoření, pokud nejsou nezbytné pro již zahájené kontrolní postupy.

Článek 11
Nouzové postupy v případě technické nemožnosti použít Evropský vyhledávací portál

1. Pokud je technicky nemožné použít ESP k vyhledávání v jednom či více informačních systémech EU uvedených v čl. 9 odst. 1 nebo CIR z důvodu poruchy ESP, jsou uživatelé ESP o této skutečnosti informováni agenturou eu-LISA.

2. Pokud je technicky nemožné použít ESP k vyhledávání v jednom či více informačních systémech EU uvedených v čl. 9 odst. 1 nebo v CIR z důvodu poruchy vnitrostátní infrastruktury v členském státě, příslušný orgán tohoto členského státu o této skutečnosti informuje agenturu eu-LISA a Komisi.

3. V obou případech a až do odstranění technické poruchy se neuplatní povinnost uvedená v čl. 7 odst. 2 a 4 a členské státy mohou získat přístup k informačním systémům uvedeným v čl. 9 odst. 1 nebo CIR přímo s použitím příslušných vnitrostátních jednotných rozhraní nebo vnitrostátních komunikačních infrastruktur.

KAPITOLA III
Sdílená služba pro porovnávání biometrických údajů

Článek 12
Sdílená služba pro porovnávání biometrických údajů

1. Zřizuje se sdílená služba pro porovnávání biometrických údajů (sdílená BMS), která uchovává biometrické šablony a umožňuje vyhledávání s využitím biometrických údajů v několika informačních systémech EU, za účelem podpory CIR a detektoru vícenásobné totožnosti, jakož i cílů systémů EES, VIS, Eurodac, SIS a [systému ECRIS-TCN].

2. Sdílenou BMS tvoří:

   a) ústřední infrastruktura obsahující nástroj pro vyhledávání a ukládání údajů uvedených v článku 13;

   b) zabezpečená komunikační infrastruktura mezi sdílenou BMS, centrálním SIS a CIR.

3. Agentura eu-LISA vyvine sdílenou BMS a zajistí její technickou správu.

Článek 13
Údaje uložené ve sdílené službě pro porovnávání biometrických údajů

1. Sdílená BMS ukládá biometrické šablony, které získá z těchto biometrických údajů:

   a) údaje uvedené v čl. 16 odst. 1 písm. d) a čl. 17 odst. 1 písm. b) a c) nařízení (EU) 2017/2226;

   b) údaje uvedené v čl. 9 odst. 6 nařízení (ES) č. 767/2008;

   c) [údaje uvedené v čl. 20 odst. 2 písm. w) a x) nařízení o SIS v oblasti hraničních kontrol];

   d) údaje uvedené v čl. 20 odst. 3 písm. w) a x) nařízení o SIS v oblasti prosazování práva;

   e) údaje uvedené v čl. 4 odst. 3 písm. t) a u) nařízení o SIS v oblasti navracení neoprávněně pobývajících osob];

   f) [údaje uvedené v čl. 13 písm. a) nařízení o Eurodacu;]

   g) [údaje uvedené v čl. 5 odst. 1 písm. b) a čl. 5 odst. 2 nařízení o ECRIS-TCN.]

2. Sdílená BMS v každé biometrické šabloně uvede odkaz na informační systémy, v nichž jsou uloženy odpovídající biometrické údaje.

3. Biometrické šablony lze zadávat do sdílené BMS pouze po automatizované kontrole kvality biometrických údajů přidaných do jednoho z informačních systémů, kterou provede sdílená BMS, 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.

Článek 14
Vyhledávání biometrických údajů s využitím sdílené služby pro porovnávání biometrických údajů

Aby bylo možné vyhledat biometrické údaje uložené v CIR a SIS, musí CIR a SIS používat biometrické šablony uložené ve sdílené BMS. Vyhledávání na základě biometrických údajů musí proběhnout v souladu s účely stanovenými v tomto nařízení a v nařízení o EES, nařízení o VIS, nařízení o Eurodacu, [nařízeních o SIS] a [nařízení o ECRIS-TCN].

Článek 15
Uchovávání údajů ve sdílené službě pro porovnávání biometrických údajů

Údaje uvedené v článku 13 jsou ve sdílené BMS uloženy tak dlouho, dokud jsou odpovídající biometrické údaje uloženy v CIR nebo SIS.

Článek 16
Vedení protokolů

1. Aniž je dotčen [článek 39 nařízení o Eurodacu], [články 12 a 18 nařízení o SIS v oblasti prosazování práva], [článek 29 nařízení o ECRIS-TCN], vede agentura eu-LISA protokoly o všech operacích zpracování údajů v rámci BMS. V těchto protokolech se uvedou zejména tyto údaje:
   a) historie související s vytvořením a uložením biometrických šablon;
   b) odkaz na informační systémy EU, v nichž se vyhledává s použitím biometrických šablon uložených ve sdílené BMS;
   c) datum a čas vyhledávání;
   d) druh biometrických údajů použitých k zahájení vyhledávání;
   e) délka vyhledávání;
   f) výsledky vyhledávání a datum a čas výsledku;
   g) v souladu s vnitrostátními pravidly nebo nařízením (EU) 2016/794, případně nařízením (EU) 45/2001 identifikační značka osoby, která vyhledávání provedla.
2. Protokoly lze použít pouze pro účely dohledu nad ochranou údajů, včetně kontroly přípustnosti vyhledávání a zákonnosti zpracování údajů, a pro zabezpečení údajů podle článku 42. Tyto protokoly musí být chráněny vhodnými opatřeními proti neoprávněnému přístupu a vymazány po uplynutí jednoho roku od svého vytvoření, pokud nejsou nezbytné pro již zahájené kontrolní postupy. Protokoly uvedené v odst. 1 písm. a) je nutno vymazat, jakmile dojde k vymazání příslušných údajů.

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 systému EES, VIS, [ETIAS], Eurodac nebo [systému ECRIS-TCN] a obsahuje údaje uvedené v článku 18, s cílem usnadnit

a napomáhat správnému zjištění totožnosti osob registrovaných v systémech EES, VIS, [ETIAS], Eurodac a [v systému ECRIS-TCN], podpořit fungování detektoru vícenásobné totožnosti a usnadnit a zefektivnit přístup donucovacích orgánů k informačním systémům, jež neslouží k prosazování práva, na úrovni EU, pokud je to nezbytné pro prevenci, vyšetřování, odhalování či stíhání závažné trestné činnosti.

2. CIR se skládá:

a) z ústřední infrastruktury, která nahrazuje příslušné ústřední systémy EES, VIS, [ETIAS], Eurodac a [systém ECRIS-TCN] do takové míry, že uchovává údaje uvedené v článku 18;

b) ze zabezpečeného komunikačního kanálu mezi CIR, členskými státy a subjekty EU, které jsou oprávněné používat Evropský vyhledávací portál (ESP) v souladu s unijním právem;

c) ze zabezpečené komunikační infrastruktury mezi CIR a systémem EES, [ETIAS], VIS, Eurodac a [systémem ECRIS-TCN], jakož i ústředními infrastrukturami ESP, sdílenou BMS a detektorem vícenásobné totožnosti.

3. Agentura eu-LISA vyvine CIR a zajistí jeho technickou správu.

Článek 18
Údaje společného úložiště údajů o totožnosti

1. CIR ukládá tyto údaje – logicky oddělené – v souladu s informačním systémem, z něhož pocházejí:

a) – (nepoužije se);

b) – (nepoužije se);

c) – (nepoužije se);

d) [údaje uvedené v čl. 13 písm. a) až e), g) a h) [nařízení o Eurodacu;]

e) [údaje uvedené v čl. 5 odst. 1 písm. b) a čl. 5 odst. 2 a tyto údaje uvedené v čl. 5 odst. 1 písm. a) nařízení o ECRIS-TCN: příjmení; jméno (jména); pohlaví; datum narození; místo a země narození; státní příslušnost (příslušnosti); pohlaví a případně dřívější jména, pseudonym (pseudonymy) a/nebo přezdívka (přezdívky).]

2. Pro každý soubor údajů uvedený v odstavci 1 musí CIR uvést odkaz na informační systémy, do kterých údaje patří.

3. 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 dojde v Eurodacu nebo v [systému ECRIS-TCN] k doplnění, změně nebo výmazu údajů, automaticky se příslušně doplní, změní nebo vymažou údaje uvedené v článku 18 uložené v individuálním souboru CIR.

2. Pokud detektor vícenásobné totožnosti vytvoří v souladu s články 32 a 33 bílé nebo červené propojení mezi údaji dvou nebo více informačních systémů EU, z nichž se CIR skládá, CIR namísto vytvoření nového individuálního souboru přidá nové údaje do individuálního souboru propojených údajů.

Článek 20

Přístup do společného úložiště údajů o totožnosti pro účely zjištění totožnosti

1. Pokud je policejní orgán členského státu na základě vnitrostátních legislativních opatření uvedené v odstavci 2 zmocněn, může výhradně pro účely zjištění totožnosti osoby vyhledávat v CIR s využitím biometrických údajů této osoby, které získal během kontroly totožnosti.

   Pokud vyhledávání ukáže, že údaje o této osobě jsou uložené v CIR, je orgánu členského státu umožněno nahlížet do údajů uvedených 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 dané osoby ve spojení s údaji v cestovním dokladu nebo s použitím údajů o totožnosti poskytnutých touto osobou.

2. Členské státy, které si přejí využít možnost stanovenou v tomto článku, přijmou příslušná vnitrostátní legislativní opatření. Taková legislativní opatření vymezí přesné účely kontrol 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.

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 kontrolu různých totožností určený v souladu s článkem 29 má výhradně pro účely takového ověření přístup k údajům o totožnosti uloženým v CIR, které patří do různých informačních systémů spojených 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 o totožnosti uloženým v CIR, které patří do různých informačních systémů spojených červeným propojením.

Článek 22

Vyhledávání ve společném úložišti údajů o totožnosti pro účely prosazování práva

1. Určené orgány členských států a Europol mohou v CIR vyhledávat pro účely prevence, odhalování a vyšetřování teroristických trestných činů nebo jiných závažných trestných činů v souvislosti s konkrétním případem a za účelem získání informací o tom, zda se údaje týkající se konkrétní osoby vyskytují v systému Eurodac.

2. Určené orgány členských států a Europol nejsou při nahlížení do CIR pro účely uvedené v odstavci 1 oprávněny nahlížet do údajů spadajících do [systému ECRIS-TCN].

3. Pokud CIR v odpovědi na vyhledávání uvede, že se údaje o dané osobě vyskytují v systému Eurodac, zašle určeným orgánům členských států a Europolu odpověď v podobě odkazu uvádějícího, který informační systém obsahuje odpovídající údaje uvedené v čl. 18 odst. 2. CIR odpoví takovým způsobem, aby nebylo narušeno zabezpečení těchto údajů.

4. Plný přístup k údajům obsaženým v informačních systémech EU pro účely prevence, odhalování a vyšetřování teroristických trestných činů nebo jiných závažných trestných činů nadále podléhá podmínkám a postupům stanoveným v příslušných legislativních nástrojích upravujících takový přístup.

Článek 23
Uchovávání údajů ve společném úložišti údajů o totožnosti

1. Údaje uvedené v čl. 18 odst. 1 a 2 se z CIR vymažou v souladu s ustanoveními o uchovávání údajů [nařízení o Eurodacu], resp. [nařízení o ECRIS-TCN].

2. Individuální soubor je v CIR uložen tak dlouho, dokud jsou odpovídající údaje uloženy alespoň v jednom z informačních systémů, jejichž údaje jsou obsaženy v CIR. Vytvoření propojení nemá vliv na období uchovávání jednotlivých položek propojených údajů.

Článek 24
Vedení protokolů

1. Aniž je dotčen [článek 39 nařízení o Eurodacu] a [článek 29 nařízení o ECRIS-TCN], vede agentura eu-LISA protokoly o všech operacích zpracování údajů v rámci CIR v souladu s odstavci 2, 3 a 4.

2. V souvislosti s jakýmkoli přístupem do CIR podle čl. 20 vede agentura eu-LISA protokoly o všech operacích zpracování údajů v rámci CIR. V těchto protokolech se uvedou zejména tyto údaje:

   a) účel přístupu uživatele, který vyhledává prostřednictvím CIR;

   b) datum a čas vyhledávání;

   c) druh údajů použitých k zahájení vyhledávání;

   d) výsledky vyhledávání;

   e) v souladu s vnitrostátními pravidly nebo nařízením (EU) 2016/794, případně nařízením (EU) 45/2001 identifikační značka osoby, která vyhledávání provedla.

3. V souvislosti s jakýmkoli přístupem do CIR podle článku 21 vede agentura eu-LISA protokoly o všech operacích zpracování údajů v rámci CIR. V těchto protokolech se uvádí zejména tyto údaje:

   a) účel přístupu uživatele, který vyhledává prostřednictvím CIR;

   b) datum a čas vyhledávání;

   c) případné údaje použité k zaslání dotazu;

   d) případné výsledky vyhledávání;

   e) v souladu s vnitrostátními pravidly nebo nařízením (EU) 2016/794, případně nařízením (EU) 45/2001 identifikační značka osoby, která vyhledávání provedla.

4. V souvislosti s jakýmkoli přístupem do CIR podle článku 22 vede agentura eu-LISA protokoly o všech operacích zpracování údajů v rámci CIR. V těchto protokolech se uvádí zejména tyto údaje:

   a) odkaz na vnitrostátní spis;

b) datum a čas vyhledávání;

c) druh údajů použitých k zahájení vyhledávání;

d) výsledky vyhledávání;

e) název orgánu nahlížejícího do CIR;

f) v souladu s vnitrostátními pravidly nebo nařízením (EU) 2016/794, případně nařízením (EU) 45/2001 identifikační značka pracovníka, který vyhledávání provedl, a pracovníka, který vyhledávání nařídil.

Protokoly o takovém přístupu pravidelně ověřuje příslušný dozorový úřad zřízený v souladu s článkem 51 nařízení (EU) 2016/679 nebo v souladu s článkem 41 směrnice 2016/680, a to v intervalech nepřekračujících šest měsíců, s cílem ověřit, zda jsou dodržovány postupy a podmínky stanovené v čl. 22 odst. 1 až 3.

5. Každý členský stát vede protokoly o vyhledávání, které provedli pracovníci s řádně oprávněním k používání CIR podle článků 20, 21 a 22.

6. Protokoly uvedené v odstavcích 1 a 5 lze použít pouze pro účely dohledu nad ochranou údajů, včetně kontroly přípustnosti žádostí a zákonnosti zpracování údajů, a pro zabezpečení údajů uvedených v článku 42. Musí být chráněny vhodnými opatřeními proti neoprávněnému přístupu a vymazány po uplynutí jednoho roku od svého vytvoření, pokud nejsou nezbytné pro již zahájené kontrolní postupy.

7. Agentura eu-LISA vede protokoly související s historií údajů uložených v individuálním souboru pro účely vymezené v odstavci 6. Protokoly související s historií údajů se vymažou, jakmile dojde k vymazání údajů.

KAPITOLA V
Detektor vícenásobné totožnosti

Článek 25
Detektor vícenásobné totožnosti

1. S cílem podpořit fungování CIR a účely systémů EES, VIS, ETIAS], Eurodac, SIS a [systému ECRIS-TCN] se zřizuje detektor vícenásobné totožnosti (MID), který vytváří a ukládá propojení mezi údaji v informačních systémech EU zahrnutých ve společném úložišti údajů o totožnosti (CIR) a v SIS a následně odhaluje vícenásobné totožnosti s dvojím účelem, kterým je usnadnění kontrol totožnosti a potírání podvodného zneužití totožnosti.

2. MID se skládá:

a) z ústřední infrastruktury, která uchovává propojení a odkazy na informační systémy;

b) ze zabezpečené komunikační infrastruktury k propojení MID se SIS a ústředními infrastrukturami Evropského vyhledávacího portálu a CIR.

3. Agentura eu-LISA vyvine MID a zajistí jeho technickou správu.

Článek 26
Přístup k detektoru vícenásobné totožnosti

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

   a) – (nepoužije se);

   b) – (nepoužije se);

   c) – (nepoužije se);

   d) orgánům příslušným k posouzení žádosti o mezinárodní ochranu uvedeným v nařízení o Eurodacu při posuzování nové žádosti o mezinárodní ochranu;

   e) centrálám SIRENE členského státu při vytváření záznamu podle [nařízení o SIS v oblasti prosazování práva nebo nařízení o SIS v oblasti navracení neoprávněně pobývajících osob];

   f) [ústředním orgánům odsuzujícího členského státu při záznamu nebo aktualizaci údajů v systému ECRIS-TCN v souladu s článkem 5 nařízení o ECRIS-TCN.]

2. Orgány členských států a subjekty EU s přístupem alespoň do jednoho informačního systému EU, který je součástí společného úložiště údajů o totožnosti, nebo do systému SIS mají přístup k údajům podle čl. 34 písm. a) a b), pokud jde o červená propojení uvedená v článku 32.

Článek 27
Odhalování vícenásobných totožností

1. Odhalování vícenásobných totožností ve společném úložišti údajů o totožnosti a v systému SIS bude zahájeno v případě, že:

   a) – (nepoužije se);

   b) – (nepoužije se);

   c) – (nepoužije se);

   d) [žádost o mezinárodní ochranu je vytvořena nebo aktualizována v systému Eurodac v souladu s článkem 10 nařízení o Eurodacu];

   e) [záznam o osobě je vytvořen nebo aktualizován v SIS v souladu s kapitolami VI, VII, VIII a IX nařízení o SIS v oblasti prosazování práva a článkem 3 nařízení o SIS v oblasti navracení neoprávněně pobývajících osob];

   f) [datový záznam je vytvořen nebo aktualizován v systému ECRIS-TCN v souladu s článkem 5 nařízení o ECRIS-TCN.]

2. Pokud údaje obsažené v informačním systému uvedeném v odstavci 1 obsahují biometrické údaje, společné úložiště údajů o totožnosti (CIR) a centrální SIS použijí sdílenou službu pro porovnávání biometrických údajů (sdílená BMS), aby odhalily vícenásobné totožnosti. 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 témuž státnímu příslušníkovi třetí země jsou již uloženy v CIR nebo v centrálním SIS.

3. Kromě postupu uvedeného v odstavci 2 využije CIR a centrální SIS Evropský vyhledávací portál a vyhledá údaje uložené v CIR a v centrálním SIS s využitím následujících údajů:

a) – (nepoužije se);

b) – (nepoužije se);

c) – (nepoužije se);

d) [příjmení; jméno (jména); rodné (rodná) příjmení, dřívější jména a přezdívky; datum narození, místo narození, státní příslušnost (příslušnosti) a pohlaví uvedené v článku 12 nařízení o Eurodacu];

e) – (nepoužije se);

f) [příjmení; jméno (jména); rodné (rodná) příjmení, dřívější jména a přezdívky; datum narození, místo narození, státní příslušnost (příslušnosti) a pohlaví uvedené v čl. 20 odst. 3 nařízení o SIS v oblasti prosazování práva];

g) [příjmení; jméno (jména); rodné (rodná) příjmení, dřívější jména a přezdívky; datum narození, místo narození, státní příslušnost (příslušnosti) a pohlaví uvedené v článku 4 nařízení o SIS v oblasti navracení neoprávněně pobývajících osob];

h) [příjmení; jméno (jména); datum narození, místo narození, státní příslušnost (příslušnosti) a pohlaví uvedené v čl. 5 odst. 1 písm. a) nařízení o ECRIS-TCN.]

4. Odhalování vícenásobných totožností bude zahájeno pouze pro porovnání údajů dostupných v jednom informačním systému s údaji dostupnými v jiných informačních systémech.

Článek 28
Výsledky odhalení vícenásobných totožností

1. Pokud výsledkem vyhledávání uvedeného v čl. 27 odst. 2 a odst. 3 není žádný pozitivní nález, pokračují postupy uvedené v čl. 27 odst. 1 v souladu s příslušnými nařízeními, která je upravují.

2. Pokud je výsledkem vyhledávání uvedeného v čl. 27 odst. 2 a odst. 3 jeden či více pozitivních nálezů, společné úložiště údajů o totožnosti a případně i systém SIS vytvoří propojení mezi údaji použitými při vyhledávání a údaji, které vedly k pozitivnímu nálezu.

   Pokud je výsledkem více pozitivních nálezů, vytvoří se propojení mezi všemi údaji, které k takovému pozitivnímu nálezu vedly. Pokud propojení mezi údaji již existuje, stávající propojení se rozšíří i na údaje použité při vyhledávání.

3. Pokud je výsledkem vyhledávání uvedeného v čl. 27 odst. 2 nebo odst. 3 jeden či více pozitivních nálezů a údaje o totožnosti v propojených souborech jsou shodné nebo podobné, vytvoří se v souladu s článkem 33 bílé propojení.

4. Pokud je výsledkem vyhledávání uvedeného v čl. 27 odst. 2 nebo odst. 3 jeden či více pozitivních nálezů a údaje o totožnosti v propojených souborech nelze považovat za shodné nebo podobné, vytvoří se v souladu s článkem 30 žluté propojení a uplatní se postup uvedený v článku 29.

5. Komise stanoví postupy pro určení případů, kdy lze údaje o totožnosti považovat za shodné nebo podobné, v prováděcích aktech. Tyto prováděcí akty se přijímají přezkumným postupem uvedeným v čl. 64 odst. 2.

6. Propojení budou uložena v souboru údajů souvisejících s potvrzením totožnosti uvedeným v článku 34.

Komise stanoví technická pravidla pro spojování údajů z různých informačních systémů prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem uvedeným v čl. 64 odst. 2.

Článek 29
Manuální ověření různých totožností

1. Aniž jsou dotčena ustanovení odstavce 2, je orgánem odpovědným za ověření různých totožností:

   a) – (nepoužije se);

   b) – (nepoužije se);

   c) – (nepoužije se);

   d) orgán posuzující žádost o mezinárodní ochranu, jak je uvedeno v nařízení o Eurodacu, v případě pozitivních nálezů, které se vyskytnou při posuzování takové žádosti;

   e) centrály SIRENE členských států v případě pozitivních nálezů, které se vyskytnou při vytváření záznamu v SIS v souladu s [nařízením o SIS v oblasti prosazování práva a nařízením o SIS v oblasti navracení neoprávněně pobývajících osob];

   f) ústřední orgány odsuzujícího členského státu v případě pozitivních nálezů, které se vyskytnou při zaznamenávání nebo aktualizaci údajů v systému ECRIS-TCN v souladu s článkem 5 [nařízení o ECRIS-TCN].

   Detektor vícenásobné totožnosti uvede orgán odpovědný za ověření různých totožností v souboru údajů souvisejících s ověřením totožnosti.

2. Orgánem odpovědným za 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:

   a) v záznamu o osobách hledaných za účelem zatčení a předání nebo vydání uvedeném v článku 26 [nařízení o SIS v oblasti prosazování práva];

   b) v záznamu o pohřešovaných nebo zranitelných osobách uvedeném v článku 32 [nařízení o SIS v oblasti prosazování práva];

   c) v záznamu o osobách hledaných za účelem zajištění jejich spolupráce v soudním řízení uvedeném v článku 34 [nařízení o SIS v oblasti prosazování práva];

   d) [v záznamu týkajícím se navracení v souladu s nařízením o SIS v oblasti navracení neoprávněně pobývajících osob];

   e) v záznamu o osobách pořízených pro účely skrytých kontrol, vyšetřovacích kontrol nebo zvláštních kontrol uvedeném v článku 36 [nařízení o SIS v oblasti prosazování práva];

   f) v záznamu o neznámých hledaných osobách za účelem zjištění totožnosti v souladu s vnitrostátním právem či vyhledávání pomocí biometrických údajů uvedeném v článku 40 [nařízení o SIS v oblasti prosazování práva].

3. Aniž je dotčen odstavec 4, má orgán odpovědný za ověření různých totožností přístup k souvisejícím údajům obsaženým v příslušném souboru údajů souvisejících

s potvrzením totožnosti a k údajům o totožnosti spojeným ve společném úložišti údajů o totožnosti a případně v systému SIS a posoudí různé totožnosti a v souladu s články 31, 32 a 33 aktualizuje propojení a neprodleně je doplní do souboru údajů souvisejících s potvrzením totožnosti.

4. – (nepoužije se).

5. Pokud je výsledkem více než jedno propojení, posoudí orgán odpovědný za ověřování různých totožností každé propojení zvlášť.

6. Pokud byly údaje oznamující pozitivní nález již propojeny, zváží orgán odpovědný za ověření různých totožností, zda je s ohledem na tato stávající propojení třeba vytvořit nová propojení.

Článek 30
Žluté propojení

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

   a) propojené údaje mají stejné biometrické údaje, ale odlišné údaje o totožnosti, a neproběhlo žádné manuální ověření různé totožnosti;

   b) propojené údaje mají odlišné údaje o totožnosti a neproběhlo žádné manuální ověření různé totožnosti.

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

Článek 31
Zelené propojení

1. Propojení mezi údaji ze dvou či více informačních systémů se označí jako zelené, pokud propojené údaje nesdílejí stejné biometrické údaje, ale mají podobné údaje o totožnosti, a orgán odpovědný za ověření různých totožností dospěl k závěru, že odkazuje na dvě různé osoby.

2. Pokud se vyhledávání uskuteční ve společném úložišti údajů o totožnosti (CIR) nebo v SIS a pokud existuje zelené propojení mezi dvěma či více informačními systémy tvořícími CIR nebo se systémem SIS, detektor vícenásobné totožnosti uvede, že údaje o totožnosti propojených údajů neodpovídají téže osobě. Prohledávaný informační systém v odpovědi uvede pouze údaje o osobě, jejíž údaje byly použity pro vyhledávání, aniž by to vedlo k pozitivnímu nálezu na základě údajů, na které se vztahuje zelené propojení.

Článek 32
Červené propojení

1. Propojení mezi údaji ze dvou či více informačních systémů se označí jako červené ve všech těchto případech:

   a) propojené údaje mají stejné biometrické údaje, ale odlišné údaje o totožnosti a orgán odpovědný za ověření různých totožností dospěl k závěru, že nezákonně odkazují na tutéž osobu;

b) propojené údaje mají podobné údaje o totožnosti a orgán odpovědný za ověřování různých totožností dospěl k závěru, že nezákonně odkazují na tutéž osobu.

2. Pokud se vyhledávání uskuteční v CIR nebo v SIS a pokud existuje červené propojení mezi dvěma či více informačními systémy tvořícími CIR nebo se systémem SIS, uvede detektor vícenásobné totožnosti ve své odpovědi údaje uvedené v článku 34. Opatření v návaznosti na červené propojení se provádějí v souladu s unijním a vnitrostátním právem.

3. Pokud se vytvoří červené propojení mezi údaji ze systému EES, VIS, [ETIAS], Eurodac nebo [systému ECRIS-TCN], individuální soubor uložený v CIR se aktualizuje v souladu s čl. 19 odst. 1.

4. Aniž jsou dotčena ustanovení týkající se zpracování záznamů v SIS uvedená v [nařízení o SIS v oblasti hraničních kontrol, nařízení o SIS v oblasti prosazování práva a nařízení o SIS v oblasti navracení neoprávněně pobývajících osob] a aniž jsou dotčena omezení nezbytná pro ochranu bezpečnosti a veřejného pořádku, prevenci trestné činnosti a záruku, že nedojde k ohrožení žádného vnitrostátního vyšetřování, pokud se vytvoří červené propojení, orgán odpovědný za ověření různých totožností informuje dotčenou osobu o existenci nezákonných totožností.

5. Pokud se vytvoří červené propojení, poskytne orgán odpovědný za ověření různých totožností odkaz na orgány, které jsou za propojené údaje odpovědné.

Článek 33
Bílé propojení

1. Propojení údajů ze dvou či více informačních systémů 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 alespoň jeden z informačních systémů neobsahuje biometrické údaje o dané osobě;

   c. propojené údaje mají stejné biometrické údaje, ale odlišné údaje o totožnosti a orgán odpovědný za ověřování různých totožností dospěl k závěru, že odkazují na tutéž osobu, která má oprávněně různé údaje o totožnosti.

2. Pokud se vyhledávání uskuteční v CIR nebo v SIS a pokud existuje bílé propojení mezi dvěma či více informačními systémy tvořícími CIR nebo se systémem SIS, detektor vícenásobné totožnosti uvede, že údaje o totožnosti propojených údajů odpovídají téže osobě. Prohledávané informační systémy ve vhodných případech v odpovědi uvedou veškeré propojené údaje o dané osobě, což povede k pozitivnímu nálezu na základě údajů, na které se vztahuje bílé propojení, jestliže orgán, který vyhledávání zahájil, má podle unijního nebo vnitrostátního práva k propojeným údajům přístup.

3. Pokud se vytvoří bílé propojení mezi údaji ze systému EES, VIS, [ETIAS], Eurodac nebo [systému ECRIS-TCN], individuální soubor uložený v CIR se aktualizuje v souladu s čl. 19 odst. 1.

4. Aniž jsou dotčena ustanovení týkající se zpracování záznamů v SIS podle [nařízení o SIS v oblasti hraničních kontrol, nařízení o SIS v oblasti prosazování práva a nařízení o SIS v oblasti navracení neoprávněně pobývajících osob], pokud se po

manuálním ověření vícenásobných identit vytvoří bílé propojení, orgán odpovědný za ověření různých totožností informuje osobu o rozdílech mezi jejími osobními údaji v různých systémech a poskytne odkaz na orgány, které jsou za propojené údaje odpovědné.

Článek 34
Soubor údajů souvisejících s potvrzením totožnosti

Soubor údajů souvisejících s potvrzením totožnosti obsahuje tyto údaje:

a) propojení včetně jejich popisu v podobě barevného označení uvedeného v článcích 30 až 33;

b) odkaz na informační systémy, jejichž údaje jsou propojené;

c) jediné identifikační číslo umožňující získat údaje z informačních systémů odpovídajících propojených souborů;

d) ve vhodných případech orgán odpovědný za ověření různých totožností.

Článek 35
Uchovávání údajů v detektoru vícenásobné totožnosti

Soubory údajů souvisejících s potvrzením totožnosti a jejich údaje včetně propojení jsou v detektoru vícenásobné totožnosti (MID) uloženy jen tak dlouho, dokud jsou propojené údaje uloženy ve dvou či více informačních systémech EU.

Článek 36
Vedení protokolů

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

   a) účel přístupu uživatele a jeho přístupová práva;

   b) datum a čas vyhledávání;

   c) druh údajů použitých k zahájení vyhledávání;

   d) odkaz na propojené údaje;

   e) historie souboru údajů souvisejících s potvrzením totožnosti;

   f) identifikační značka osoby, která vyhledávání provedla.

2. Každý členský stát vede protokoly o pracovnících řádně oprávněných k používání MID.

3. Protokoly lze použít pouze pro dohled nad ochranou údajů, včetně kontroly přípustnosti žádostí a zákonnosti zpracování údajů, a pro zabezpečení údajů podle článku 42. Tyto protokoly musí být chráněny vhodnými opatřeními proti neoprávněnému přístupu a vymazány po uplynutí jednoho roku od svého vytvoření, pokud nejsou nezbytné pro již zahájené kontrolní postupy. Protokoly související s historií souboru údajů souvisejících s potvrzením totožnosti se vymažou, jakmile dojde k vymazání souboru údajů souvisejících s potvrzením totožnosti.

KAPITOLA VI
Opatření na podporu interoperability

Článek 37
Kvalita údajů

1. Agentura eu-LISA zavede mechanismy a postupy pro automatizovanou kontrolu kvality údajů, jež se budou vztahovat na údaje uložené v SIS, Eurodacu, [systému ECRIS-TCN], sdílené službě pro porovnávání biometrických údajů (sdílená BMS), společném úložišti údajů o totožnosti (CIR) a v detektoru vícenásobné totožnosti (MID).

2. Agentura eu-LISA zavede společné ukazatele kvality údajů a minimální normy kvality pro ukládání údajů v SIS, Eurodacu, [systému ECRIS-TCN], sdílené BMS, CIR a MID.

3. Agentura eu-LISA pravidelně předkládá zprávy o mechanismech a postupech pro automatizovanou kontrolu kvality údajů a o společných ukazatelích kvality údajů členským státům. Agentura eu-LISA rovněž pravidelně předkládá Komisi zprávy, jež se týkají vzniklých problémů a dotčených členských států.

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, [systému ECRIS-TCN], sdílené BMS, CIR a MID, zejména v souvislosti s biometrickými údaji, se stanoví v prováděcích aktech. Tyto prováděcí akty se přijímají přezkumným postupem uvedeným v čl. 64 odst. 2.

5. Po uplynutí jednoho roku od zavedení mechanismů a postupů pro automatizovanou kontrolu kvality údajů a společných ukazatelů 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 oznámí veškerý pokrok v souvislosti s tímto akčním plánem až do jeho plného provedení. Komise zašle hodnotící zprávu Evropskému parlamentu, Radě, evropskému inspektorovi ochrany údajů a Agentuře Evropské unie pro základní práva zřízené nařízením Rady (ES) č. 168/2007[63].

Článek 38
Univerzální formát pro zprávy

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

2. Norma UMF se použije při vývoji [Eurodacu] a [systému ECRIS-TCN], Evropského vyhledávacího portálu, CIR, MID a případně při vývoji nových modelů pro výměnu informací a informačních systémů v oblasti spravedlnosti a vnitřních věcí ze strany agentury eu-LISA nebo jakéhokoli jiného orgánu EU.

[63] 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).

3. Zavedení normy UMF může být zváženo v případě SIS a jakýchkoli stávajících nebo nových modelů pro přeshraniční výměnu informací a informačních systémů v oblasti spravedlnosti a vnitřních věcí, které vyvíjejí členské státy nebo přidružené země.

4. Komise přijme prováděcí akt, kterým stanoví a vypracuje normu UMF uvedenou v odstavci 1. Tyto prováděcí akty se přijímají přezkumným postupem uvedeným v čl. 64 odst. 2.

Článek 39
Centrální úložiště pro účely podávání zpráv a statistiky

1. Zřizuje se centrální úložiště pro účely podávání zpráv a statistiky (CRRS) za účelem podpory cílů Eurodacu, SIS a [systému ECRIS-TCN] a vytváření mezisystémových statistických údajů a analytických zpráv pro politické a provozní účely a pro účely kvality údajů.

2. Agentura eu-LISA zřídí, zavede a ve svých technických zařízeních umístí CRRS obsahující údaje uvedené v [čl. 42 odst. 8 nařízení o Eurodacu], [článku 71 nařízení o SIS v oblasti prosazování práva] a [článku 30 nařízení o ECRIS-TCN], které budou logicky oddělené. Údaje obsažené v CRRS nesmějí umožňovat zjištění totožnosti jednotlivců. Přístup do úložiště je poskytován pomocí zabezpečeného přístupu prostřednictvím sítě transevropských služeb pro telematiku mezi správními orgány (TESTA) s kontrolou přístupu a specifickými uživatelskými profily, a to výlučně pro účely podávání zpráv a statistiky orgánům uvedeným v [čl. 42 odst. 8 nařízení o Eurodacu], [článku 71 nařízení o SIS v oblasti prosazování práva] a [článku 30 nařízení o ECRIS-TCN].

3. Agentura eu-LISA údaje anonymizuje a tyto anonymizované údaje zaznamená v CRRS. Anonymizace údajů je automatizovaná.

4. CRRS se skládá:

   a) z ústřední infrastruktury, kterou tvoří úložiště údajů umožňující anonymizaci údajů;

   b) ze zabezpečené komunikační infrastruktury pro připojení CRRS k SIS, Eurodacu a [systému ECRIS-TCN], jakož i k centrálním infrastrukturám sdílené BMS, CIR a MID.

5. Komise stanoví podrobná pravidla pro fungování CRRS, včetně ochranných opatření pro zpracovávání osobních údajů uvedených v odstavcích 2 a 3 a bezpečnostních pravidel týkajících se úložiště, prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem uvedeným v čl. 64 odst. 2.

KAPITOLA VII
Ochrana údajů

Článek 40
Správce údajů

1. V souvislosti se zpracováním údajů ve sdílené službě pro porovnávání biometrických údajů (sdílená BMS) se orgány členských států, které jsou správci pro Eurodac, SIS a [systém ECRIS-TCN], rovněž považují za správce v souladu s čl. 4 odst. 7 nařízení

(EU) 2016/679, pokud jde o biometrické šablony získané z údajů uvedených v článku 13, které zadávají do příslušných systémů, a jsou odpovědné za zpracovávání biometrických šablon ve sdílené BMS.

2. V souvislosti se zpracováváním údajů ve společném úložišti údajů o totožnosti (CIR) se orgány členských států, které jsou správci pro Eurodac a [systém ECRIS-TCN], rovněž považují za správce v souladu s čl. 4 odst. 7 nařízení (EU) 2016/679, pokud jde o údaje uvedené v článku 18, které zadávají do příslušných systémů, a jsou odpovědné za zpracovávání osobních údajů v CIR.

3. Co se týče zpracování údajů v detektoru vícenásobné totožnosti:

   a) za správce údajů v souladu s čl. 2 písm. b) nařízení (ES) č. 45/2001 se ve vztahu ke zpracování osobních údajů ústřední jednotkou ETIAS považuje Evropská agentura pro pohraniční a pobřežní stráž;

   b) orgány členského státu, které doplňují nebo mění údaje v souboru údajů souvisejících s potvrzením totožnosti, se rovněž považují za správce v souladu s čl. 4 odst. 7 nařízení (EU) 2016/679 a jsou odpovědné za zpracovávání osobních údajů v detektoru vícenásobné totožnosti.

Článek 41
Zpracovatel údajů

V souvislosti se zpracováním osobních údajů v CIR se za zpracovatele údajů v souladu s čl. 2 písm. e) nařízení (ES) č. 45/2001 považuje agentura eu-LISA.

Článek 42
Bezpečnost zpracování

1. Agentura eu-LISA a orgány členských států zajistí bezpečnost zpracování osobních údajů, k němuž dochází v souladu s uplatňováním tohoto nařízení. Agentura eu-LISA, [ústřední jednotka ETIAS] a orgány členských států spolupracují při úkolech týkajících se bezpečnosti údajů.

2. Aniž je dotčen článek 22 nařízení (ES) č. 45/2001, 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, s cílem:

   a) fyzicky chránit údaje včetně pomocí plánů pro mimořádné situace pro ochranu kritické infrastruktury;

   b) zabránit neoprávněnému čtení, kopírování, změnám či odstranění nosičů dat;

   c) zabránit neoprávněnému vkládání údajů a neoprávněnému prohlížení, změnám nebo vymazávání uložených osobních údajů;

   d) zabránit neoprávněnému zpracovávání údajů a jakémukoli neoprávněnému kopírování, změnám nebo vymazávání údajů;

   e) zajistit, 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 totožnosti jednotlivých uživatelů a chráněných režimů přístupu k informacím;

f) zajistit, aby bylo možné ověřit a zjistit, kterým subjektům se mohou osobní údaje předávat prostřednictvím zařízení pro přenos údajů;

g) zajistit, aby bylo možné ověřit a zjistit, které údaje byly zpracovány složkami interoperability, kdy, kým a pro jaký účel;

h) zabránit neoprávněnému čtení, kopírování, změnám nebo vymazávání osobních údajů během jejich přenosu do složek interoperability a z nich nebo během přepravy nosičů dat, zejména prostřednictvím vhodných technik šifrování;

i) sledovat účinnost bezpečnostních opatření uvedených v tomto odstavci a přijmout nezbytná organizační opatření související s interním sledováním pro zajištění dodržování tohoto nařízení.

4. Členské státy přijmou opatření rovnocenná opatřením uvedeným v odstavci 3, pokud jde o zpracování osobních údajů orgány s oprávněným přístupem ke všem složkám interoperability.

Článek 43
Důvěrnost údajů SIS

1. Každý členský stát uplatní v souladu se svým vnitrostátním právem na všechny osoby a subjekty, které musí pracovat s údaji SIS dostupnými prostřednictvím složek interoperability, příslušná pravidla služebního tajemství nebo jiné srovnatelné povinnosti zachování důvěrnosti. Tato povinnost trvá i poté, co dotyčné osoby opustí svůj úřad nebo zaměstnanecký poměr, nebo poté, co dotyčné subjekty ukončí svou činnost.

2. Aniž je dotčen článek 17 služebního řádu úředníků Evropské unie a pracovního řádu ostatních zaměstnanců Unie, agentura eu-LISA použije na všechny své zaměstnance, kteří musí pracovat s údaji SIS, odpovídající pravidla služebního tajemství nebo jiné obdobné povinnosti zachování důvěrnosti, které jsou srovnatelné s normami stanovenými v odstavci 1. Tato povinnost trvá i poté, co dotyčné osoby opustí svůj úřad nebo zaměstnanecký poměr, nebo poté, co ukončí svou činnost.

Článek 44
Bezpečnostní incidenty

1. Každá událost, která má nebo může mít dopad na zabezpečení složek interoperability a může poškodit údaje v nich uložené 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, neporušenost 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 bezpečnostní incidenty Komisi, agentuře eu-LISA a evropskému inspektorovi ochrany údajů. V případě bezpečnostního incidentu v ústřední infrastruktuře složek interoperability uvědomí agentura eu-LISA Komisi a evropského inspektora ochrany údajů.

4. Informace o bezpečnostním incidentu, který má nebo může mít dopad na provoz složek interoperability nebo na dostupnost, neporušenost a důvěrnost údajů, jsou poskytnuty členským státům a nahlášeny v souladu s plánem pro řešení incidentů poskytnutým agenturou eu-LISA.

5. V případě bezpečnostního incidentu dotčené členské státy a agentura eu-LISA spolupracují. Komise stanoví parametry tohoto procesu spolupráce prostřednictvím prováděcích aktů. Tyto prováděcí akty se přijímají přezkumným postupem uvedeným v čl. 64 odst. 2.

Článek 45
Vlastní kontrola

Členské státy a příslušné subjekty EU zajistí, aby každý orgán, který má právo na přístup ke složkám interoperability, přijal opatření nezbytná pro dohled nad dodržováním tohoto nařízení a v případě potřeby spolupracoval s dozorovým úřadem.

Správci údajů uvedení v článku 40 přijmou nezbytná opatření pro dohled nad dodržováním zpracování údajů v souladu s tímto nařízením, a to včetně časté kontroly protokolů, a spolupracují podle potřeby s dozorovými úřady uvedenými v článcích 49 a 50.

Článek 46
Právo na informace

1. Aniž je dotčeno právo na informace uvedené v článcích 11 a 12 nařízení (ES) 45/2001 a článcích 13 a 14 nařízení (EU) 2016/679, musí být osoby, jejichž údaje jsou uloženy ve sdílené službě pro porovnávání biometrických údajů, společném úložišti údajů o totožnosti nebo v detektoru vícenásobné totožnosti, v době, kdy se jejich údaje shromažďují, informováni orgánem shromažďujícím jejich údaje o tom, že jejich osobní údaje jsou zpracovávány pro účely tohoto nařízení, a musí jim být poskytnuty kontaktní údaje příslušných správců údajů a informace o postupech pro výkon jejich práv na přístup, opravu a vymazání, jakož i kontaktní údaje evropského inspektora ochrany údajů a vnitrostátního dozorového úřadu v členském státě, který je odpovědný za shromažďování údajů.

2. Osoby, jejichž údaje jsou zaznamenány v Eurodacu nebo v [systému ECRIS-TCN], musí být informovány o zpracování údajů pro účely tohoto nařízení v souladu s odstavcem 1, pokud:

   a) – (nepoužije se);

   b) – (nepoužije se);

   c) – (nepoužije se);

   d) [žádost o mezinárodní ochranu je vytvořena nebo aktualizována v systému Eurodac v souladu s článkem 10 nařízení o Eurodacu];

   e) [datový záznam je vytvořen nebo aktualizován v systému ECRIS-TCN v souladu s článkem 5 nařízení o ECRIS-TCN.]

Článek 47
Právo na přístup, opravu a vymazání

1. Za účelem výkonu svých práv podle článků 13, 14, 15 a 16 nařízení (ES) č. 45/2001 a článků 15, 16, 17 a 18 nařízení (EU) 2016/679 má každá osoba právo obrátit se na

členský stát odpovědný za manuální ověření různých totožností nebo na jakýkoli členský stát, který žádost posoudí a odpoví na ni.

2. Členský stát odpovědný za manuální ověření různých totožností uvedené v článku 29 nebo členský stát, kterému byla žádost podána, na tuto žádost odpoví do 45 dnů od jejího přijetí.

3. Pokud je žádost o opravu nebo vymazání osobních údajů zaslána jinému členskému státu, než je odpovědný členský stát, členský stát, kterému byla žádost podána, se do sedmi dnů obrátí na orgány odpovědného členského státu a odpovědný členský stát do 30 dní ode dne, kdy se na něj tento členský stát obrátil, zkontroluje správnost údajů a zákonnost zpracování údajů.

4. Pokud je v návaznosti na toto přezkoumání zjištěno, že údaje uložené v detektoru vícenásobné totožnosti (MID) jsou věcně nesprávné nebo že byly zaznamenány nezákonně, odpovědný členský stát nebo případně členský stát, kterému byla žádost podána, tyto údaje opraví nebo vymaže.

5. Pokud jsou údaje v MID pozměněny odpovědným členským státem během doby jejich platnosti, provede odpovědný členský stát zpracování stanovené v článku 27 a případně článku 29, aby se určilo, zda se pozměněné údaje mají propojit. Pokud zpracování nevykáže žádný pozitivní nález, odpovědný členský stát nebo případně členský stát, kterému byla žádost podána, vymaže údaje ze souboru údajů souvisejících s potvrzením totožnosti. Pokud automatizované zpracování vykáže jeden či více pozitivních nálezů, odpovědný členský stát vytvoří nebo aktualizuje odpovídající propojení v souladu s příslušnými ustanoveními tohoto nařízení.

6. Pokud se odpovědný členský stát nebo případně členský stát, kterému byla žádost podána, domnívá, že údaje uložené v MID nejsou věcně nesprávné ani zaznamenané nezákonně, neprodleně přijme správní rozhodnutí a písemně vyrozumí dotčenou osobu, proč není ochoten opravit nebo vymazat údaje, které se jí týkají.

7. V tomto rozhodnutí se dotčené osobě poskytnou rovněž informace o tom, že má možnost napadnout rozhodnutí přijaté ve vztahu k žádosti podle odstavce 3, 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 příslušných vnitrostátních dozorových úřadů.

8. Jakákoli žádost podaná v souladu s odstavcem 3 musí obsahovat nezbytné informace pro zjištění totožnosti dotčené osoby. Uvedené informace se použijí výhradně k umožnění výkonu práv uvedených v odstavci 3 a ihned poté se vymažou.

9. Odpovědný členský stát nebo případně členský stát, kterému byla žádost podána, uchová písemný záznam o podání žádosti uvedené v odstavci 3 a způsobu, jakým byla vyřešena, a neprodleně jej zpřístupní vnitrostátním dozorovým úřadům příslušným k ochraně údajů.

Článek 48

Předávání osobních údajů třetím zemím, mezinárodním organizacím a soukromým subjektům

Osobní údaje uložené ve složkách interoperability nebo přístupné jejich prostřednictvím nesmějí být předány ani zpřístupněny žádné třetí zemi, mezinárodní organizaci ani soukromému subjektu.

Článek 49

Dozor vykonávaný vnitrostátním dozorovým úřadem

1. Dozorový úřad nebo dozorové úřady určené podle článku 49 nařízení (EU) 2016/679 zajistí, aby byl alespoň jednou za čtyři roky proveden audit operací zpracovávání údajů příslušnými vnitrostátními orgány podle příslušných mezinárodních auditorských standardů.
2. Členské státy zajistí, aby měly jejich orgány dozoru dostatek prostředků k plnění úkolů, které jim toto nařízení ukládá.

Článek 50

Dozor vykonávaný evropským inspektorem ochrany údajů

Evropský inspektor ochrany údajů zajistí, aby byl alespoň jednou za čtyři roky podle příslušných mezinárodních auditorských standardů proveden audit činností agentury eu-LISA souvisejících se zpracováváním osobních údajů. Zpráva o tomto auditu se zasílá Evropskému parlamentu, Radě, agentuře eu-LISA, Komisi a členským státům. Agentura eu-LISA má možnost se ke zprávám před jejich přijetím vyjádřit.

Článek 51

Spolupráce vnitrostátních dozorových úřadů s evropským inspektorem ochrany údajů

1. Evropský inspektor ochrany údajů jedná v úzké spolupráci s vnitrostátními dozorovými úřady, pokud se jedná o konkrétní problematiku vyžadující účast na vnitrostátní úrovni, zejména pokud evropský inspektor ochrany údajů nebo vnitrostátní dozorový úřad zjistí velké nesrovnalosti mezi postupy členských států nebo zjistí potenciálně nezákonné předávání prostřednictvím komunikačních kanálů složek interoperability nebo v souvislosti s otázkami týkajícími se provádění a výkladu tohoto nařízení, nastolenými jedním nebo více vnitrostátními dozorovými úřady.
2. V případech uvedených v odstavci 1 je nutno zajistit koordinovaný dohled v souladu s článkem 62 nařízení (EU) XXXX/2018 [revidované nařízení 45/2001].

KAPITOLA VIII
Oblasti odpovědnosti

Článek 52

Oblasti odpovědnosti agentury eu-LISA během fáze návrhu a vývoje

1. Agentura eu-LISA zajistí, aby ústřední infrastruktury složek interoperability byly provozovány v souladu s tímto nařízením.
2. Složky interoperability jsou umístěny v technických zařízeních agentury eu-LISA a zajišťují funkce stanovené tímto nařízením v souladu s podmínkami bezpečnosti, dostupnosti, kvality a rychlosti uvedenými v čl. 53 odst. 1.
3. Agentura eu-LISA odpovídá za vývoj složek interoperability, za veškeré změny nezbytné pro zajištění interoperability mezi ústředními systémy EES, VIS, [ETIAS], SIS a Eurodac a [ECRIS-TCN] a Evropským vyhledávacím portálem, sdílenou službou pro porovnávání biometrických údajů, společným úložištěm údajů o totožnosti a detektorem vícenásobné totožnosti.

Agentura eu-LISA navrhne fyzickou architekturu složek interoperability, včetně jejich komunikačních infrastruktur, jakož i technické specifikace a jejich vývoj, pokud jde o ústřední infrastrukturu a zabezpečenou komunikační infrastrukturu, které přijme správní rada s podmínkou kladného stanoviska Komise. Agentura eu-LISA rovněž provede veškeré nezbytné úpravy systémů SIS, Eurodac nebo [systému ECRIS-TCN] vyplývající ze zavedení 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 6, čl. 37 odst. 4, čl. 38 odst. 4, čl. 39 odst. 5 a čl. 44 odst. 5.

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

4. Během fáze návrhu a vývoje se ustaví rada pro řízení programu složená maximálně z 10 členů. Skládá se ze sedmi členů jmenovaných správní radou agentury eu-LISA, vybraných z jejích členů nebo náhradníků, dále z předsedy poradní skupiny pro interoperabilitu uvedené v článku 65, člena zastupujícího agenturu eu-LISA jmenovaného jejím výkonným ředitelem a 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 rozsáhlých informačních systémů řízených agenturou eu-LISA a které jsou 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 každý měsíc správní radě 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 legislativními nástroji upravujícími vývoj, zřizování, provoz a používání všech rozsáhlých informačních systémů řízených agenturou eu-LISA.

   Všechny cestovní výdaje a výdaje na pobyt, které vzniknou členům rady pro řízení programu, hradí agentura a obdobně se použije článek 10 jednacího řádu agentury eu-LISA. Služby sekretariátu rady pro řízení programu zajišťuje agentura eu-LISA.

   Poradní skupina pro interoperabilitu uvedená v článku 65 zasedá pravidelně až do zahájení provozu složek interoperability. Po každém zasedání 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 53
Oblasti odpovědnosti agentury eu-LISA po zahájení provozu

1. Po zahájení provozu každé složky interoperability je agentura eu-LISA odpovědná za technickou správu ústřední infrastruktury a vnitrostátních jednotných rozhraní. Ve spolupráci s členskými státy zajišťuje vždy nejlepší dostupnou technologii určenou na základě analýzy nákladů a přínosů. Agentura eu-LISA je rovněž odpovědná za technickou správu komunikační infrastruktury uvedené v článcích 6, 12, 17, 25 a 39.

   Technická správa složek interoperability sestává ze všech úkolů nezbytných pro zachování funkčnosti složek interoperability 24 hodin denně 7 dní v týdnu v souladu s tímto nařízením, zejména z údržby a technického rozvoje nezbytných k tomu, aby složky fungovaly na uspokojivé úrovni technické kvality, zejména co se týče doby odezvy na dotazování v ústředních databázích v souladu s technickými specifikacemi.

2. Aniž je dotčen článek 17 služebního řádu úředníků Evropské unie, použije agentura eu-LISA na všechny své pracovníky, kteří musí pracovat s údaji uloženými ve složkách interoperability, odpovídající pravidla zachování služebního tajemství nebo jiné srovnatelné povinnosti zachování důvěrnosti. Tato povinnost je zachována i poté, co dotyčné osoby opustí svou funkci nebo zaměstnanecký poměr, nebo poté, co ukončí svou činnost.

3. Agentura eu-LISA vyvine a spravuje mechanismus a postupy pro provádění kontrol kvality údajů uložených ve sdílené službě pro porovnávání biometrických údajů a ve společném úložišti údajů o totožnosti v souladu s článkem 37.

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

Článek 54
Oblasti odpovědnosti členských států

1. Každý členský stát odpovídá za:

   a) připojení ke komunikační infrastruktuře Evropského vyhledávacího portálu (ESP) a společného úložiště údajů o totožnosti (CIR);

   b) začlenění stávajících vnitrostátních systémů a infrastruktur do ESP, sdílené služby pro porovnávání biometrických údajů, CIR a detektoru vícenásobné totožnosti;

   c) organizaci, správu, provoz a údržbu své stávající vnitrostátní infrastruktury a jejího spojení se složkami interoperability;

   d) správu a úpravu přístupu pro řádně oprávněné pracovníky a řádně zmocněné pracovníky příslušných vnitrostátních orgánů do ESP, CIR a detektoru vícenásobné totožnosti v souladu s tímto nařízením a vypracovávání a pravidelnou aktualizaci seznamu těchto pracovníků a jejich profilů;

   e) přijetí legislativních opatření uvedených v čl. 20 odst. 3, aby se zajistil přístup do CIR pro účely zjištění totožnosti;

   f) manuální ověření různých totožností uvedené v článku 29;

g) zavedení požadavků na kvalitu údajů v informačních systémech EU a ve složkách interoperability;

h) 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 uvedené v čl. 4 odst. 24 s CIR.

Článek 54a
Povinnosti Europolu

1. Europol zajistí provedení vyhledávání, které požaduje ESP, v údajích Europolu a odpovídajícím způsobem upraví rozhraní pro údaje základního stupně ochrany (BPL) svých systémů Querying Europol Systems (QUEST).

2. Europol je odpovědný za řízení a opatření týkající se jeho řádně oprávněných pracovníků, aby v souladu s tímto nařízením mohli příslušně využívat Evropský vyhledávací portál a společné úložiště údajů o totožnosti a měli k nim přístup, a za vypracování a pravidelnou aktualizaci seznamu těchto pracovníků a jejich profilů.

Článek 55
Oblasti odpovědnosti ústřední jednotky ETIAS

Ústřední jednotka ETIAS odpovídá za:

a) manuální ověření různých totožností uvedené v článku 29;

b) odhalování vícenásobných identit mezi údaji uloženými v systému VIS, Eurodac a SIS uvedené v článku 59.

KAPITOLA IX
Závěrečná ustanovení

Článek 56
Podávání zpráv a statistiky

1. Výhradně pro účely podávání zpráv a statistiky, a aniž by byla možná individuální identifikace, mohou řádně oprávnění pracovníci příslušných orgánů členských států, Komise a agentury eu-LISA nahlížet do těchto údajů souvisejících s Evropským vyhledávacím portálem (ESP):

a) počet vyhledávání na uživatele profilu ESP;

b) – (nepoužije se).

2. Výhradně pro účely podávání zpráv a statistiky, a aniž by byla možná individuální identifikace, mohou řádně oprávnění pracovníci příslušných orgánů členských států, Komise a agentury eu-LISA nahlížet do těchto údajů souvisejících se společným úložištěm údajů o totožnosti:

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 vydávající země;

d) počet vyhledávání provedených s biometrickými údaji a bez nich.

3. Výhradně pro účely podávání zpráv a statistiky, a aniž by byla možná individuální identifikace, mohou řádně oprávnění pracovníci příslušných orgánů členských států, Komise a agentury eu-LISA nahlížet do těchto údajů souvisejících s detektorem vícenásobné totožnosti:

a) státní příslušnost, pohlaví a rok narození osoby;

b) druh cestovního dokladu a třípísmenný kód vydávající země;

c) počet vyhledávání provedených s biometrickými údaji a bez nich;

d) počet jednotlivých typů propojení.

4. Řádně oprávnění zaměstnanci Evropské agentury pro pohraniční a pobřežní stráž zřízené nařízením Evropského parlamentu a Rady (EU) 2016/1624[64] mají přístup k údajům uvedeným v odstavcích 1, 2 a 3 pro účely provádění analýz hrozeb a posuzování zranitelnosti podle článků 11 a 13 uvedeného nařízení.

5. Pro účely prvního odstavce tohoto článku ukládá agentura eu-LISA údaje uvedené v prvním odstavci tohoto článku v centrálním úložišti pro účely podávání zpráv a statistiky uvedené v kapitole VII tohoto nařízení. Údaje v úložišti neumožňují zjistit totožnost jednotlivců, ale umožňují orgánům uvedeným v odstavci 1 tohoto článku získávat zprávy a statistiky přizpůsobené jejich potřebám s cílem zvýšit účinnost hraničních kontrol, usnadnit orgánům vyřizování žádostí o víza a podpořit vytváření fakticky podložených politik Unie v oblasti migrace a bezpečnosti.

Článek 57
Přechodné období pro používání Evropského vyhledávacího portálu

Po dobu dvou let od data zahájení provozu ESP se neuplatní povinnosti uvedené v čl. 7 odst. 2 a 4 a používání ESP je nepovinné.

Článek 58
Přechodné období, které se uplatní na ustanovení o přístupu ke společnému úložišti údajů o totožnosti pro účely prosazování práva

Článek 22 se použije od data zahájení provozu uvedeného v čl. 62 odst. 1.

Článek 59
Přechodné období pro odhalování vícenásobné totožnosti

1. Po období jednoho roku poté, co agentura eu-LISA oznámí provedení testu uvedeného v čl. 62 odst. 1 písm. b) v souvislosti s detektorem vícenásobné totožnosti (MID), a před zahájením provozu MID je za zjišťování vícenásobné totožnosti s použitím údajů uložených v systémech VIS, Eurodac a SIS odpovědná ústřední jednotka ETIAS uvedená v [čl. 33 písm. a) nařízení (EU) 2016/1624]. Odhalování vícenásobné totožnosti se provádí pouze s použitím biometrických údajů v souladu s čl. 27 odst. 2 tohoto nařízení.

[64] Nařízení Evropského parlamentu a Rady (EU) 2016/1624 ze dne 14. září 2016 o Evropské pohraniční a pobřežní stráži 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).

2. Pokud je výsledkem vyhledávání jeden či více pozitivních nálezů a údaje o totožnosti v propojených souborech jsou shodné nebo podobné, vytvoří se v souladu s článkem 33 bílé propojení.

   Pokud je výsledkem vyhledávání jeden či více pozitivních nálezů a údaje o totožnosti v propojených souborech nelze považovat za podobné, vytvoří se v souladu s článkem 30 žluté propojení a uplatní se postup uvedený v článku 29.

   Pokud je výsledkem více pozitivních nálezů, vytvoří se se všemi údaji, které vedly k pozitivnímu nálezu, propojení.

3. Pokud se vytvoří žluté propojení v souladu s odstavcem 3, MID udělí přístup k údajům o totožnosti přítomným v různých informačních systémech ústřední jednotce ETIAS.

4. Pokud se vytvoří propojení se záznamem v SIS, který je jiný než záznam o odepření vstupu nebo o cestovním dokladu, jenž byl nahlášen jako ztracený či odcizený nebo prohlášen za neplatný, v souladu s článkem 24 nařízení o SIS v oblasti hraničních kontrol, resp. článkem 38 nařízení o SIS v oblasti prosazování práva, MID udělí přístup k údajům o totožnosti přítomným v různých informačních systémech centrále SIRENE členského státu, který záznam vytvořil.

5. Ústřední jednotka ETIAS nebo 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. Při odhalování vícenásobné totožnosti uvedené v tomto článku je ústřední jednotce ETIAS podle potřeby nápomocna agentura eu-LISA.

Článek 60
Náklady

1. Náklady vzniklé ve spojení se zřízením a provozem ESP, sdílené služby pro porovnávání biometrických údajů, společného úložiště údajů o totožnosti (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 tzv. hostingem 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 tzv. hosting vnitrostátních informačních systémů (prostory, instalace, elektřina, chlazení);

   c) fungování vnitrostátních informačních systémů (smlouvy s operátory a technickou podporou);

   d) návrh, vývoj, realizace, provoz a údržba vnitrostátních komunikačních sítí.

3. Náklady na určené orgány uvedené v čl. 4 odst. 24 jsou hrazeny jednotlivými členskými státy, resp. Europolem. Náklady na připojení určených orgánů k CIR jsou hrazeny jednotlivými členskými státy, resp. Europolem.

Článek 61
Oznámení

1. Členské státy oznámí agentuře eu-LISA orgány uvedené v článcích 7, 20, 21 a 26, které mohou využívat ESP, CIR a MID nebo k nim mají 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 62. V případě změn v tomto seznamu zveřejní agentura eu-LISA jednou za rok aktualizovaný konsolidovaný seznam.

2. Agentura eu-LISA oznámí Komisi úspěšné provedení testu uvedeného v čl. 62 odst. 1 písm. b).

3. Ústřední jednotka ETIAS oznámí Komisi úspěšné provedení přechodného opatření stanoveného v článku 59.

4. Komise zpřístupní členským státům a veřejnosti na nepřetržitě aktualizované veřejné webové stránce informace oznámené v souladu s odstavcem 1.

Článek 62
Zahájení provozu

1. Komise stanoví datum zprovoznění jednotlivých složek interoperability, jakmile jsou splněny tyto podmínky:

   a) jsou přijata opatření uvedená v čl. 8 odst. 2, čl. 9 odst. 7, čl. 28 odst. 5 a 6, čl. 37 odst. 4, čl. 38 odst. 4, čl. 39 odst. 5 a čl. 44 odst. 5;

   b) agentura eu-LISA oznámí úspěšné provedení souhrnného testu příslušné složky interoperability, který provede agentura eu-LISA spolu s členskými státy;

   c) agentura eu-LISA potvrdí, že byla provedena nezbytná technická a právní opatření týkající se shromažďování a předávání údajů uvedených v čl. 8 odst. 1 a v článcích 13, 19, 34 a 39 a oznámí je Komisi;

   d) členské státy učiní oznámení Komisi, jak je uvedeno v čl. 61 odst. 1;

   e) v souvislosti s detektorem vícenásobné totožnosti ústřední jednotka ETIAS učiní oznámení Komisi, jak je uvedeno v čl. 61 odst. 3.

2. Komise sdělí Evropskému parlamentu a Radě výsledky testu provedeného v souladu s odst. 1 písm. b).

3. Rozhodnutí Komise uvedené v odstavci 1 se zveřejní v *Úředním věstníku Evropské unie*.

4. Členské státy a Europol začnou používat složky interoperability ode dne stanoveného Komisí v souladu s odstavcem 1.

Článek 63
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. 8 odst. 2 a čl. 9 odst. 7 je svěřena Komisi na dobu neurčitou počínaje [*dnem vstupu tohoto nařízení v platnost*].

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 8 odst. 2 a čl. 9 odst. 7 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 o zdokonalení tvorby právních předpisů ze dne 13. dubna 2016.

5. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

6. Akt v přenesené pravomoci přijatý podle čl. 8 odst. 2 a čl. 9 odst. 7 vstoupí v platnost, pouze 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 64
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.

Článek 65
Poradní skupina

Agentura eu-LISA zřídí poradní skupinu a poskytne jí odborné poznatky související s interoperabilitou, zejména v souvislosti s přípravou svého ročního pracovního programu a výroční zprávy o činnosti. Během fáze návrhu a vývoje nástrojů interoperability se uplatní čl. 52 odst. 4 až 6.

Článek 66
Odborná příprava

Agentura eu-LISA plní úkoly související s poskytováním odborné přípravy zaměřené na technické aspekty používání složek interoperability podle nařízení (EU) č. 1077/2011.

Článek 67
Praktické pokyny

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

Článek 68
Sledování a hodnocení

1. Agentura eu-LISA zajistí zavedení postupů, které budou sledovat vývoj složek interoperability vzhledem k cílům v oblasti plánování a nákladů a dále budou sledovat fungování složek interoperability, pokud jde o porovnání jejich technických výstupů, nákladové efektivnosti, bezpečnosti a kvality služeb se stanovenými cíli.

2. Do [*šesti měsíců od vstupu tohoto nařízení v platnost* – Úřad pro publikace, nahraďte prosím skutečným datem] a poté každých šest měsíců během fáze vývoje složek interoperability předloží agentura eu-LISA Evropskému parlamentu a Radě zprávu o stavu vývoje složek interoperability. 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. Pro účely technické údržby má agentura eu-LISA přístup k potřebným informacím, které se týkají operací zpracovávání údajů složek interoperability.

4. Čtyři roky po zahájení provozu jednotlivých složek interoperability a poté vždy po čtyřech letech předloží agentura eu-LISA Evropskému parlamentu, Radě a Komisi zprávu o technickém fungování složek interoperability, včetně jejich zabezpečení.

5. Dále pak po uplynutí jednoho roku od jednotlivých zpráv agentury eu-LISA vytvoří Komise celkové hodnocení složek, které bude zahrnovat:

   a) posouzení provádění tohoto nařízení;

   b) posouzení dosažených výsledků ve vztahu ke stanoveným cílům a dopadu na základní práva;

   c) posouzení trvající platnosti výchozího principu složek interoperability;

   d) posouzení zabezpečení složek interoperability;

   e) posouzení všech faktorů včetně všech nepřiměřených dopadů na plynulost provozu na hraničních přechodech a faktorů majících dopady na souhrnný rozpočet Unie.

   Hodnocení zahrnují jakákoli nezbytná doporučení. Komise předloží tuto hodnotící zprávu Evropskému parlamentu, Radě, Evropskému inspektorovi ochrany údajů a Agentuře Evropské unie pro základní práva zřízené nařízením Rady (ES) č. 168/2007[65].

6. Členské státy a Europol poskytnou agentuře eu-LISA a Komisi informace nezbytné k vypracování zpráv uvedených v odstavcích 4 a 5. Tyto informace nesmějí ohrozit pracovní metody ani obsahovat informace, které prozrazují zdroje, pracovníky nebo informace o vyšetřování určených orgánů.

7. Agentura eu-LISA poskytne Komisi informace nezbytné k vypracování hodnocení uvedených v odstavci 5.

8. Všechny členské státy a Europol vypracují – při dodržení vnitrostátních právních předpisů o zveřejňování citlivých informací – výroční zprávu o efektivitě přístupu k údajům uloženým ve společném úložišti údajů o totožnosti pro účely prosazování práva, která obsahuje informace a statistické údaje o:

[65] 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).

a) přesném účelu nahlížení do údajů, včetně typu teroristického nebo závažného trestného činu,

b) oprávněných důvodech pro důvodné podezření, že se na podezřelou osobu, pachatele nebo oběť vztahuje nařízení o Eurodacu;

c) počtu žádostí o přístup do společného úložiště údajů o totožnosti pro účely prosazování práva;

d) počtu a typu případů, které byly završeny úspěšným zjištěním totožnosti;

e) potřebě a využití postupu pro výjimečně naléhavé případy včetně případů, kdy ústřední přístupový bod při ověření *ex post* výjimečnou naléhavost neuznalo.

Výroční zprávy členských států a Europolu se předají Komisi do 30. června následujícího roku.

Článek 69
Vstup v platnost a použitelnost

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

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

Ve Štrasburku dne

Za Evropský parlament	*Za Radu*
předseda	*předseda/předsedkyně*

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

1.2. Příslušné oblasti politik

1.3. Povaha návrhu/podnětu

1.4. Cíle

1.5. Odůvodnění návrhu/podnětu

1.6. Doba trvání akce a finanční dopad

1.7. Předpokládaný způsob řízení

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

2.2. Systém řízení a kontroly

2.3. Opatření k zamezení podvodů a nesrovnalostí

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

3.2. Odhadovaný dopad na výdaje

3.2.1. Odhadovaný souhrnný dopad na výdaje

3.2.2. Odhadovaný dopad na operační prostředky

3.2.3. Odhadovaný dopad na prostředky správní povahy

3.2.4. Soulad se stávajícím víceletým finančním rámcem

3.2.5. Příspěvky třetích stran

3.3. Odhadovaný dopad na příjmy

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Návrh nařízení Evropského parlamentu a Rady o zřízení interoperability mezi informačními systémy Evropské unie pro bezpečnost, správu hranic a řízení migrace.

1.2. Příslušné oblasti politik

Vnitřní věci (hlava 18)

1.3. Povaha návrhu/podnětu

X Návrh/podnět se týká **nové akce**

☐ Návrh/podnět se týká **nové akce následující po pilotním projektu / přípravné akci**[66]

☐ Návrh/podnět se týká **prodloužení stávající akce**

☐ Návrh/podnět se týká **akce přesměrované na jinou akci**

1.4. Cíle

1.4.1. Víceleté strategické cíle Komise sledované návrhem/podnětem

Správa hranic – záchrana životů a zabezpečení vnějších hranic

Složky interoperability vytvářejí příležitost lépe využívat informace obsažené ve stávajících systémech EU pro bezpečnost, správu hranic a řízení migrace. Tato opatření především zabraňují tomu, aby byla tatáž osoba vedena v různých systémech s různou totožností. V současnosti je možná jedinečná identifikace osoby v rámci daného systému, nikoli však napříč systémy. To může vést k chybným rozhodnutím orgánů, nebo toho mohou zneužívat cestují se zlými úmysly k zakrytí své pravé totožnosti.

Lepší výměna informací

Navrhovaná opatření také nabízejí zjednodušený, ale stále vymezený přístup donucovacích orgánů k těmto údajům. Na rozdíl od současnosti zde však je jediný soubor podmínek, spíše než různé soubory podmínek pro přístup ke každé sbírce údajů.

1.4.2. Specifické cíle a Specifický cíl č. [ ]

Zřízení složek interoperability má tyto obecné cíle:

a) zlepšit správu vnějších hranic;

b) pomáhat při prevenci a potírání nelegální migrace; a

c) přispívat k vysoké úrovni bezpečnosti v oblasti svobody, bezpečnosti a práva Unie, včetně zachovávání veřejné bezpečnosti a veřejného pořádku a ochrany bezpečnosti na územích členských států.

Cílů zajišťování interoperability se dosáhne těmito kroky:

[66] Uvedené v čl. 54 odst. 2 písm. a) nebo b) finančního nařízení.

a) zajištěním správného zjištění totožnosti osob;

b) přispíváním k boji proti podvodnému zneužívání totožnosti;

c) zlepšováním a slaďováním požadavků na kvalitu údajů jednotlivých informačních systémů EU;

d) usnadněním technického a provozního provádění stávajících a budoucích informačních systémů EU ze strany členských států;

e) posilováním, zjednodušováním a zajištěním jednotnějších podmínek pro bezpečnost a ochranu údajů, kterými se řídí příslušné informační systémy EU;

f) zjednodušením a zajištěním jednotnějších podmínek pro přístup k systémům EES, VIS, ETIAS a Eurodac pro účely prosazování práva;

g) podporou účelů systémů EES, VIS, ETIAS, Eurodac, SIS a systému ECRIS-TCN.

Příslušné aktivity ABM/ABB

Kapitola „Bezpečnost a ochrana svobod: vnitřní bezpečnost“

1.4.3. Očekávané výsledky a dopady

Upřesněte účinky, které by návrh/podnět měl mít na příjemce / cílové skupiny.

Obecné cíle tohoto podnětu vyplývají ze dvou cílů uvedených ve Smlouvě:

1. Zlepšovat správu vnějších hranic schengenského prostoru, vycházet z Evropského programu pro migraci a následných sdělení, včetně sdělení o ochraně a posílení Schengenu.

2. Přispívat k vnitřní bezpečnosti Evropské unie, vycházet z Evropského programu pro bezpečnost a z úsilí Komise o vytvoření účinné a skutečné bezpečnostní unie.

Specifické politické cíle tohoto podnětu o interoperabilitě jsou:

Návrh má tyto specifické cíle:

1. zajistit, aby koncoví uživatelé, zejména příslušníci pohraniční stráže, donucovacích orgánů, imigrační úředníci a soudní orgány získali rychlý, plynulý, systematický a řízený přístup k informacím, které potřebují pro plnění svých úkolů;

2. přinést řešení pro odhalování vícenásobných totožností propojených se stejným souborem biometrických údajů, s dvojím účelem zajistit správné zjištění totožnosti osob jednajících v dobré víře a bojovat proti podvodnému zneužívání totožnosti;

3. usnadnit kontroly totožnosti státních příslušníků třetích zemí na území členského státu ze strany policejních orgánů; a

4. usnadnit a zjednodušit přístup donucovacích orgánů k informačním systémům, jež neslouží k prosazování práva, na úrovni EU, pokud to je nezbytné pro prevenci, vyšetření, odhalení nebo stíhání závažné trestné činnosti a terorismu.

Aby byl splněn specifický cíl 1, bude vyvinut Evropský vyhledávací portál (ESP).

Aby byl splněn specifický cíl 2, bude zřízen detektor vícenásobné totožnosti (MID) podporovaný společným úložištěm údajů o totožnosti (CIR) a sdílenou službou pro porovnávání biometrických údajů (sdílená BMS).

Aby byl splněn specifický cíl 3, bude oprávněným úředním osobám udělen přístup do CIR pro účely zjištění totožnosti.

Aby byl splněn cíl 4, bude CIR obsahovat funkci označení pozitivního nálezu, která umožní dvoufázový postup pro přístup k systémům správy hranic pro účely prosazování práva.

Kromě těchto čtyř složek interoperability budou cíle popsané v oddíle 1.4.2 dále podporovány zřízením a správou univerzálního formátu pro zprávy (UMF) jako normy EU pro vývoj informačních systémů v oblasti spravedlnosti a vnitřních věcí a zřízením společného úložiště pro účely podávání zpráv a statistiky (CRRS).

1.4.4. Ukazatele výsledků a dopadů

Upřesněte ukazatele, podle kterých je možno uskutečňování návrhu/podnětu sledovat.

Každé z navrhovaných opatření vyžaduje vývoj a následnou údržbu a provoz dané složky.

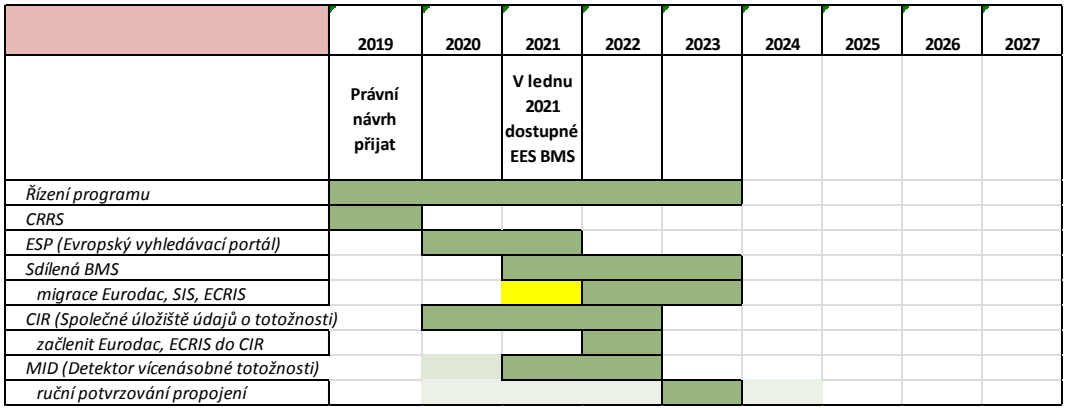
V průběhu vývoje

Vývoj každé složky bude prováděn po splnění nezbytných předpokladů, tj. právní návrh je přijat spolunormotvůrci a jsou splněny technické podmínky, jelikož některé složky lze vytvořit až poté, co je k dispozici jiná složka.

Specifický cíl: připravenost k provozu do cílového data

Do konce roku 2017 je návrh zaslán spolunormotvůrcům k přijetí. Předpokládá se, že proces přijímání bude dokončen během roku 2018, analogicky k době nutné pro jiné návrhy.

Podle tohoto předpokladu je začátek období vývoje stanoven na počátek roku 2019 (= T0) tak, aby existoval referenční bod, od kterého se počítají lhůty, nikoli absolutní data. Pokud k přijetí ze strany spolunormotvůrců dojde později, celý harmonogram se odpovídajícím způsobem posune. Na druhou stranu musí být sdílená BMS k dispozici předtím, než bude možné dokončit CIR a MID. Doba pro vývoj je uvedená v následující tabulce:



(Oddíl vyznačený žlutě se vztahuje na konkrétní úkol související se systémem Eurodac.)

– Společné úložiště pro účely podávání zpráv a statistiky (CRRS): lhůta: T0 + 12 měsíců (2019–2020)

– Evropský vyhledávací portál (ESP): lhůta: T0 + 36 měsíců (2019–2021)

– Sdílená služba pro porovnávání biometrických údajů (sdílená BMS) se nejprve vytvoří pro dodání Systému vstupu/výstupu (EES). Po dosažení tohoto milníku se aplikace, které budou využívat sdílenou BMS, musejí aktualizovat a údaje obsažené v systému automatizované identifikace otisků prstů (AFIS) SIS, Eurodac AFIS a údaje ECRIS-TCN se musejí migrovat do sdílené BMS. Lhůta pro dokončení je konec roku 2023.

– Společné úložiště údajů o totožnosti (CIR) se nejprve vytvoří při zavádění EES. Po dokončení EES se údaje ze systémů Eurodac a ECRIS zapracují do CIR. Lhůta pro dokončení je konec roku 2022 (dostupnost sdílené BMS + 12 měsíců).

– Detektor vícenásobné totožnosti (MID) se vytvoří po zprovoznění CIR. Lhůta pro dokončení je konec roku 2022 (dostupnost sdílené BMS + 24 měsíců), je zde však období, které je velmi náročné na zdroje, kdy se potvrzují propojení mezi totožnostmi, jež navrhuje MID. Každé z odhadnutých propojení je nutno manuálně potvrdit. To potrvá do konce roku 2023.

Období provozu začne po dokončení výše uvedeného období vývoje.

Provoz

Ukazatele související s každým specifickým cílem uvedeným v bodě 1.4.3 jsou následující:

1. Specifický cíl: Rychlý, plynulý a systematický přístup ke zdrojům údajů, k nimž je přístup oprávněn

– Počet realizovaných případů využití (= počet vyhledávání, který ESP může zpracovat) za časové období.

– Počet vyhledávání zpracovaných ze strany ESP ve srovnání s celkovým počtem vyhledávání (přes ESP a přes systémy přímo) za časové období.

2. Specifický cíl: Odhalovat vícenásobné totožnosti

– Počet totožností propojených se stejným souborem biometrických údajů v porovnání s počtem totožností s biografickou informací za časové období.

– Počet odhalených případů podvodného zneužití totožnosti v porovnání s počtem propojených totožností a celkovým počtem totožností za časové období.

3. Specifický cíl: Usnadnit zjišťování totožnosti státních příslušníků třetích zemí

– Počet vykonaných kontrol totožnosti v porovnání s celkovým počtem transakcí za časové období.

4. Specifický cíl: Zjednodušit přístup ke zdrojům údajů, k nimž je přístup oprávněn, pro účely prosazování práva

– Počet přístupů „1. fáze“ (= kontrola přítomnosti údajů) pro účely prosazování práva za časové období.

– Počet přístupů „2. fáze“ (= skutečné nahlížení do údajů ze systémů EU v oblasti působnosti) pro účely prosazování práva za časové období.

5. Doplňkový průřezový cíl: Zlepšování kvality údajů a využívání údajů pro lepší vytváření politik

– Pravidelné vydávání zpráv o sledování kvality údajů.

– Počet žádostí *ad hoc* o statistické informace za časové období.

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu

Jak dokládá posouzení dopadů připojené k tomuto právnímu návrhu, jednotlivé navrhované složky jsou pro dosažení interoperability nezbytné:

- Má-li být splněn cíl poskytnout oprávněným uživatelům rychlý, plynulý, systematický a řízený přístup k příslušným informačním systémům, měl by být vytvořen Evropský vyhledávací portál (ESP) vycházející ze sdílené BMS pro kontakty na všechny databáze.

- Má-li být splněn cíl usnadnit kontroly totožnosti státních příslušníků třetích zemí na území členského státu ze strany oprávněných pracovníků, mělo by vzniknout společné úložiště údajů o totožnosti (CIR) obsahující minimální soubor identifikačních údajů a vycházející z téže sdílené BMS.

- Má-li být splněn cíl odhalování vícenásobných totožností propojených se stejným souborem biometrických údajů, s dvojím účelem usnadňovat kontroly

totožnosti cestujících v dobré víře a potírat podvodné zneužívá totožnosti, měl by být vytvořen detektor vícenásobné totožnosti (MID) obsahující propojení mezi vícenásobnými totožnostmi napříč systémy.

• Má-li být splněn cíl usnadnění a zjednodušení přístupu donucovacích orgánů k informačním systémům, jež neslouží k prosazování práva, pro účely prevence, vyšetřování, odhalování nebo stíhání závažné trestné činnosti a terorismu, měla by být do společného úložiště údajů o totožnosti (CIR) začleněna funkce označení pozitivního nálezu.

Jelikož musejí být splněny všechny cíle, je úplným řešením kombinace ESP, CIR (s funkcí označení pozitivního nálezu) a MID, všechny vycházející ze sdílené BMS.

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší efektivnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota vyplývající ze zásahu Unie, jež doplňuje hodnotu, která by se jinak vytvořila činností samotných členských států.

Je zapotřebí činnost na celoevropské úrovni, protože systémy, jejichž interoperabilita je navrhována, jsou systémy, které využívá více členských států: buď všechny členské státy (v případě systému Eurodac), nebo všechny členské státy, které jsou součástí schengenského prostoru (systémy EES, VIS, ETIAS a SIS). Z definice nelze tedy postupovat na jiné úrovni.

Hlavní očekávanou přidanou hodnotou je eliminovat případy podvodného zneužívání totožnosti, zmapovat případy, kdy konkrétní osoba využila různé totožnosti pro vstup do EU, a zabránit tomu, aby osoby jednající v dobré víře byly zaměňovány za osoby se stejným jménem, ale jednající se zlými úmysly. Další přidanou hodnotou je, že zde navrhovaná interoperabilita umožňuje snazší zavádění a údržbu rozsáhlých informačních systémů EU. Pro donucovací orgány by navrhovaná opatření měla vést k častějšímu a úspěšnějšímu přístupu ke konkrétním údajům v rozsáhlých informačních systémech EU. Na provozní úrovni lze kvalitu údajů udržet a zlepšit pouze tehdy, pokud probíhá její sledování. Pro vytváření politik a rozhodování je nutné umožnit *ad hoc* vyhledávání anonymizovaných údajů.

Součástí posouzení dopadu je analýza nákladů a přínosů a bere do úvahy pouze ty přínosy, které lze kvantifikovat, očekávané přínosy pak lze odůvodněně očekávat ve výši 77,5 milionu EUR za rok a těžily by z nich hlavně členské státy. Příčinou těchto přínosů jsou především:

– Nižší náklady na změny vnitrostátních aplikací, když je v provozu ústřední systém (odhadem 6 milionů EUR ročně pro oddělení zabývající se informačními technologiemi v členských státech).

– Úspora nákladů plynoucí z využití jedné ústřední sdílené BMS namísto jedné BMS na každý ústřední systém obsahující biometrické údaje (odhadem 1,5 milionu EUR ročně a jednorázová úspora 8 milionů EUR pro agenturu eu-LISA).

– Úspora nákladů na identifikaci vícenásobných totožností v porovnání se situací, kdy by se shodných výsledků dosahovalo bez navrhovaných prostředků. To by znamenalo úsporu ve výši alespoň 50 milionů EUR ročně pro členské státy v oblasti správy hranic, řízení migrace a prosazování práva.

– Úspora nákladů na odborné vzdělávání velké skupiny koncových uživatelů v porovnání se situací, kdy je vzdělávání nutné opakovaně, v odhadované výši 20

milionů EUR ročně pro členské státy v oblasti správy hranic, řízení migrace a prosazování práva.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

Ze zkušeností s vývojem Schengenu druhé generace (SIS II) a Vízového informačního systému (VIS) lze vytěžit následující ponaučení:

1. Aby bylo možné zabránit překračování nákladů a vzniku zpoždění kvůli měnícím se požadavkům, neměl by se v prostoru svobody, bezpečnosti a práva vyvíjet žádný nový informační systém, zejména pokud zahrnuje rozsáhlý informační systém, aniž by byly nejprve s konečnou platností přijaty základní právní nástroje, které stanoví jeho účel, oblast působnosti, funkce a technické podrobnosti.

2. V případě SIS II a VIS mohl být vnitrostátní vývoj těchto systémů v členských státech spolufinancován z Fondu pro vnější hranice (EBF), avšak nebylo to povinné. Nebylo tudíž možné získat přehled o míře pokroku v těch členských státech, které nestanovily příslušné činnosti v rámci svého víceletého programování nebo jejich programování nebylo přesné. Proto se nyní navrhuje, aby Komise proplatila veškeré náklady na integraci vzniklé členským státům, aby bylo možné sledovat pokrok v tomto vývoji.

3. S ohledem na usnadnění obecné koordinace provádění budou všechny navrhované výměny zpráv mezi vnitrostátními a ústředními systémy využívat stávající sítě a vnitrostátní jednotné rozhraní.

1.5.4. Soulad a možná synergie s dalšími vhodnými nástroji

Soulad se stávajícím víceletým finančním rámcem

Nařízení o ISF – hranice je finanční nástroj, do nějž byl začleněn rozpočet na provedení iniciativy týkající se interoperability.

V čl. 5 písm. b) stanoví, že 791 milionů EUR je nutno realizovat v rámci programu na vývoj systémů informačních technologií založených na stávajících nebo nových systémech na podporu řízení migračních toků přes vnější hranice Unie, s výhradou přijetí příslušných právních předpisů Unie a při dodržení podmínek stanovených v článku 15. Z těchto 791 milionů EUR je vyhrazeno 480,2 milionu EUR na vývoj systému EES, 210 milionů EUR na systém ETIAS a 67,9 milionu EUR na revizi systému SIS II. Zbývající částka (32,9 milionu EUR) má být přerozdělena s využitím mechanismů ISF – hranice. Tento návrh požaduje 32,1 milionu EUR na stávající období víceletého finančního rámce, které spadá do zbývajícího rozpočtu.

Tento návrh vyžaduje rozpočet 424,7 milionu EUR celkem (včetně okruhu 5) na období od roku 2019 do roku 2027. Stávající víceletý finanční rámec pokrývá pouze dvouleté období let 2019 a 2020. Náklady však jsou odhadovány až do roku 2027 včetně, aby se zajistil informovaný náhled na finanční dopady tohoto návrhu a aniž by byl předjímán příští víceletý finanční rámec.

Rozpočet požadovaný na období devíti let dosahuje částky 424,7 milionu EUR a pokrývá i následující položky:

1) 136,3 milionu EUR pro členské státy na pokrytí změn vnitrostátních systémů pro použití složek interoperability, NUI od agentury eu-LISA a rozpočet na odbornou přípravu značné komunity koncových uživatelů. Není zde žádný dopad na stávající víceletý finanční rámec, jelikož finanční zdroje jsou poskytovány od roku 2021 dále.

2) 4,8 milionu EUR pro Evropskou agenturu pro pohraniční a pobřežní stráž (EBCG) na hostování týmu specialistů, kteří budou během jednoho roku (2023) potvrzovat propojení mezi totožnostmi v okamžiku spuštění MID. Činnosti týmu lze spojit s odstraňováním nejednoznačnosti v souvislosti s totožností, které je přiděleno agentuře EBCG v rámci návrhu ETIAS. Není zde žádný dopad na stávající víceletý finanční rámec, jelikož finanční zdroje jsou poskytovány od roku 2021 dále.

3) 48,9 milionu EUR pro Europol na pokrytí modernizace IT systémů Europolu na objem zpráv, které budou zpracovávány, a na vyšší výkonnostní úroveň. Složky interoperability budou využívány systémem ETIAS pro nahlížení do údajů Europolu. Aktuální kapacita zpracování informací ze strany Europolu však není v souladu se značnými objemy (průměrně 100 000 dotazů za den) a se zkrácenou dobou odezvy. Celkem 9,1 milionu EUR se vynaloží v rámci stávajícího víceletého finančního rámce.

4) 2,0 milionu EUR pro CEPOL na pokrytí přípravy a poskytnutí odborného vzdělávání provozním pracovníkům. Celkem 0,1 milionu EUR je naplánováno na rok 2020.

5) 225,0 milionu EUR pro agenturu eu-LISA, což pokrývá celkové náklady na vývoj programu, který zajistí všech pět složek interoperability (68,3 milionu EUR), náklady na údržbu od okamžiku dodání složek až do roku 2027 (56,1 milionu EUR), zvláštní rozpočet 25,0 milionu EUR pro migraci údajů ze stávajících systémů do sdílené BMS a další náklady na aktualizaci NUI, síť, odbornou přípravu a zasedání. Zvláštní rozpočet 18,7 milionu EUR pokrývá náklady na modernizaci a provoz ECRIS-TCN v režimu vysoké dostupnosti od roku 2022. Z celkové částky se 23,0 milionu EUR vynaloží během stávajícího víceletého finančního rámce.

6) 7,7 milionu EUR pro GŘ HOME na pokrytí omezeného navýšení počtu zaměstnanců a souvisejících nákladů ve vývojovém období různých složek, jelikož Komise také převezme odpovědnost za výbor zabývající se univerzálním formátem pro zprávy (UMF). Tento rozpočet spadající do okruhu 5 nebude pokryt rozpočtem ISF. Pro informaci je v období 2019–2020 splatných 2,0 milionu EUR.

Soulad s předchozími iniciativami

Tato iniciativa je v souladu s následujícími:

V dubnu 2016 představila Komise **sdělení *Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost*** zaměřené na řešení řady strukturálních nedostatků v informačních systémech. Z něho vyplynuly tři akce:

Nejprve Komise přijala **kroky k posílení a maximalizaci přínosů stávajících informačních systémů**. V prosinci 2016 Komise přijala návrhy na další posílení stávajícího Schengenského informačního systému (SIS). Mezitím, po návrhu Komise z května 2016, byla urychlena jednání o revidovaném právním základu pro Eurodac – databázi EU s otisky prstů žadatelů o azyl. Návrh nového právního základu pro Vízový informační systém (VIS) se také připravuje a bude předložen ve druhém čtvrtletí roku 2018.

Zadruhé Komise navrhla **další informační systémy k řešení zjištěných mezer** v architektuře EU pro správu údajů. Jednání o návrhu Komise z dubna 2016 zřítit systém vstupu/výstupu (EES)[67] – s cílem zlepšit postupy hraničních kontrol pro státní příslušníky třetích zemí cestující do EU – byla uzavřena již v červenci 2017, kdy

[67] COM(2016) 194 ze dne 6. dubna 2016.

spolunormotvůrci nalezli politickou shodu, již potvrdil Evropský parlament v říjnu 2017 a v listopadu 2017 ji formálně schválila Rada. V listopadu 2016 Komise také představila návrh na zřízení evropského systému pro cestovní informace a povolení (ETIAS)[68]. Tento návrh má posílit bezpečnostní kontroly cestujících bez vízové povinnosti tím, že umožní předem provádět kontroly zaměřené na nelegální migraci a bezpečnostní rizika. V současnosti probíhají jednání mezi spolunormotvůrci. V červnu 2017 byl také navržen Evropský informační systém rejstříků trestů pro státní příslušníky třetích zemí (systém ECRIS-TCN)[69] s cílem řešit mezeru odhalenou v souvislosti s výměnou informací mezi členskými státy ohledně odsouzených státních příslušníků třetích zemí.

Zatřetí Komise pracovala **na interoperabilitě informačních systémů** se zaměřením na čtyři možnosti představené ve sdělení z dubna 2016[70] k dosažení interoperability. Tři ze čtyř možností jsou jmenovitě ESP, CIR a sdílená BMS. Následně bylo zjevné, že je nutno rozlišit mezi CIR jako databází totožností a novou složkou, která identifikuje vícenásobné totožnosti propojené s tímtéž biometrickým identifikátorem (MID). Čtyři složky tedy nyní jsou: ESP, CIR, MID a sdílená BMS.

Synergický účinek

Synergie se zde chápe jako přínos, kterého se dosahuje opětovným použitím stávajících řešení a předcházením dalším novým investicím.

Zásadní synergický účinek lze spatřit mezi těmito iniciativami a vývojem systému EES a ETIAS.

Pro fungování systému EES se vytvoří individuální soubor pro všechny státní příslušníky třetích zemí, kteří vstupují do schengenského prostoru za účelem krátkodobého pobytu. Pro tento účel bude stávající systém porovnávání biometrických údajů používaný pro VIS, který obsahuje šablony otisků prstů pro všechny cestující s vízovou povinností, rozšířen tak, aby zahrnoval i biometrické údaje od cestujících bez vízové povinnosti. Sdílená BMS je tedy koncepčně dalším zobecněním nástroje na porovnávání biometrických údajů, který vznikne jako součást EES. Biometrické šablony obsažené v nástroji na porovnávání biometrických údajů SIS a Eurodac pak budou migrovány (jde o technický termín, kdy se údaje přesouvají z jednoho systému do druhého) do uvedené sdílené BMS. Podle údajů dodavatelů jsou náklady na uložení v oddělených databázích průměrně 1 EUR na soubor biometrických údajů (celkem existuje potenciálně 200 milionů datových souborů), zatímco po vzniku řešení sdílené BMS klesnou průměrné náklady na 0,35 EUR na soubor biometrických údajů. Vyšší náklady na hardware nezbytný pro vysoký objem údajů tyto přínosy částečně stírají, ale v konečném důsledku se náklady na sdílenou BMS odhadují o 30 % nižší než při uložení shodných údajů ve více menších systémech BMS.

Pro provoz ETIAS musí být daná složka dostupná pro dotazování sady systémů EU. Použije se buď ESP, nebo se vytvoří zvláštní složka v rámci návrhu ESP. Návrh týkající se interoperability umožňuje vybudovat jednu složku namísto dvou.

Dosahuje se zde synergického účinku i díky opětovnému použití stejného vnitrostátního jednotného rozhraní (NUI), které se používá pro EES a ETIAS. NUI bude nutno aktualizovat, ale bude se používat i nadále.

[68] COM(2016) 731 ze dne 16. listopadu 2016.
[69] COM(2017) 344 ze dne 29. června 2017.
[70] COM(2016) 205 ze dne 6. dubna 2016.

1.6. Doba trvání akce a finanční dopad

☐ **Časově omezený** návrh/podnět

– ☐ Návrh/podnět s platností od [DD/MM]RRRR do [DD/MM]RRRR

– ☐ Finanční dopad od RRRR do RRRR

☒ **Časově neomezený** návrh/podnět

– Období vývoje od roku 2019 do roku 2023 včetně, poté provoz v plném rozsahu.

– Časové období finančního dopadu je tedy uvedeno pro roky 2019 až 2027.

1.7. Předpokládaný způsob řízení[71]

☒ **Přímé řízení** Komisí

– X prostřednictvím jejích útvarů, včetně jejích zaměstnanců v delegacích Unie;

– ☐ prostřednictvím výkonných agentur

☒ **Sdílené řízení** s členskými státy

☒ **Nepřímé řízení**, při kterém jsou úkoly souvisejícími s plněním rozpočtu pověřeny:

– ☐ třetí země nebo subjekty určené těmito zeměmi;

– ☐ mezinárodní organizace a jejich agentury (upřesněte);

– ☐EIB a Evropský investiční fond;

– ☒ subjekty uvedené v článcích 208 a 209 finančního nařízení;

– ☐ veřejnoprávní subjekty;

– ☐ soukromoprávní subjekty pověřené výkonem veřejné služby v rozsahu, v jakém poskytují dostatečné finanční záruky;

– ☐ soukromoprávní subjekty členského státu pověřené uskutečňováním partnerství soukromého a veřejného sektoru a poskytující dostatečné finanční záruky;

– ☐ osoby pověřené prováděním zvláštních činností v rámci společné zahraniční a bezpečnostní politiky podle hlavy V Smlouvy o EU a určené v příslušném základním právním aktu.

– *Pokud vyberete více způsobů řízení, upřesněte je v části „Poznámky“.*

Poznámky

Bloky	Fáze vývoje	Provozní fáze	Způsob řízení	Aktér
Vývoj a údržba (složek interoperability pro ústřední systémy, vzdělávání týkající se systémů)	X	X	Nepřímý	eu-LISA Europol CEPOL
Migrování údajů (migrování	X	X	Nepřímý	eu-LISA

[71] Vysvětlení způsobů řízení spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Bloky	Fáze vývoje	Provozní fáze	Způsob řízení	Aktér
biometrických šablon do sdílené BMS), náklady sítě, aktualizace NUI, zasedání a odborná příprava				
Potvrzování propojení při vytváření MID	X	–	Nepřímý	Evropská agentura pro pohraniční a pobřežní stráž
Přizpůsobení NUI, začlenění vnitrostátních systémů a odborná příprava koncových uživatelů	X	X	Sdílené (nebo přímé) (1)	COM + Členské státy

1) Do tohoto nástroje nejsou zahrnuty žádné částky na provozní fázi.

Období vývoje začíná v roce 2019 a trvá do dodání každé složky, probíhá od roku 2019 do roku 2023 (viz oddíl 1.4.4).

1. Přímé řízení ze strany GŘ HOME: Během období vývoje mohou být podle potřeby některé kroky realizovány přímo Komisí. Sem by mohla patřit zejména finanční podpora Unie pro činnosti v podobě grantů (včetně grantů vnitrostátním orgánům členských států), smlouvy na veřejné zakázky a/nebo úhrada nákladů externích odborníků.

2. Sdílené řízení: Během fáze vývoje budou členské státy muset přizpůsobit své vnitrostátní systémy pro přístup k ESP namísto jednotlivých systémů (toto platí pro odchozí zprávy z členských států) a pro změny v odpovědích na jejich žádosti o vyhledávání (příchozí zprávy směrem k členským státům). Proběhne také aktualizace stávajícího NUI realizovaného pro EES a ETIAS.

3. Nepřímé řízení: Agentura eu-LISA pokryje vývojovou část všech okruhů informačních technologií projektu, tj. složek interoperability, aktualizace vnitrostátního jednotného rozhraní (NUI) v každém členském státě, aktualizace komunikační infrastruktury mezi ústředními systémy a vnitrostátními jednotnými rozhraními, migrace biometrických šablon ze stávajících systémů pro porovnávání biometrických údajů SIS a Eurodac do sdílené BMS a činnost čištění údajů, která s tím souvisí.

Během provozního období bude agentura eu-LISA vykonávat všechny technické činnosti související s údržbou složek.

Evropská agentura pro pohraniční a pobřežní stráž (EBCG) začlení další tým vyhrazený na potvrzování propojení poté, co dojde ke zprovoznění MID. Tento úkol je časově omezený.

Europol pokryje vývoj a údržbu svých systémů tak, aby se zajistila interoperabilita s ESP a ETIAS.

CEPOL připraví a dodá odbornou přípravu provozním službám metodou školení školitelů.

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Pravidla pro sledování a podávání zpráv pro vývoj a údržbu dalších systémů:

1. Agentura eu-LISA zajistí zavedení postupů, které budou sledovat vývoj složek interoperability vzhledem k cílům v oblasti plánování a nákladů a dále budou sledovat fungování složek, pokud jde o cíle týkající se technických výstupů, nákladové efektivnosti, bezpečnosti a kvality služeb.

2. Do šesti měsíců od vstupu tohoto nařízení v platnost a následně každých šest měsíců během fáze vývoje složek předloží agentura eu-LISA Evropskému parlamentu a Radě zprávu o stavu vývoje každé složky. Po ukončení vývoje bude Evropskému parlamentu a Radě předložena zpráva, která podrobně vysvětlí, jak byly splněny cíle týkající se zejména plánování a nákladů, a odůvodní případné odchylky.

3. Pro účely technické údržby má agentura eu-LISA přístup k potřebným informacím, které se týkají operací zpracovávání údajů prováděných ve složkách.

4. Čtyři roky po zahájení provozu poslední provedené složky a poté vždy po čtyřech letech předloží agentura eu-LISA Evropskému parlamentu, Radě a Komisi zprávu o technickém fungování složek.

5. Pět let po zahájení provozu poslední provedené složky a poté každé čtyři roky vypracuje Komise celkové hodnocení a učiní veškerá nezbytná doporučení. Toto celkové hodnocení musí zahrnovat: výsledky, jichž bylo dosaženo ze strany složek vzhledem k jejich cílům v oblasti interoperability, údržby, výkonnosti a finančních důsledků a dopadu na základní práva.

Komise předloží tuto hodnotící zprávu Evropskému parlamentu a Radě.

6. Členské státy a Europol poskytnou agentuře eu-LISA a Komisi informace nezbytné pro vypracování zpráv uvedených v odstavcích 4 a 5 v souladu s kvantitativními ukazateli předem stanovenými Komisí a/nebo agenturou eu-LISA. Tyto informace nesmějí ohrozit pracovní metody ani obsahovat informace, které odhalují zdroje, totožnosti pracovníků nebo vyšetřování určených orgánů.

7. Agentura eu-LISA poskytne Komisi informace nezbytné k vypracování celkových hodnocení podle odstavce 5.

8. Všechny členské státy a Europol vypracují – při dodržení vnitrostátních právních předpisů o zveřejňování citlivých informací – výroční zprávy o efektivitě přístupu k údajům systémů EU pro účely prosazování práva, které obsahují informace a statistické údaje o:

– přesném účelu nahlížení do údajů, včetně typu teroristického nebo závažného trestného činu,

– oprávněných důvodech pro důvodné podezření, že se na podezřelou osobu, pachatele nebo oběť vztahuje toto nařízení;

– počtu žádostí o přístup do složek pro účely prosazování práva;

– počtu a typu případů, které byly završeny úspěšným zjištěním totožnosti;

– potřebě a využití postupu pro výjimečně naléhavé případy včetně případů, kdy ústřední přístupový bod při ověření *ex post* výjimečnou naléhavost neuznal.

Výroční zprávy členských států a Europolu se předají Komisi do 30. června následujícího roku.

2.2. Systém řízení a kontroly

2.2.1. Zjištěná rizika

Rizika se týkají vývoje pěti složek informačních technologií ze strany externího dodavatele řízeného agenturou eu-LISA. Jde o běžná rizika projektu:

1. riziko nedokončení projektu včas;

2. riziko nedokončení projektu s dodržením rozpočtu;

3. riziko nedodání projektu v plném rozsahu.

První riziko je nejvýznamnější, jelikož překročení termínu vede k vyšším nákladům, protože většina nákladů se vztahuje k časovému období: náklady na zaměstnance, náklady na licence placené ročně atd.

Tato rizika lze zmírnit použitím technik projektového řízení, včetně mimořádných událostí v projektech vývoje a zajištění dostatečného počtu pracovníků tak, aby bylo možno zvládat i pracovní špičku. Odhad zátěže se obvykle provádí na základě předpokladu rovnoměrně rozloženého pracovního zatížení v čase, zatímco ve skutečnosti projekty vykazují nerovnoměrné zatížení, které se řeší vyšší alokací zdrojů.

Existuje několik rizik spojených s využíváním externích dodavatelů pro tyto vývojové práce:

1. zejména riziko, že dodavatel na projekt nevyčlení dostatečné zdroje nebo že navrhne a vyvine systém, který nebude technicky aktuální;

2. riziko, že dodavatel nebude plně dodržovat administrativní techniky a metody pro rozsáhlé informační projekty za účelem snížení nákladů;

3. nelze zcela vyloučit riziko, že dodavatel bude čelit finančním obtížím z důvodů, jež nesouvisejí s tímto projektem.

Tato rizika jsou zmírňována udělováním zakázek na základě přísných kritérií kvality, kontrolou referencí na dodavatele a udržováním pevných vztahů s nimi. Jako poslední možnost lze pak podle potřeby použít přísné doložky o pokutách a výpovědní doložky.

2.2.2. Informace o zavedeném systému vnitřní kontroly

Agentura eu-LISA má být centrem excelence v oblasti vývoje a řízení rozsáhlých informačních systémů. Má vykonávat činnosti související s vývojem a provozem různých složek interoperability včetně údržby vnitrostátního jednotného rozhraní v členských státech.

Během fáze vývoje bude veškeré činnosti související s vývojem vykonávat agentura eu-LISA. Tím bude pokryt vývoj všech oblastí projektu. Náklady související se začleněním systémů v členských státech během vývoje bude řídit Komise prostřednictvím sdíleného řízení nebo grantů.

Během provozní fáze bude agentura eu-LISA odpovědná za technické a finanční řízení složek používaných na ústřední úrovni, zejména udělování a řízení smluv. Finanční prostředky pro členské státy na výdaje na vnitrostátní jednotky bude Komise řídit prostřednictvím ISF – hranice (vnitrostátní programy).

Aby se zabránilo zpoždění na vnitrostátní úrovni, je třeba před zahájením vývoje plánovat účinné řízení mezi všemi zúčastněnými stranami. Komise předpokládá, že interoperabilní architektura bude vymezena na začátku projektu tak, aby ji bylo možno použít v projektech EES a ETIAS, jelikož tyto projekty dodávají a využívají sdílenou BMS, společné úložiště údajů o totožnosti a Evropský vyhledávací portál. Člen týmu projektového řízení projektu interoperability by měl být součástí struktury řízení projektu EES a ETIAS.

2.2.3. Odhad nákladů a přínosů kontrol a posouzení očekávané míry rizika výskytu chyb

Není poskytován žádný odhad, jelikož kontrola a zmírňování rizik jsou nedílnou součástí struktury řízení projektu.

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření.

Zamýšlená opatření pro boj proti podvodům jsou stanovena v článku 35 nařízení (EU) č. 1077/2011, jenž stanoví:

1. Za účelem boje proti podvodům, úplatkářství a jakékoli jiné nedovolené činnosti se použije nařízení (ES) č. 1073/1999.

2. Agentury přistoupí k interinstitucionální dohodě o vnitřním vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF) a neprodleně vydají odpovídající předpisy platné pro všechny jejich zaměstnance.

3. Rozhodnutí o financování a prováděcí dohody a nástroje z nich vyplývající výslovně stanoví, že Účetní dvůr a OLAF mohou v případě potřeby provádět kontroly na místě u příjemců finančních prostředků od agentur a zaměstnanců zodpovědných za přidělování těchto prostředků.

V souladu s tímto ustanovením přijala správní rada Evropské agentury pro provozní řízení rozsáhlých informačních systémů v rámci prostoru svobody, bezpečnosti a práva dne 28. června 2012 rozhodnutí týkající se požadavků a podmínek vnitřních šetření v souvislosti s předcházením podvodům, korupci a jiným protiprávním činnostem poškozujícím zájmy Unie.

Použije se strategie GŘ HOME pro předcházení podvodům a jejich odhalování.

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

ODHADOVANÝ DOPAD NA VÝDAJE A ZAMĚSTNANCE NA ROK 2021 A NÁSLEDUJÍCÍ ROKY V TOMTO LEGISLATIVNÍM FINANČNÍM VÝKAZU SE DOPLŇUJE POUZE PRO ORIENTACI A NEPŘEDJÍMÁ PŘÍŠTÍ VÍCELETÝ FINANČNÍ RÁMEC

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

- Stávající rozpočtové položky

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdaje	Příspěvek			
	číslo [název……...……]	RP/NRP[72]	zemí ESVO[73]	kandidátských zemí[74]	třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení
3	18.02.01.03 – Inteligentní hranice	RP	Ne	Ne	Ano	Ne
3	18.02.03 – Evropská agentura pro pohraniční a pobřežní stráž (Frontex)	RP	Ne	Ne	Ano	Ne
3	18.02.04 – EUROPOL	RP	Ne	Ne	Ne	Ne
3	18.02.05 – CEPOL	NRP	Ne	Ne	Ne	Ne
3	18.02.07 – Evropská agentura pro provozní řízení rozsáhlých informačních systémů v oblasti svobody, bezpečnosti a práva (eu-LISA)	RP	Ne	Ne	Ano	Ne

[72] RP = rozlišené prostředky / NRP = nerozlišené prostředky.
[73] ESVO: Evropské sdružení volného obchodu.
[74] Kandidátské země a případně potenciální kandidátské země západního Balkánu.

3.2. Odhadovaný dopad na výdaje

[Tento oddíl se vyplní pomocí **tabulky rozpočtových údajů správní povahy** (druhý dokument v příloze tohoto finančního výkazu) a pro účely konzultace mezi útvary se vloží do aplikace DECIDE.]

3.2.1. Odhadovaný souhrnný dopad na výdaje

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce	3	Bezpečnost a občanství

GŘ Home			Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**Rok 2028**	**CELKEM**
• Operační prostředky													
18.02.01.03 – Inteligentní hranice	Závazky	(1)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Platby	(2)	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300
Prostředky správní povahy financované z rámce na zvláštní programy[75]													
Číslo rozpočtové položky		(3)											
CELKEM prostředky pro GŘ HOME	Závazky	=1+1a +3)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Platby	=2+2a +3	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300

Výdaje pokryjí náklady související s/se:

– Náklady na úpravu NUI (vnitrostátního jednotného rozhraní), jehož vývoj je financován v rámci návrhu EES, rozpočtovaná částka na změny systémů v členských státech s cílem zapracovat změny ústředních systémů a rozpočtovaná částka na odbornou přípravu koncových uživatelů.

[75] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

18.0203 – EBCG			Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
Hlava 1: Výdaje na zaměstnance	Závazky	(1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Platby	(2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Hlava 2: Výdaje na infrastrukturu a provoz	Závazky	(1a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Platby	(2a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Hlava 3: Provozní výdaje	Závazky	(3a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Platby	(3b)	0	0	0	0,183	2,200	0	0	0	0	2,383
CELKEM prostředky za Europol	(Závazky celkem = platby celkem)	=1+1a +3a	**0**	**0**	**0**	**0,776**	**4,744**	**0,402**	**0**	**0**	**0**	**5,923**

– Rozpočet pro EBCG pokrývá výdaje týmu určeného pro potvrzování propojení generovaných z MID (detektoru vícenásobné totožnosti) u původních údajů (přibližně 14 milionů záznamů). Objem propojení, která mají být manuálně potvrzena, se odhaduje přibližně na 550 000. Vyhrazený tým zřízený pro tento účel se přidá k týmu EBCG zřízenému pro ETIAS, jelikož je to z hlediska funkce blízké, a předejde se tak nákladům na zřízení nového týmu. Práce by měla proběhnout v roce 2023. Smluvní zaměstnanci se tudíž najímají až 3 měsíce předem a jejich smlouva se ukončuje až 2 měsíce po konci migrování. Další část požadovaných zdrojů se nenajímá jako smluvní zaměstnanci a bude se najímat jako konzultanti. Tím se objasňují náklady v hlavě 3 pro rok 2023. Předpokládá se jejich najímání jeden měsíc předem. Další údaje o počtech zaměstnanců jsou uvedeny později.

– Hlava 1 proto zahrnuje náklady na 20 interních zaměstnanců a prostředky pro posílení vedoucích a podpůrných pracovníků.

– Hlava 2 obsahuje další náklady na hostování 10 dalších zaměstnanců dodavatele.

– Hlava 3 obsahuje poplatek za 10 dalších zaměstnanců dodavatele. Žádné jiné druhy nákladů nejsou zahrnuty.

18.0204 – Europol			Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
Hlava 1: Výdaje na zaměstnance	Závazky	(1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Platby	(2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952

Hlava 2: Výdaje na infrastrukturu a provoz	Závazky	(1a)	0	0	0	0	0	0	0	0	0	0
	Platby	(2a)	0	0	0	0	0	0	0	0	0	0
Hlava 3: Provozní výdaje	Závazky	(3a)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
	Platby	(3b)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
CELKEM prostředky za Europol	(Závazky celkem = platby celkem)	=1+1a +3a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

Výdaje Europolu pokryjí modernizaci schopnosti systémů IKT Europolu vypořádat se s objemem zpráv, které je třeba zpracovat, a požadované navýšení úrovní výkonnosti (čas odezvy).

Hlava 1 výdaje na zaměstnance pokrývá náklady související s dalšími pracovníky IKT, kteří budou najímáni pro posílení informačních systémů Europolu z výše uvedených důvodů. Další údaje související s rozdělením pozic mezi dočasnými pracovníky a smluvními pracovníky a jejich odborností jsou uvedeny níže.

Hlava 3 zahrnuje náklady na hardware a software nezbytné pro posílení informačních systémů Europolu. Informační systémy Europolu v současnosti slouží omezené a pevně dané komunitě Europolu, styčným důstojníkům a vyšetřovatelům Europolu v členských státech, kteří tyto systémy využívají pro účely analýz a vyšetřování. Se zavedením rozhraní QUEST (systémové rozhraní, které umožní ESP vyhledávat údaje Europolu) na základní úrovni ochrany (informační systémy Europolu jsou nyní akreditovány až do úrovně *EU restricted* a *EU confidential*) budou informační systémy Europolu dostupné mnohem širší komunitě oprávněných donucovacích orgánů. Kromě těchto navýšení bude ETIAS využívat ESP pro automatické vyhledávání údajů Europolu při zpracovávání cestovních povolení. Tím se zvýší objem dotazů směřujících na údaje Europolu ze současných přibližně 107 000 dotazů měsíčně na více než 100 000 dotazů denně, bude také nezbytná non-stop dostupnost informačních systémů Europolu a velmi krátký čas odezvy, aby se splnily požadavky stanovené nařízením ETIAS. Většina nákladů se omezuje na období před zprovozněním složek interoperability, ale některé probíhající závazky jsou nezbytné k zajištění vysoké a nepřerušené dostupnosti informačních systémů Europolu. Pro zavedení složek interoperability ze strany Europolu jako uživatele je také zapotřebí provést několik činností v oblasti vývoje.

18.0205 – CEPOL			Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
Hlava 1: Výdaje na	Závazky	(1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210

zaměstnance	Platby	(2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Hlava 2: Výdaje na infrastrukturu a provoz	Závazky	(1a)	0	0	0	0	0	0	0	0	0	0
	Platby	(2a)	0	0	0	0	0	0	0	0	0	0
Hlava 3: Provozní výdaje	Závazky	(3a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Platby	(3b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
CELKEM prostředky za CEPOL	(Závazky celkem = platby celkem)	=1+1a +3a	0	0,144	0,384	0,482	0,208	0,208	0,208	0,208	0,208	2,050

Odborná příprava koordinovaná centrálně na úrovni EU zlepšuje soudržné zavádění vzdělávacích kurzů na vnitrostátní úrovni, a tím zaručuje správné a úspěšné zavedení a využití složek interoperability. CEPOL – jako Agentura Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva – má dobrou pozici pro poskytování vzdělávání na centrální úrovni EU. Tyto výdaje pokrývají přípravu „školení pro školitele z členských států“ nezbytného k využívání ústředních systémů poté, co budou interoperabilní. Mezi náklady patří ty, které souvisejí s malým navýšením počtu zaměstnanců agentury CEPOL pro koordinaci, řízení, organizaci a aktualizaci kurzů, a náklady na dodání určitého počtu školení za rok a přípravu on-line kurzu. Podrobnosti týkající se těchto nákladů jsou objasněny níže. Úsilí v oblasti odborné přípravy se soustředí na období bezprostředně předcházející uvedení do provozu. I po uvedení do provozu je nezbytné pokračující úsilí, jelikož interoperabilní složky vyžadují údržbu a školiteli nejsou vždy tytéž osoby, jak vyplývá ze zkušeností s poskytováním stávající odborné přípravy v oblasti schengenského informačního systému.

18.0207 – eu-LISA			Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
Hlava 1: Výdaje na zaměstnance	Závazky	(1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
	Platby	(2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Hlava 2: Výdaje na infrastrukturu a provoz	Závazky	(1a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
	Platby	(2a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Hlava 3: Provozní výdaje	Závazky	(3a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309

	Platby	(3b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
CELKEM prostředky pro eu-LISA	(Závazky celkem = platby celkem)	=1+1a +3a	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**

Tyto výdaje pokryjí:

– Vývoj a údržbu čtyř složek interoperability (Evropského vyhledávacího portálu (ESP), sdílené služby pro porovnávání biometrických údajů (sdílené BMS), společného úložiště údajů o totožnosti (CIR) a detektoru vícenásobné totožnosti (MID) zahrnutých do právního návrhu a společného úložiště pro účely podávání zpráv a statistiky (CRRS). Agentura eu-LISA bude působit jako zástupce vlastníka projektu a využívat vlastní zaměstnance pro návrhy specifikací, výběr dodavatelů, řízení práce, předkládání výsledků souboru zkoušek a přijímání odvedené práce.

– Náklady související s migrováním údajů z dřívějších systémů do nových složek. Agentura eu-LISA však nemá žádnou přímou úlohu v úvodním nahrání údajů pro MID (potvrzování propojení), jelikož jde o činnost zaměřenou na samotný obsah údajů. Migrování biometrických údajů z dřívějších systémů se zabývá formátem a značením údajů, nikoli obsahem údajů.

– Náklady na modernizaci a přesunutí provozu ECRIS-TCN na systém vysoké dostupnosti od roku 2022. ECRIS-TCN je ústřední systém obsahující rejstříky trestů s údaji o státních příslušnících třetích zemí. Podle plánu by se měl systém stát dostupný do roku 2020. Očekává se, že složky interoperability budou využívat přístup i ke zmíněnému systému, který by se tudíž měl také stát systémem vysoké dostupnosti. Provozní výdaje zahrnují i další náklady na dosažení této vysoké dostupnosti. Pro rok 2021 je plánován značný výdaj na vývoj a poté průběžné náklady na údržbu a provoz. Tyto náklady nejsou zahrnuty do legislativního finančního výkazu revize zřizovacího nařízení agentury eu-LISA[76], který obsahuje pouze rozpočty od roku 2018 do roku 2020, a tedy nedochází k překrývání s tímto rozpočtovým požadavkem.

– Vzorec výdajů je výsledkem sekvence projektu. Jelikož jednotlivé složky nejsou navzájem nezávislé, období vývoje sahá od roku 2019 do roku 2023. Od roku 2020 však již začíná údržba a provoz prvních dostupných složek. Tím se objasňuje pomalý start výdajů, jejich zvyšování a pak pokles na stálou hodnotu.

– Výdaje v rámci hlavy 1 (výdaje na zaměstnance) sledují sekvenci projektu: více zaměstnanců je nutných k dodání projektu s dodavatelem (jehož výdaje jsou uvedeny v hlavě 3). Po dodání projektu se část týmu dodávky přesune na oblast rozvoje a údržby. Zároveň se zvýší počet zaměstnanců určených na provoz nově dodaných systémů.

[76] COM 2017/0145 (COD) Návrh nařízení Evropského parlamentu a Rady o Evropské agentuře pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva a o změně nařízení (ES) č. 1987/2006 a rozhodnutí Rady 2007/533/SVV a zrušení nařízení (EU) č. 1077/2011.

– Výdaje uvedené v hlavě 2 (výdaje na infrastrukturu a provoz) pokrývají další kancelářské prostory na dočasné hostování týmů dodavatele pověřených vývojem, údržbou a provozními úkoly. Vzorec výdajů v čase tudíž také sleduje vývoj počtu zaměstnanců. Náklady na hostování dalšího vybavení již jsou zahrnuty do rozpočtu agentury eu-LISA. Neexistují také žádné další výdaje na hostování zaměstnanců agentury eu-LISA, jelikož ty jsou již zapracovány do standardních nákladů na zaměstnance.

– Výdaje uvedené v hlavě 3 (provozní výdaje) zahrnují náklady na dodavatele na vývoj a údržbu systému, pořízení zvláštního hardwaru a softwaru.
Náklady na dodavatele začínají studiemi pro specifikaci složek a vývoj začíná pouze pro jednu složku (CRRS). Za období let 2020–2022 se pak náklady zvyšují, jelikož se souběžně vyvíjí více složek. Po dosažení vrcholu náklady neklesají, protože úkoly související s migrováním údajů jsou v tomto projektovém portfoliu obzvláště náročné. Náklady na dodavatele pak klesají, jelikož složky jsou dodány a uvedou se do provozního režimu, což vyžaduje stabilní vzorec zdrojů.
Souběžně s výdaji uvedenými v hlavě 3 se výdaje v roce 2020 prudce zvýší v porovnání s předchozím rokem, a to kvůli počáteční investici do hardwaru a softwaru, které jsou během vývoje nezbytné. Výdaje uvedené v hlavě 3 (provozní výdaje) náhle vzrostou v roce 2021 a 2022, protože investiční náklady na hardware a software pro provozní prostředí informačních technologií (produkční a předprodukční fáze jak pro ústřední jednotku, tak i pro záložní ústřední jednotku) vzniknou v roce před uvedením do provozu, totéž platí pro složky interoperability (CIR a MID) s vysokými nároky na software a hardware. Po zprovoznění jsou náklady na hardware a software převážně v úrovni nákladů na údržbu.

– Další podrobnosti jsou uvedeny dále.

Okruh víceletého finančního rámce	**5**	„Správní výdaje“

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
GŘ HOME										
• Lidské zdroje Číslo rozpočtové položky: 18.01	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Ostatní správní výdaje (zasedání atd.)	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727

GŘ HOME CELKEM	Prostředky	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

CELKEM prostředky na OKRUH 5 víceletého finančního rámce	(Závazky celkem = platby celkem)	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	Rok 2028	**CELKEM**
CELKEM prostředky z OKRUHU 1 až 5 víceletého finančního rámce	Závazky	**7,533**	**26,569**	**104,672**	**98,591**	**83,363**	**25,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**
	Platby	**7,533**	**26,569**	**96,042**	**97,591**	**83,993**	**34,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**

3.2.2. Odhadovaný dopad na operační prostředky

3.2.2.1. Odhadovaný dopad na prostředky agentury EBCG

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

– ☒ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uveďte cíle a výstupy **Agentura EBCG** ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**CELKEM**	
	Druh 77	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 1[78] Potvrzení propojení																						
Počet zaměstnanců najatých jako odborníci k potvrzování propojení	Náklady na dodavatele		0	0	0	0	0	0	0.8	0,183	10	2,200	0	0	0	0	0	0	0	0		2,383
Mezisoučet za specifický cíl č. 1			**0**	**0**	**0**	**0**	**0**	**0**	**0.8**	**0,183**	**10**	**2,200**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**2,383**

Tyto výdaje pokryjí:

– Nábor dostatečného počtu dalších pracovníků (odhadem přibližně 10 odborníků) ke stávajícím interním zaměstnancům (odhadem přibližně 20 osob), kteří budou působit v EBCG za účelem potvrzování propojení. Pro dosažení požadovaného množství zaměstnanců se plánuje nábor pouze jeden měsíc před datem spuštění.

[77] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

[78] Popsaný v bodě 1.4.2. „Specifické cíle…“.

– Nejsou odhadovány žádné další náklady na dodavatele. Požadovaný software je součástí nákladů na licence sdílené BMS. Neexistuje žádná specifická hardwarová kapacita v oblasti zpracovávání. Zaměstnanci dodavatele by měli působit v EBCG. Z tohoto důvodu je ve výdajích uvedených v hlavě 2 přidán roční náklad na průměrně 12 čtverečních metrů na osobu.

3.2.2.2. Odhadovaný dopad na prostředky Europolu

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

– ☒ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uveďte cíle a výstupy **Europol** ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**CELKEM**	
	Druh 79	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 1[80] Vývoj a údržba systémů (Europol)																						
Prostředí informačních technologií	Infrastruktura					1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096
Prostředí informačních technologií	Hardware					3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144
Prostředí informačních technologií	Software					0,670		0,670		0,268		0,268		0,268		0,268		0,268		0,268		2,948

[79] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

[80] Popsaný v bodě 1.4.2. „Specifické cíle…“.

Vývojové práce	Dodavatel				0,360		0,360												0,720
Mezisoučet			**0**		**6,380**		**6,380**		**2,408**		**2,408**		**2,408**		**7,758**		**7,758**		**2,408**		**37,908**

Tyto výdaje pokryjí nutnost posílit informační systémy a infrastrukturu Europolu pro zvládnutí rostoucího počtu dotazů. Mezi tyto náklady patří:

– modernizace bezpečnosti a síťové infrastruktury, hardwaru (servery, úložiště) a softwaru (licence). Tuto modernizaci je nutno dokončit před zprovozněním Evropského vyhledávacího portálu a ETIAS v roce 2021, náklady byly rozloženy rovnoměrně mezi roky 2020 a 2021. Od roku 2022 byla pro výpočet nákladů na údržbu použita roční sazba na údržbu ve výši 20 %. Dále byl zohledněn standardní pětiletý cyklus výměny zastaralého hardwaru a infrastruktury.

– Náklady na dodavatele na vývojové práce pro zavedení nástroje QUEST na základní úrovni ochrany.

3.2.2.3. Odhadovaný dopad na prostředky CEPOL

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

– ☒ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uveďte cíle a výstupy CEPOL ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**CELKEM**	
	Druh [81]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 1[82] Vývoj a dodání vzdělávacích kurzů																						
Počet rezidenčních kurzů	0,34 na kurz		0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788
On-line školení	0,02			0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052
Mezisoučet				**0**		**0,040**		**0,176**		**0,274**		**0,070**		**0,070**		**0,070**		**0,070**		**0,070**		**0,840**

[81] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

[82] Popsaný v bodě 1.4.2. „Specifické cíle…“.

Aby se zajistila rovnoměrnost zavádění a využívání řešení pro interoperabilitu, bude odborná příprava organizována jak na ústřední úrovni EU prostřednictvím CEPOL, tak i členskými státy. Výdaje na odbornou přípravu na úrovni EU zahrnují:

– vývoj společného vzdělávacího programu, který členské státy využijí při provádění vnitrostátní odborné přípravy;

– rezidenční činnosti pro školení školitelů. Během dvou let bezprostředně po zprovoznění řešení pro interoperabilitu se očekává zavedení školicích programů v širším rozsahu, později budou udržovány v rozsahu dvou rezidenčních vzdělávacích kurzů ročně.

– on-line kurz na doplnění rezidenčních činností na úrovni EU a v členských státech.

3.2.2.4. Odhadovaný dopad na prostředky agentury eu-LISA

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

– ☒ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uveďte cíle a výstupy **eu-LISA** ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**CELKEM**	
	Druh 83	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 1[84] Vývoj složek interoperability																						
Vybudované systémy	Dodavatel			1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Softwarové produkty	Software			0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202
Hardwarové produkty	Hardware			0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133
Odborná příprava v oblasti výpočetní techniky	Odborná příprava a další			0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340

[83] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

[84] Popsaný v bodě 1.4.2. „Specifické cíle…“.

Mezisoučet za specifický cíl č. 1		**2,390**		**11,151**		**28,879**		**16,131**		**6,830**		**1,815**		**0,415**		**0,335**		**0,335**		**68,281**

– Tento cíl zahrnuje pouze náklady na dodávku čtyř složek interoperability a CRRS.

– Náklady na sdílenou BMS byly odhadnuty s ohledem na předpoklad, že systém EES, jehož vývoj se připravuje, bude sloužit jako základní systém pro vývoj. Proto se plánuje znovu použít licence k softwaru pro biometrické údaje (36 milionů EUR), jež jsou započteny pro systém EES.

– V tomto rozpočtu se sdílená BMS rozpočtově posuzuje jako další rozšíření BMS pro EES. Proto aktuální finanční výkaz zahrnuje marginální náklady na softwarové licence (6,8 milionu EUR) na přidání přibližně 20 milionů souborů biometrických údajů obsažených v systému SIS AFIS (AFIS je systém automatizované identifikace otisků prstů = „BMS“ v rámci SIS), Eurodac AFIS a v budoucím ECRIS-TCN (Evropský informační systém rejstříků trestů pro státní příslušníky třetích zemí) do BMS dodané pro EES. Náklady na začlenění různých systémů (SIS, Eurodac, ECRIS-TCN) do sdílené BMS jsou zahrnuty v tomto finančním výkazu.

– V rámci činností za období 2019 a 2020, bude agentura eu-LISA vyzvána ke zpracování přesného technického řešení, které nelze definovat v okamžiku předkládání právního návrhu, a k odhadnutí nákladových dopadů na zavedení upřednostňovaného technického řešení. Z tohoto důvodu může dojít ke změně oproti zde uvedenému odhadu nákladů.

– Všechny složky se dodají do konce roku 2023, proto se k tomuto datu výdaje na dodavatele snižují téměř na nulu. Zůstává pouze zbytková částka za opakující se aktualizaci CRSS.

– Za období let 2019 až 2021 se výdaje na softwarové vybavení výrazně zvyšují, jelikož náklady na softwarové licence vznikají za různá prostředí nezbytná pro produkci, předprodukci a testování, a to v ústředním i záložním zařízení. Některé specifické a nezbytné softwarové složky jsou dále naceněny podle počtu „odkazovaných objektů“ (neboli objemu údajů). Jelikož databáze bude v konečném důsledku obsahovat přibližně 220 milionů totožností, je cena za software úměrná této hodnotě.

Uveďte cíle a výstupy eu-LISA ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**CELKEM**	
	Druh [85]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL č. 2 Údržba a provoz složek interoperability																						
Systémy udržované v provozuschopném stavu	Dodavatel			0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501
Softwarové produkty	Software			0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032
Hardwarové produkty	Hardware			0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423
Odborná příprava v oblasti výpočetní techniky	Odborná příprava			0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150
Mezisoučet za specifický cíl č. 2				**0**		**0,325**		**0,325**		**3,567**		**10,034**		**10,464**		**10,464**		**10,464**		**10,464**		**56,105**

[85] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

– Údržba bude zahájena bezprostředně po dodání některých složek. Rozpočet pro dodavatele údržby je tedy zahrnut již od okamžiku dodání ESP (v roce 2021). Rozpočet na údržbu se zvyšuje s dodávkou dalších složek, pak dosahuje víceméně stálé hodnoty představující procentní podíl (15 až 22 %) počáteční investice.

– Údržba hardwaru a softwaru začíná od roku zahájení provozu: vývoj nákladů je obdobný jako v případě nákladů na dodavatele.

Uveďte cíle a výstupy eu-LISA ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**CELKEM**	
	Druh 86	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 3[87] Migrace dat																						
Dřívější data BMS migrována	Do sdílené BMS			0		0		0		7,000		3,000		0		0		0		0		10,000
Dřívější data EDAC připravena k migraci	Změna návrhu a přepracování EDAC			0		0		7,500		7,500				0		0		0		0		15,000
Mezisoučet za specifický cíl č. 3				**0**		**0**		**7,500**		**14,500**		**3,000**										**25,000**

– V případě projektu sdílené BMS je nutno migrovat údaje z ostatních biometrických nástrojů do sdílené BMS, jelikož tento společný systém je provozně účinnější a také přináší finanční výhodu v porovnání se situací, kdy by pokračovala údržba více menších systémů BMS.

– Současná obchodní logika systému Eurodac není jednoznačně oddělena od mechanismů pro porovnávání biometrických údajů, jak tomu je se službou BMS, která funguje se systémem VIS. Interní fungování systému Eurodac a mechanismus, jakým se obchodní služby obracejí na

[86] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

[87] Popsaný v bodě 1.4.2. „Specifické cíle…“.

základní služby pro porovnávání biometrických údajů, je pro pozorovatele zvenčí černou skříňkou a vychází z chráněné technologie. Nebude možné pouze migrovat data do sdílené BMS a zachovat stávající obchodní vrstvu. Proto migraci údajů doprovázejí značné náklady na změnu komunikačních mechanismů s ústřední aplikací Eurodac.

Uveďte cíle a výstupy **eu-LISA** ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**CELKEM**	
	Druh [88]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 4[89] Síť																						
Síťová připojení	Nastavení sítě			0		0		0		0,505										0		0,505
Zpracovaný síťový provoz	Síťové operace			0		0						0,246		0,246		0,246		0,246		0,246		1,230
Mezisoučet za specifický cíl č. 4				**0**		**0**		**0**		**0,505**		**0,246**		**0,246**		**0,246**		**0,246**		**0,246**		**1,735**

– Složky interoperability mají na síťový provoz jen okrajový vliv. Co se týče údajů, vytvářejí se propojení pouze mezi stávajícími údaji, což je maloobjemová položka. Zde zahrnuté náklady znamenají pouze okrajové navýšení rozpočtu nad rámec rozpočtů na systémy EES a ETIAS pro nastavení sítě a provoz.

[88] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).
[89] Popsaný v bodě 1.4.2. „Specifické cíle…“.

Uveďte cíle a výstupy eu-LISA ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**CELKEM**	
	Druh [90]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 5[91] Aktualizace NUI																						
NUI po aktualizaci	Dodavatel			0		0		0		0,505		0,505								0		1,010
Mezisoučet za specifický cíl č. 5				**0**		**0**		**0**		**0,505**		**0,505**										**1,010**

– Návrh systému EES zavedl koncepci vnitrostátního jednotného rozhraní (NUI), jehož vývoj a údržbu má zajistit agentura eu-LISA. V tabulce výše je uveden rozpočet pro aktualizaci rozhraní NUI na další druh výměny informací. Provoz rozhraní NUI neznamená žádné další náklady, ty již byly rozpočtovány v rámci návrhu systému EES.

[90] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).
[91] Popsaný v bodě 1.4.2. „Specifické cíle…“.

Uveďte cíle a výstupy eu-LISA ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**CELKEM**	
	Druh[92]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 6: Zasedání a odborná příprava																						
Měsíční zasedání o pokroku (Vývoj)	0,021 na zasedání x 10 za rok		10	*0,210*	10	*0,210*	10	*0,210*	10	*0,210*											40	0,840
Čtvrtletní zasedání (provoz)	0,021 x 4 za rok		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Poradní skupiny	0,021 x 4 za rok		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Školení členských států	0,025 na školení		2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150
Mezisoučet za specifický cíl č. 6			20	**0,428**	22	**0,478**	22	**0,478**	24	**0,528**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**		**3,502**

[92] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

– Mezisoučet 6 zahrnuje náklady na zasedání pořádaná řídicím orgánem (v tomto případě agenturou eu-LISA) pro účely řízení projektu. Jedná se o náklady na další zasedání za účelem dodávky složek interoperability.

– Mezisoučet 6 zahrnuje náklady na zasedání agentury eu-LISA s pracovníky z členských států, kteří se zabývají vývojem, údržbou a provozem složek interoperability a organizací a dodávkou odborné přípravy pro pracovníky z oblasti informačních technologií z členských států.

– Během vývoje zahrnuje rozpočet 10 projektových zasedání za rok. Jakmile je provoz připravován (tato situace nastane od roku 2019 dále), uskuteční se ročně čtyři zasedání. Na vyšší úrovni se od počátku zřídí poradní skupina za účelem provádění prováděcích rozhodnutí Komise. Plánují se čtyři zasedání ročně stejně jako pro stávající poradní skupiny. Agentura eu-LISA navíc připraví a dodá odbornou přípravu pro pracovníky z oblasti informačních technologií v členských státech. Jde o odbornou přípravu zaměřenou na technické aspekty složek interoperability.

Uveďte cíle a výstupy **eu-LISA** ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**CELKEM**	
	Druh [93]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 7[94] Vysoká dostupnost systému ECRIS-TCN																						
Systém s vysokou dostupností	Nastavení systému			0		0		8,067												0		8,067

[93] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

[94] Popsaný v bodě 1.4.2. „Specifické cíle…“.

Provozy s vysokou dostupností	Systém udržován a provozován		0		0		0		1,768		1,768		1,768		1,768		1,768		1,768		10,608
Mezisoučet za specifický cíl č. 4			**0**		**0**		**8,067**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**18,675**

– Cíl 7 se týká systému ECRIS-TCN a spočívá v přechodu ze systému se „standardní“ dostupností na systém s vysokou dostupností. Uvedenou modernizací, která vyžaduje především pořízení dalšího hardwaru, by systém ECRIS-TCN prošel v roce 2021. Vzhledem k tomu, že systém ECRIS-TCN má být podle plánu hotov v roce 2020, nabízí se vytvářet tento systém již od začátku jako systém s vysokou dostupností a integrovat jej se složkami interoperability. Jelikož však mnoho projektů závisí jeden na druhém, opatrnost velí nečinit takový předpoklad a rozpočtovat oddělené postupy. Tento rozpočet je dodatečným rozpočtem k nákladům na vývoj, údržbu nebo provoz systému ECRIS-TCN v letech 2019 a 2020.

3.2.2.5. Odhadovaný dopad na prostředky GŘ Home

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

– ☒ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uveďte cíle a výstupy **GŘ Home** ⇩			Rok **2019**		Rok **2020**		Rok **2021**		Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		**CELKEM**	
	Druh 95	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 1: Začlenění vnitrostátních systémů (členských států (ČS))																						
Rozhraní NUI připraveno k použití	Úpravy rozhraní NUI – vývoj						30	3,150	30	3,150											30	6,300
Systémy ČS upravené pro interoperabilitu	Náklady na začlenění						30	40,000	30	40,000	30	40,000									30	120,000

[95] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

Proškolení koncoví uživatelé	10 000 školení koncových uživatelů celkem při 1 000 EUR za školení							5 000	5,000	5 000	5,000									10 000	10,000
Mezisoučet za specifický cíl č. 1							**43,150**		**48,150**		**45,000**										**136,300**

– Specifický cíl 1 se týká finančních prostředků, které byly zpřístupněny členským státům, aby mohly využít interoperabilních ústředních systémů. Rozhraní NUI je přizpůsobeno, když je zaveden ESP a když je zprovozněn MID. Každý členský stát pak má za úkol provést velmi mírné změny (odhadem 150 člověkodní), aby došlo k přizpůsobení těmto aktualizovaným výměnám zpráv s ústředními systémy. Zásadnější je změna obsahu údajů, kterou přinese interoperabilita a která je zahrnuta do „nákladů na začlenění“. Tyto finanční prostředky se týkají změn druhu zpráv zasílaných do ústředního systému a pro zpracování vrácené odpovědi. Pro odhad nákladů na tyto změny je na členský stát přidělen rozpočet ve výši 4 milionů EUR. Tato částka je stejná jako pro systém EES, jelikož se očekává srovnatelné množství práce pro přizpůsobení integrace vnitrostátních systémů s rozhraním NUI.

– Je třeba, aby koncoví uživatelé byli pro tyto systémy školeni. Tato odborná příprava pro velmi vysoký počet koncových uživatelů bude financována na základě 1 000 EUR na školení 10 až 20 koncových uživatelů s odhadovaným počtem 10 000 školení, která všechny členské státy uspořádají ve vlastních prostorech.

3.2.3. Odhadovaný dopad na lidské zdroje

3.2.3.1. Shrnutí agentury EBCG

☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

☒ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
Úředníci (třídy AD)										
Úředníci (třídy AST)	0									
Smluvní zaměstnanci	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Dočasní zaměstnanci	0	0	0	0	0	0	0	0	0	0
Vyslaní národní odborníci										
CELKEM	**0,0**	**0,0**	**0,0**	**0,350**	**1,400**	**0,233**	**0,0**	**0,0**	**0,0**	**1,983**

Práce, kterou by měli tito další zaměstnanci vykonat pro EBCG, je časově omezená (2023), přesněji začíná 24 měsíců po datu dostupnosti biometrického nástroje pro EES). Pracovníci budou však muset být najati předem (v průměru se počítá se lhůtou tří měsíců), což objasňuje hodnotu pro rok 2022. Po odvedené práci následují závěrečné/souhrnné činnosti v délce dvou měsíců, což vysvětluje počty zaměstnanců v roce 2024.

Samotné počty zaměstnanců vycházejí z počtu 20 osob nutných k vykonání práce (plus 10 osob od dodavatele, tento údaj se odráží v hlavě 3). Tyto činnosti by také měly probíhat v prodloužené pracovní době, neměly by být omezeny běžnou pracovní dobou. Pomocní a vedoucí pracovníci by měli být zajišťováni ze zdrojů agentury.

Počet zaměstnanců vychází z předpokladu, že bude nutno posoudit přibližně 550 000 otisků prstů při průměrné době 5 až 10 minut na případ (ročně ověřeno 17 000 otisků prstů)[96].

[96] Údaje o počtu pracovníků na rok 2020 a následující roky jsou orientační a bude třeba posoudit, zda je jejich počet dodatečný k odhadovanému počtu pracovníků Evropské agentury pro pohraniční a pobřežní stráž, jak je stanoven v dokumentu COM(2015) 671, či nikoli.

Počet zaměstnanců	2019	2020	2021	2022	2023	2024	2025	2026	2027	Celkem
Zaměstnanci pro ruční zpracovávání propojení a rozhodnutí	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Hlava 1 celkem – SZ	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Hlava 1 celkem – DZ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Hlava 1 celkem	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3

.

3.2.3.2. Souhrn za Europol

☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

☒ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
Úředníci (třídy AD)										
Úředníci (třídy AST)	0									
Smluvní zaměstnanci	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Dočasní zaměstnanci	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Vyslaní národní odborníci										
CELKEM	**0,690**	**2,002**	**2,002**	**1,181**	**1,181**	**0,974**	**0,974**	**0,974**	**0,974**	**10,952**

Náklady jsou odhadnuty na základě následujících počtů zaměstnanců:

Počet FTE pro IKT	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**celkem**
Smluvní zaměstnanci	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0
Dočasní zaměstnanci	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Zaměstnanci celkem (FTE)	**5,0**	**15,0**	**15,0**	**12,5**	**12,5**	**11,0**	**11,0**	**11,0**	**11,0**	**104,0**

Další zaměstnanci v oblasti IKT pro Europol by měli posílit informační systémy Europolu, aby se bylo možné vypořádat s vyšším počtem dotazů z ESP a ETIAS a aby později bylo možno systémy provozovat non-stop.

– Pro zaváděcí fázi ESP (v letech 2020 a 2021) se objevuje další potřeba technických odborníků (architektů, techniků, vývojářů, testerů). Nižší počet technických odborníků bude potřebný pro roky 2022 a další při zavádění zbývajících složek interoperability a při údržbě systémů.

– Již od druhé poloviny roku 2021 bude nezbytné zavést non-stop monitorování systému IKT, aby se zajistily provozní úrovně ESP a ETIAS. To by měli vykonávat 2 smluvní pracovníci pracující ve 4 směnách non-stop.

– Profily byly v maximální možné míře rozděleny mezi dočasné pracovníky a smluvní pracovníky. Je však nutno mít na paměti, že s ohledem na vysoké požadavky na zabezpečení je možné na některých pozicích využívat pouze dočasné pracovníky. Požadavek týkající se dočasných pracovníků bude vycházet z výsledků dohodovacího prostupu o rozpočtu na rok 2018.

3.2.3.3. Souhrn za CEPOL

☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

☒ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
Úředníci (třídy AD)										
Úředníci (třídy AST)										
Smluvní zaměstnanci			0,070	0,070						**0,140**
Dočasní zaměstnanci		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Vyslaní národní odborníci										
CELKEM		**0,104**	**0,208**	**0,208**	**0,138**	**0,138**	**0,138**	**0,138**	**0,138**	**1,210**

Bude potřeba najmout další pracovníky, jelikož školení pro školitele z členských států je nutno vyvinout konkrétně s ohledem na používání složek interoperability v provozních podmínkách.

– Vývoj vzdělávacího programu a modulů odborné přípravy by měl začít nejméně 8 měsíců před zprovozněním systému. V prvních dvou letech po zprovoznění je odborná příprava na

nejintenzivnější úrovni. Je však nutno ji takto udržovat delší období, aby se zajistilo jednotné provádění v závislosti na zkušenostech se schengenským informačním systémem.

– Budou potřeba další pracovníci pro přípravu, koordinaci a zavádění vzdělávacího programu, rezidenčních kurzů a on-line kurzů. Tyto kurzy lze zavést pouze jako doplněk stávajícího katalogu školení CEPOL, je tedy nutné najmout další pracovníky.

– Plánuje se, že jeden dočasný zaměstnanec bude pracovat jako manažer kurzů po celou dobu vývoje a udržování a v nejintenzivnějším období organizace odborné přípravy mu bude pomáhat jeden smluvní zaměstnanec.

3.2.3.4. Souhrn za agenturu eu-LISA

☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

☒ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
Úředníci (třídy AD)										
Úředníci (třídy AST)										
Smluvní zaměstnanci	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570
Dočasní zaměstnanci	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Vyslaní národní odborníci										
CELKEM	**2,876**	**4,850**	**6,202**	**6,902**	**6,624**	**5,482**	**5,136**	**5,136**	**5,136**	**48,344**

– Požadavky na zaměstnance vycházejí z toho, že všechny čtyři složky a CRRS představují portfolio projektů se závislostmi (tj. určitý program). Pro správu závislostí mezi projekty vznikne tým řízení programu zahrnující programové a projektové manažery a profily (často označované termínem architekti), které jsou nezbytné pro vymezení společných prvků mezi nimi. Pro realizaci programu/projektu jsou také nezbytné profily pro programovou a projektovou podporu.

– Požadavky na zaměstnance na projekt byly odhadnuty analogicky k předchozím projektům (vízový informační systém) a s odlišením dokončovací fáze projektu a jeho provozní fáze.

– Pracovníci profilů, které by měly zůstat při provozní fázi, jsou najímáni jako dočasní zaměstnanci. Pracovníci profilů nezbytných během provádění programu/projektu se najímají jako smluvní zaměstnanci. Aby se zajistila očekávaná kontinuita úkolů a aby se

udržely znalosti v rámci agentury, poměr pozic se rozdělí téměř 50/50 mezi dočasné a smluvní zaměstnance.

– Předpokládá se, že žádní další zaměstnanci nebudou pro realizaci projektu vysoké dostupnosti systému ECRIS-TCN nutní a že projektoví zaměstnanci agentury eu-LISA budou převzati ze stávajících zaměstnanců z projektů, které budou v daném časovém úseku dobíhat.

Tyto odhady vycházejí z následujících počtů zaměstnanců:

Na smluvní zaměstnance:

3.2.1. výstupy EU-LISA (rovná se H1) v počtu osob	2019	2020	2021	2022	2023	2024	2025	2026	2027	Celkem (vzorec)
Smluvní zaměstnanci										-
Řízení programu/projektu	4,0	5,0	5,5	5,5	4,5	3,0	3,0	3,0	3,0	36,5
CRRS PM	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*1,5*
MID	*0,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*2,0*
Kancelář programu/projektu	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*14,0*
Zajištění kvality	*1,0*	*2,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*19,0*
Finance a zadávání zakázek	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Finanční řízení										*0,0*
Rozpočtové plánování a kontrola										*0,0*
Řízení zakázek/smluv	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Techničtí odborníci	7,0	7,0	7,0	7,0	6,0	5,0	5,0	5,0	5,0	54,0
CRRS	*3,0*	*3,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*22,0*
ESP	*4,0*	*4,0*	*4,0*	*4,0*	*4,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Sdílená BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Testování	1,5	3,0	4,0	4,0	4,0	3,0	2,0	2,0	2,0	25,5
CRRS	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*6,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Sdílená BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,5*	*1,0*	*2,0*	*2,5*	*2,5*	*1,5*	*1,0*	*1,0*	*1,0*	*13,0*
MID	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*6,5*
Sledování systému	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Společné (non-stop)	0,0	*5,0*	*10,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*135,0*
Obecná koordinace	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Lidské zdroje	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Lidské zdroje	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Mezisoučet za smluvní zaměstnance	**12,5**	**20,0**	**26,5**	**36,5**	**34,5**	**31,0**	**30,0**	**30,0**	**30,0**	**251,0**

Na dočasné zaměstnance:

Dočasní zaměstnanci										
Řízení programu/projektu	3,0	4,0	5,5	5,5	5,5	4,5	4,0	4,0	4,0	40,0
Programový manažer	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Řízení projektu	*0,0*	*0,0*	*1,0*	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*12,0*
Kancelář programu/projektu	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
ESP	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
Sdílená BMS	*0,5*	*0,5*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*4,0*
CIR	*0,0*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Finance a zadávání zakázek	3,0	3,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	34,0
Finanční řízení	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*7,0*
Rozpočtové plánování a kontrola	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Řízení zakázek/smluv	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*18,0*
Techničtí odborníci	6,0	14,0	17,0	17,0	15,0	11,0	10,0	10,0	10,0	110,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Sdílená BMS	*2,0*	*3,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
CIR	*2,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Bezpečnost	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*17,0*
MID	*0,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*12,0*
Architekti	*1,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,0*	*1,0*	*1,0*	*17,0*
Testování	2,5	3,0	4,0	4,0	4,0	2,5	2,0	2,0	2,0	26,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,5*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*6,5*
Sdílená BMS	*2,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,5*	*1,5*	*1,5*	*19,5*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Sledování systému	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Sdílená BMS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Odborná příprava	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	8,0
Odborná příprava	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*8,0*
Lidské zdroje	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Lidské zdroje	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Ostatní	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Odborník na ochranu údajů	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	*5,0*
Mezisoučet za dočasné zaměstnance	**14,5**	**25,0**	**31,5**	**31,5**	**30,5**	**24,0**	**22,0**	**22,0**	**22,0**	**223,0**
Celkem	**27,0**	**45,0**	**58,0**	**68,0**	**65,0**	**55,0**	**52,0**	**52,0**	**52,0**	**474,0**

3.2.4. Odhadovaný dopad na prostředky správní povahy

3.2.4.1. GŘ Home: Shrnutí

– ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

– ☒ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
OKRUH 5 víceletého finančního rámce										
Lidské zdroje GŘ HOME	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Ostatní správní výdaje	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
Mezisoučet za OKRUH 5 víceletého finančního rámce	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Mimo OKRUH 5[97] víceletého finančního rámce	(nevyužito)									
Lidské zdroje										
Ostatní výdaje správní povahy										
Mezisoučet mimo OKRUH 5 víceletého finančního rámce										

CELKEM	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

.

[97] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

3.2.4.2. Odhadované potřeby v oblasti lidských zdrojů

– ☐ Návrh/podnět nevyžaduje využití lidských zdrojů.

– ☒ Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

Odhad vyjádřete v přepočtu na plné pracovní úvazky

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
• Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)										
18 01 01 01 (v ústředí a v zastoupeních Komise) GŘ HOME	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
XX 01 01 02 (při delegacích)										
XX 01 05 01 (v nepřímém výzkumu)										
10 01 05 01 (v přímém výzkumu)										
• Externí zaměstnanci (v přepočtu na plné pracovní úvazky: FTE)[98]										
XX 01 02 02 (SZ, MZ, VNO, ZAP a MOD při delegacích)										
XX 01 04 **yy** 99 – v ústředí										
XX 01 04 **yy** 99 – při delegacích										
XX 01 05 02 (SZ, VNO, ZAP v nepřímém výzkumu)										
10 01 05 02 (SZ, ZAP, VNO v přímém výzkumu)										
Jiné rozpočtové položky (upřesněte)										
CELKEM	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**2,0**	**2,0**	**2,0**	**36,0**

18 je oblast politiky nebo dotčená hlava rozpočtu.

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeobsazeny v rámci GŘ, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Popis úkolů:

Monitoring projektů a navazující kroky. Tři úředníci pro navazující kroky. Zaměstnanci převezmou povinnosti Komise při dodávání programu: kontrola souladu s právním návrhem, řešení otázek souladu, příprava zpráv pro Evropský parlament a Radu, posuzování pokroku v členských státech. Jelikož program je dodatečnou činností v porovnání se stávajícím pracovním vytížením, je nezbytné najmout další zaměstnance. Toto navýšení počtu zaměstnanců je časově omezeno a pokrývá pouze období vývoje.

Správa UMF

Komise bude spravovat normu UMF na každodenní bázi. Pro tento účel jsou nezbytní dva úředníci: jedna osoba jako odborník na prosazování práva a druhá osoba s dobrými znalostmi modelování obchodních kroků i se znalostmi IKT.

Univerzální formát pro zprávy (UMF) nastavuje normu strukturované přeshraniční výměny informací mezi informačními systémy, orgány a/nebo organizacemi v oblasti spravedlnosti a vnitřních věcí. UMF definuje společný slovník a logické struktury pro běžně vyměňované informace tak, aby se dosáhlo cíle usnadnit

[98] SZ = smluvní zaměstnanec; MZ = místní zaměstnanec; VNO = vyslaný národní odborník; ZAP = zaměstnanec agentury práce; MOD = mladý odborník při delegaci.

[99] Dílčí strop na externí zaměstnance financované z operačních prostředků (bývalé položky „BA“).

interoperabilitu umožněním vytvoření a pročtení obsahu výměny jednotným a sémanticky odpovídajícím způsobem.

Za účelem zajištění jednotných podmínek k provádění univerzálního formátu pro zprávy se navrhuje svěřit Komisi prováděcí pravomoci. Navrhuje se vykonávat tyto pravomoci v souladu s nařízením 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.

3.2.5. Soulad se stávajícím víceletým finančním rámcem

– ☐ Návrh/podnět je v souladu se stávajícím víceletým finančním rámcem.

– ☒ Návrh/podnět si vyžádá úpravu příslušného okruhu víceletého finančního rámce.

Upřesněte požadovanou úpravu, příslušné rozpočtové položky a odpovídající částky.
Nařízení o ISF – hranice je finanční nástroj, do nějž byl začleněn rozpočet na provedení iniciativy týkající se interoperability.
V čl. 5 písm. b) stanoví, že 791 milionů EUR je nutno realizovat v rámci programu na vývoj systémů informačních technologií založených na stávajících nebo nových systémech na podporu řízení migračních toků přes vnější hranice Unie, s výhradou přijetí příslušných právních předpisů Unie a při dodržení podmínek stanovených v článku 15. Z těchto 791 milionů EUR je vyhrazeno 480,2 milionu EUR na vývoj systému EES, 210 milionů EUR na systém ETIAS a 67,9 milionu EUR na revizi systému SIS II. Zbývající částka (32,9 milionu EUR) má být přerozdělena s využitím mechanismů ISF – hranice. **Tento návrh požaduje 32,1 milionu EUR na stávající období víceletého finančního rámce, které spadá do zbývajícího rozpočtu.**

Závěr v předchozím rámečku uvádějící požadovanou částku 32,1 milionu EUR vyplývá z následujícího výpočtu:

ZÁVAZKY										
3.2. Odhadovaný dopad na výdaje GŘ HOME										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Celkem (horiz)**
18 02 01 03 – inteligentní hranice (zahrnuje podporu pro členské státy)	0	0	43,150	48,150	45,000	0	0	0	0	136,300
Celkem (1)	**0**	**0**	**43,150**	**48,150**	**45,000**	**0**	**0**	**0**	**0**	**136,300**
18.0207 -3.2. eu-LISA										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Celkem (vzorec)**
H1: Výdaje na zaměstnance	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
H2: Výdaje na infrastrukturu a provoz	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
H3: Provozní výdaje	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Celkem (2)	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**
		22,861							**202,181**	**225,041**
18.02.04 -3.2. Europol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Celkem (vzorec)**
H1: Výdaje na zaměstnance	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
H2: Výdaje na infrastrukturu a provoz	0	0	0	0	0	0	0	0	0	0
H3: Provozní výdaje	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Celkem (3)	**0,690**	**8,382**	**8,382**	**3,589**	**3,589**	**3,382**	**8,732**	**8,732**	**3,382**	**48,860**
		9,072							39,788	48,860
18.02.05 -3.2. CEPOL										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Celkem (vzorec)**
H1: Výdaje na zaměstnance	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
H2: Výdaje na infrastrukturu a provoz	0	0	0	0	0	0	0	0	0	0
H3: Provozní výdaje	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Celkem (4)	**0**	**0,144**	**0,384**	**0,482**	**0,208**	**0,208**	**0,208**	**0,208**	**0,208**	**2,050**
		0,144							**1,906**	**2,050**
18.02.0 -3.2. Frontex – EBCG										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Celkem (vzorec)**
H1: Výdaje na zaměstnance	0	0	0	0,350	1,400	0,233	0	0	0	1,983
H2: Výdaje na infrastrukturu a provoz	0	0	0	0,075	0,300	0,050	0	0	0	0,425
H3: Provozní výdaje	0	0	0	0,183	2,200	0	0	0	0	2,383
Celkem (5)	**0**	**0**	**0**	**0,608**	**3,900**	**0,283**	**0**	**0**	**0**	**4,792**
		0							**4,792**	**4,792**
CELKEM (1)+(2)+(3)+(4)+(5)	6,520	25,556	103,659	97,578	82,350	24,243	27,549	27,469	22,119	417,043
		32,076							384,966	
3.2. GŘ HOME Okruh 5 „Správní výdaje“										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Celkem**
Celkem (6)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
CELKEM (1)+(2)+(3)+(4)+(5)+(6)	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	424,738

– ☐ Návrh/podnět vyžaduje použití nástroje pružnosti nebo změnu víceletého finančního rámce.

3.2.6. Příspěvky třetích stran

– Návrh/podnět **nepočítá** se spolufinancováním od třetích stran.

3.3. Odhadovaný dopad na příjmy

– ☐ Návrh/podnět nemá žádný finanční dopad na příjmy.

– ☒ Návrh/podnět má tento finanční dopad:

– ☐ dopad na vlastní zdroje

– ☒ dopad na různé příjmy

v milionech EUR (zaokrouhleno na tři desetinná místa)

Příjmová rozpočtová položka:	Prostředky dostupné v běžném rozpočtovém roce	Dopad návrhu/podnětu[100]								
		Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**
Článek 6313 – Příspěvek od zemí přidružených k Schengenu (CH, NO, LI, IS)…… …….		pm	pm	pm	pm	pm	pm	pm	pm	pm

U účelově vázaných různých příjmů upřesněte dotčené výdajové rozpočtové položky.

18.0207

Upřesněte způsob výpočtu dopadu na příjmy.

Rozpočet zahrnuje příspěvek zemí přidružených k provádění, uplatňování a rozvoji schengenského *acquis* a opatření souvisejících s Eurodacem, jak stanoví příslušné dohody.

[100] Pokud jde o tradiční vlastní zdroje (cla, dávky z cukru), je třeba uvést čisté částky, tj. hrubé částky po odečtení 25 % nákladů na výběr.