EVROPSKÁ
KOMISE

V Bruselu dne 21.12.2016
COM(2016) 882 final

2016/0408 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol, o změně nařízení (EU) č. 515/2014 a o zrušení nařízení (ES) č. 1987/2006

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

V průběhu minulých dvou let pracovala Evropská unie souběžně na řešení zvláštních výzev, jaké představuje řízení migrace, integrovaná správa vnějších hranic EU a boj proti terorismu a přeshraniční trestné činnosti. Účinná výměna informací mezi členskými státy navzájem a mezi členskými státy a příslušnými agenturami EU má zásadní význam pro zajištění rázné reakce na tyto výzvy a pro vytvoření účinné a skutečné bezpečnostní unie.

Schengenský informační systém (dále jen „SIS“) je nejúspěšnějším nástrojem pro účinnou spolupráci imigračních, policejních, celních a justičních orgánů v EU a zemích přidružených k Schengenu. Příslušné orgány v členských státech, jako je policie, pohraniční stráž a celní správa, musí mít přístup k vysoce kvalitním informacím o osobách či věcech, které kontrolují, s jasnými pokyny, jak v jednotlivých případech postupovat. Tento rozsáhlý informační systém tvoří samotné jádro schengenské spolupráce a hraje klíčovou roli při usnadňování volného pohybu osob v schengenském prostoru. Příslušným orgánům umožňuje vkládat a prohlížet údaje o hledaných osobách, osobách, které případně nemají právo na vstup nebo pobyt na území EU, hledaných osobách – zejména dětech – a věcech, které mohly být odcizeny, neoprávněně užívány nebo ztraceny. SIS obsahuje nejen informace o konkrétní osobě nebo věci, nýbrž také jednoznačné pokyny pro příslušné orgány, jak postupovat v případě jejich nalezení.

V roce 2016, tedy tři roky po uvedení druhé generace tohoto systému do provozu, provedla Komise komplexní hodnocení SIS[1]. Toto hodnocení prokázalo skutečnou operativní úspěšnost SIS. V roce 2015 zkontrolovaly příslušné vnitrostátní orgány podle údajů v SIS osoby a věci téměř v 2,9 miliardy případech a vyměnily si přes 1,8 milionu doplňujících informací. Jak však oznámila Komise ve svém pracovním programu na rok 2017, je třeba s využitím této pozitivní zkušenosti efektivnost a účinnost tohoto systému ještě posílit. Proto Komise na základě uvedeného hodnocení předkládá první soubor tří návrhů, které mají zlepšit a rozšířit používání SIS. Zároveň v návaznosti na probíhající práci expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu nadále pracuje na zvýšení interoperability stávajících i budoucích systémů pro prosazování práva a správu hranic.

Předmětné návrhy upravují používání systému pro následující účely: a) správa hranic, b) policejní spolupráce a justiční spolupráce v trestních věcech a c) navracení neoprávněně pobývajících státních příslušníků třetích zemí. První dva návrhy tvoří společný právní základ pro zřízení, provoz a využívání SIS. Návrh týkající se využívání SIS pro účely navracení neoprávněně pobývajících státních příslušníků třetích zemí dovršuje návrh týkající se správy hranic a doplňuje ustanovení v něm obsažená. Tento návrh pro účely navracení zavádí nové kategorie záznamů a přispívá k provádění a sledování směrnice 2008/115/ES[2].

---

[1] Zpráva Komise Evropskému parlamentu a Radě o hodnocení Schengenského informačního systému druhé generace (SIS II) v souladu s čl. 24 odst. 5, čl. 43 odst. 3 a čl. 50 odst. 5 nařízení (ES) č. 1987/2006 a čl. 59 odst. 3 a čl. 66 odst. 5 rozhodnutí 2007/533/SVV a průvodní pracovní dokument útvarů Komise (Úř. věst. ...).

[2] Směrnice Evropského parlamentu a Rady 2008/115/ES ze dne 16. prosince 2008 o společných normách a postupech v členských státech při navracení neoprávněně pobývajících státních příslušníků třetích zemí (Úř. věst. L 348, 24.12.2008, s. 98).

Z důvodu diferencované účasti členských států (metoda „proměnné geometrie“) na politikách EU týkajících se prostoru svobody, bezpečnosti a práva je nezbytné přijmout tři samostatné právní nástroje, které však budou fungovat bezproblémově vedle sebe s cílem umožnit komplexní provoz a využívání systému.

Souběžně s tím zahájila Komise v dubnu 2016 za účelem posílení a zlepšení správy informací na úrovni EU proces reflexe na téma „silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost“[3], jehož všeobecným cílem je zajistit, aby příslušné orgány systematicky disponovaly potřebnými informacemi z různých informačních systémů. Za účelem dosažení tohoto cíle provádí Komise přezkum stávající informační architektury, který umožní identifikovat mezery v informacích a slabé stránky, jež jsou důsledkem nedostatků ve fungování stávajících systémů a roztříštěnosti celkové architektury EU pro správu údajů. Na podporu této činnosti zřídila Komise expertní skupinu na vysoké úrovni pro informační systémy a interoperabilitu, jejíž prozatímní zjištění v otázce kvality údajů byla v tomto souboru návrhů rovněž zohledněna[4]. Předseda Komise Juncker ve svém projevu o stavu Unie v září 2016 rovněž zmínil důležitost vyřešení současných nedostatků v oblasti správy informací a zlepšení interoperability a propojení mezi stávajícími informačními systémy.

Na základě zjištění expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu, jež budou představena v první polovině roku 2017, Komise v polovině roku 2017 zváží předložení druhého souboru návrhů s cílem dále zlepšit interoperabilitu SIS s ostatními počítačovými systémy. Stejně důležitým prvkem této práce je přezkum nařízení (EU) č. 1077/2011[5] o Evropské agentuře pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (eu-LISA), kterým se budou zabývat samostatné návrhy Komise, a to pravděpodobně také v roce 2017. Investice do rychlé, účinné a kvalitní výměny informací, řízení informací a do zajištění interoperability databází a informačních systémů EU je důležitý aspekt řešení nynějších výzev v oblasti bezpečnosti.

Stávající právní rámec SIS druhé generace, pokud jde o jeho využívání pro účely hraničních kontrol státních příslušníků třetích zemí, je založen na nástroji bývalého prvního pilíře, konkrétně na nařízení (ES) č. 1987/2006[6]. Předmětný návrh nahrazuje[7] stávající právní nástroj za účelem:

- uložení povinnosti členským státům vložit záznam do SIS ve všech případech, kdy byl vydán zákaz vstupu neoprávněně pobývajícímu státnímu příslušníkovi třetí země v souladu s ustanoveními v souladu se směrnicí 2008/115/ES,
- harmonizace vnitrostátních postupů pro využívání SIS, pokud jde o postup konzultace, aby se zamezilo případům, kdy státní příslušník třetí země, jemuž byl vydán zákaz vstupu, je zároveň držitelem platného povolení k pobytu vydaného členským státem,

---

3 COM(2016) 205 final ze dne 6. dubna 2016.

4 Rozhodnutí Komise 2016/C 257/03 ze dne 17. června 2016.

5 Nařízení Evropského parlamentu a Rady (EU) č. 1077/2011 ze dne 25. října 2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (Úř. věst. L 286, 1.11.2011, s. 1).

6 Nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 ze dne 20. prosince 2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II) (Úř. věst. L 381, 28.12.2006, s. 4).

7 Viz oddíl 2 „Volba nástroje“, v němž se vysvětluje, proč bylo zvoleno nahrazení stávajícího právního předpisu namísto jeho přepracování.

- zavedení technických změn, které zlepší bezpečnost a pomohou snížit administrativní zátěž,
- vyřešení komplexního využívání všech prvků SIS (*end-to-end*), které by pokrývalo nejen centrální a vnitrostátní systémy, ale také potřeby koncového uživatele zajištěním, že koncoví uživatelé obdrží veškeré údaje potřebné k plnění úkolů a budou při zpracování údajů SIS dodržovat všechna bezpečnostní pravidla.

Návrhy rozvíjejí a zlepšují stávající systém namísto vytvoření nového. Revize SIS, která podpoří a posílí opatření Evropské unie v rámci evropských programů pro migraci a bezpečnost, obsahuje:

(1) konsolidaci výsledků činností provedených za účelem zavedení SIS za poslední tři roky, které zahrnují technické změny centrálního SIS za účelem rozšíření některých stávajících kategorií záznamů a vytvoření nových funkcí;

(2) provedení doporučení o technických a procesních změnách, která vyplynula z komplexního hodnocení SIS[8];

(3) zohlednění žádostí koncových uživatelů SIS o provedení technických zlepšení a

(4) zohlednění prozatímních zjištění expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu[9], pokud jde o kvalitu údajů.

Vzhledem k tomu, že je tento návrh neoddělitelně spjat s navrhovaným nařízením Komise o zřízení, provozu a využívání SIS v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, je řada ustanovení v obou textech shodná. Jedná se o opatření týkající se komplexního využívání všech prvků SIS, včetně provozu centrálního a vnitrostátních systémů, ale i potřeb koncového uživatele, posílená opatření pro zachování kontinuity provozu, opatření týkající se kvality údajů, ochrany údajů a zabezpečení údajů, jakož i ustanovení o monitorování, hodnocení a podávání zpráv. Oba návrhy rovněž rozšiřují využívání biometrických informací[10].

S vystupňováním migrační a uprchlické krize v roce 2015 značně vzrostla nutnost přijmout účinné kroky k řešení nelegální migrace. V *akčním plánu EU v oblasti navracení*[11] Komise oznámila, že navrhne uložit členským státům povinnost vkládat do SIS všechny zákazy vstupu s cílem pomoci zabránit tomu, aby státní příslušníci třetích zemí, jimž není dovoleno vstoupit na území členských států a pobývat na něm, znovu vstupovali do schengenského prostoru. Zákazy vstupu vydané v souladu s ustanoveními v souladu se směrnicí 2008/115/ES mají účinek v celém schengenském prostoru, a proto mohou být na vnějších hranicích vymáhány i orgány jiného členského státu, než je stát, který zákaz vydal. Stávající nařízení (ES) č. 1987/2006 vkládání záznamů do SIS pro účely odepření vstupu a pobytu na základě zákazů vstupu členským státům pouze umožňuje, avšak tento krok v něm není vyžadován. Bude-li uložena povinnost vkládat do SIS všechny zákazy vstupu, může být dosaženo větší míry účinnosti a harmonizace.

---

8 Zpráva Komise Evropskému parlamentu a Radě o hodnocení Schengenského informačního systému druhé generace (SIS II) v souladu s čl. 24 odst. 5, čl. 43 odst. 3 a čl. 50 odst. 5 nařízení (ES) č. 1987/2006 a čl. 59 odst. 3 a čl. 66 odst. 5 rozhodnutí 2007/533/SVV a průvodní pracovní dokument útvarů Komise (Úř. věst.…).

9 Expertní skupina na vysoké úrovni – zpráva předsedy ze dne 21. prosince 2016.

10 Změny obsažené v tomto návrhu jsou podrobně vysvětleny v oddíle 5 „Ostatní prvky“.

11 COM(2015) 453 final.

- **Soulad s platnými předpisy v této oblasti politiky a se stávajícími a budoucími právními nástroji**

Tento návrh je plně v souladu s ustanoveními směrnice 2008/115/ES o vydávání a vymáhání zákazů vstupu. Doplňuje tudíž stávající ustanovení o zákazech vstupu a přispívá k účinnému vymáhání těchto zákazů na vnějších hranicích, čímž usnadňuje uplatňování povinností stanovených ve směrnici o navracení a úspěšně brání opětovnému vstupu dotčených státních příslušníků třetích zemí do schengenského prostoru.

- **Soulad s ostatními politikami Unie**

Tento návrh je úzce provázán s dalšími politikami Unie a doplňuje je. Konkrétně to jsou:

(1) **vnitřní bezpečnost** ve vztahu k úloze SIS bránit vstupu státních příslušníků třetích zemí, kteří představují bezpečnostní hrozbu;

(2) **ochrana údajů** v rozsahu, v jakém tento návrh zajišťuje ochranu základních práv fyzických osob, jejichž osobní údaje jsou zpracovávány v SIS.

(3) Tento návrh je také úzce provázán se stávajícími právními předpisy Unie a doplňuje je. Konkrétně to jsou:

(4) **správa vnějších hranic** v rozsahu, v jakém tento návrh napomáhá členským státům chránit jejich úsek vnějších hranic EU a zvyšovat účinnost systému EU pro ochranu vnějších hranic;

(5) účinná **návratová politika EU**, která je součástí systému EU pro odhalování a předcházení opětovného vstupu státních příslušníků třetích zemí po jejich navrácení a tento systém posiluje. Tento návrh by pomohl snížit motivaci k nelegální migraci do EU, což je jeden z hlavních cílů Evropského programu pro migraci[12];

(6) **Evropská pohraniční a pobřežní stráž,** pokud jde i) o možnost, aby pracovníci agentury prováděli analýzy rizik, ii) o přístup ústřední jednotky ETIAS zřízené v rámci agentury pro účely navrhovaného evropského systému pro cestovní informace a povolení (ETIAS)[13] a iii) o vytvoření technického rozhraní pro přístup do SIS pro jednotky Evropské pohraniční a pobřežní stráže, týmy pracovníků, kteří se podílejí na úkolech spojených s navracením, a členy podpůrných týmů pro řízení migrace s cílem udělit jim v rámci jejich mandátu právo na přístup k údajům vloženým do SIS a právo v těchto údajích vyhledávat;

(7) **Europol** – v rámci mandátu této agentury se navrhuje rozšíření práva na přístup k údajům SIS a práva v těchto údajích vyhledávat.

Tento návrh je také úzce provázán s budoucími právními předpisy Unie, které doplňuje. Konkrétně to jsou:

(8) **systém vstupu/výstupu** (EES) – pro účely jeho provozu se navrhuje kombinace otisku prstu a zobrazení obličeje jako biometrických identifikátorů, což je přístup, který tento návrh zohledňuje;

(9) systém **ETIAS** – navrhuje se důkladné posuzování státních příslušníků třetích zemí osvobozených od vízové povinnosti, kteří mají v úmyslu cestovat do EU, z bezpečnostního hlediska, včetně jejich ověření v SIS.

---

12 COM(2015) 240 final.

13 COM(2016) 731 final.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právní základ

Návrh používá jako právní základ pro ustanovení v oblasti integrované správy hranic a nedovoleného přistěhovalectví čl. 77 odst. 2 písm. b) a d) a čl. 79 odst. 2 písm. c) Smlouvy o fungování Evropské unie.

• Proměnná geometrie

Tento návrh navazuje na ustanovení schengenského *acquis* týkajícího se hraničních kontrol. Ve vztahu k jednotlivým protokolům a dohodám s přidruženými zeměmi je proto nutno uvážit níže uvedené důsledky:

Dánsko: Podle článku 4 Protokolu č. 22 o postavení Dánska, připojeného ke Smlouvám, se Dánsko rozhodne do šesti měsíců poté, co Rada přijala toto nařízení, zda provede tento návrh, který navazuje na schengenské *acquis*, ve svém vnitrostátním právu.

Spojené království a Irsko: V souladu s články 4 a 5 Protokolu o schengenském *acquis* začleněném do rámce Evropské unie, s rozhodnutím Rady 2000/365/ES ze dne 29. května 2000 o žádosti Spojeného království Velké Británie a Severního Irska a rozhodnutím Rady 2002/192/ES ze dne 28. února 2002 o žádosti Irska, aby se na ně vztahovala některá ustanovení schengenského *acquis*, se Spojené království a Irsko nepodílejí na nařízení (EU) 2016/399 (Schengenský hraniční kodex) ani žádném jiném z právních nástrojů, které jsou obecně známy jako „schengenské *acquis*“, totiž právních nástrojů pro organizaci a podporu zrušení kontrol na vnitřních hranicích a doprovodných opatření týkajících se kontrol na vnějších hranicích. Toto nařízení rozvíjí ustanovení tohoto *acquis*; Spojené království a Irsko se tedy nepodílejí na přijímání tohoto nařízení a toto nařízení pro ně není závazné ani použitelné.

Bulharsko a Rumunsko: Toto nařízení představuje akt navazující na schengenské *acquis* nebo s ním jinak související ve smyslu čl. 4 odst. 2 aktu o přistoupení z roku 2005. Toto nařízení je třeba vykládat ve spojení s rozhodnutím Rady 2010/365/EU ze dne 29. června 2010[14], jež stanoví, která ustanovení schengenského *acquis* týkající se Schengenského informačního systému mají být s výhradou určitých omezení použita v Bulharsku a Rumunsku.

Kypr a Chorvatsko: Toto nařízení představuje akt navazující na schengenské *acquis* nebo s ním jinak související ve smyslu čl. 3 odst. 2 aktu o přistoupení z roku 2003 a čl. 4 odst. 2 aktu o přistoupení z roku 2011.

Přidružené země: Na základě příslušných dohod o přidružení těchto zemí k provádění, uplatňování a rozvoji schengenského *acquis* má být navrhované nařízení závazné pro Island, Norsko, Švýcarsko a Lichtenštejnsko.

• Subsidiarita

Tento návrh využije jako základ, který dále rozvíjí, stávající SIS, jenž funguje od roku 1995. Původní mezivládní rámec byl nahrazen dne 9. dubna 2013 nástroji Unie (nařízením (ES) č. 1987/2006 a rozhodnutím Rady 2007/533/SVV). Při předchozích příležitostech byla

[14] Rozhodnutí Rady ze dne 29. června 2010 o uplatňování ustanovení schengenského *acquis* týkajících se Schengenského informačního systému v Bulharské republice a Rumunsku (Úř. věst. L 166, 1.7.2010, s. 17).

provedena úplná analýza subsidiarity; cílem této iniciativy je zpřesnit stávající ustanovení, odstranit zjištěné nedostatky a zlepšit provozní postupy.

Takovéto značné úrovně výměny informací mezi členskými státy nelze dosáhnout prostřednictvím decentralizovaných řešení. Z důvodu rozsahu, účinků a dopadu činnosti může být cílů tohoto návrhu lépe dosaženo na úrovni Unie.

Cílem tohoto návrhu jsou mimo jiné technická zlepšení za účelem zefektivnění SIS a harmonizace jeho využívání ve všech zúčastněných členských státech. Vzhledem k nadnárodní povaze těchto cílů a výzev při zajišťování účinné výměny informací, která zabrání stále různorodějším hrozbám, má EU dobrou pozici k tomu, aby navrhovala řešení těchto problémů, kterých nemohou dosáhnout členské státy samotné.

Pokud stávající omezení v SIS nebudou odstraněna, hrozí, že bude promarněno mnoho příležitostí k maximalizaci účinnosti a přidané hodnoty EU a že se objeví slepá místa bránící příslušným orgánům v práci. Jako příklad lze uvést neexistenci harmonizovaných pravidel pro výmaz nepotřebných záznamů v systému, která může mít za následek narušení volného pohybu osob jakožto základní zásady Unie.

- **Proporcionalita**

Podle článku 5 Smlouvy o Evropské unii nepřekročí činnost Unie rámec toho, co je nezbytné pro dosažení cílů Smlouvy. Pro toto opatření EU se musí zvolit forma, která umožní, aby návrh dosáhl daného cíle a mohl být proveden co nejúčinněji. Navrhovaná iniciativa představuje revizi SIS ve vztahu k hraničním kontrolám.

Tento návrh vychází ze zásad „ochrany soukromí již od návrhu“. Pokud jde o právo na ochranu osobních údajů, je návrh přiměřený, neboť zavádí zvláštní pravidla pro výmaz záznamů a nevyžaduje se v něm, aby údaje byly shromažďovány a uchovávány po dobu delší, než je naprosto nezbytné k tomu, aby systém mohl fungovat a plnit své cíle. Záznamy v SIS obsahují pouze údaje, které jsou potřebné pro identifikaci a nalezení osoby nebo věci a pro přijetí vhodného operativního opatření. Všechny další informace jsou poskytovány prostřednictvím centrál SIRENE, které umožňují výměnu doplňujících informací.

Návrh dále stanoví provádění všech potřebných záruk a mechanismů nezbytných pro účinnou ochranu základních práv subjektů údajů, zejména ochranu jejich soukromého života a osobních údajů. Obsahuje rovněž ustanovení, jejichž specifickým účelem je posílení bezpečnosti osobních údajů jednotlivců, které jsou uchovávány v SIS.

Pro zprovoznění systému nebudou nutné žádné další postupy nebo harmonizace na úrovni EU. Předpokládané opatření je tudíž přiměřené, neboť nepřekračuje rámec toho, co je nezbytné pro dosažení stanovených cílů v rámci opatření na úrovni EU.

- **Volba nástroje**

Navrhovaná revize bude mít také formu nařízení a nahradí nařízení (ES) č. 1987/2006. Tento přístup byl zvolen rovněž v případě rozhodnutí Rady 2007/533/SVV, a jelikož jsou oba nástroje neoddělitelně spjaty, musí být uplatněn i na nařízení (ES) č. 1987/2006. Rozhodnutí 2007/533/SVV bylo přijato jako tzv. „nástroj třetího pilíře“ podle bývalé Smlouvy o Evropské unii. Nástroje „třetího pilíře“ přijímala Rada bez účasti Evropského parlamentu jakožto spolutvůrce právních předpisů. Právním základem tohoto návrhu je Smlouva o fungování Evropské unie (SFEU), protože struktura pilířů zanikla se vstupem Lisabonské smlouvy v platnost dne 1. prosince 2009. Právní základ vyžaduje použití řádného legislativního

postupu. Musela být zvolena forma nařízení (Evropského parlamentu a Rady), protože ustanovení mají být závazná a přímo použitelná ve všech členských státech.

Návrh bude založen na stávajícím centralizovaném systému, jehož prostřednictvím členské státy vzájemně spolupracují, a takováto spolupráce vyžaduje společnou architekturu a závazná provozní pravidla. Dále stanoví závazná pravidla pro přístup do systému, včetně přístupu pro účely vymáhání práva, jež jsou shodná pro všechny členské státy i pro Evropskou agenturu pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva[15] (eu-LISA). Od 9. května 2013 je agentura eu-LISA odpovědná za provozní řízení centrálního SIS, jež zahrnuje veškeré úkoly nezbytné pro zajištění plného provozu centrálního SIS 24 hodiny denně sedm dní v týdnu. Tento návrh staví na povinnostech agentury eu-LISA v souvislosti se SIS.

Návrh dále stanoví přímo použitelná pravidla umožňující přístup subjektů údajů k údajům, které se jich týkají, a k opravným prostředkům, aniž by byla v tomto ohledu třeba další prováděcí opatření.

Proto lze jako právní nástroj zvolit pouze nařízení.

3. VÝSLEDKY HODNOCENÍ *EX POST*, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

- **Hodnocení *ex post* / kontroly účelnosti platných právních předpisů**

V souladu s nařízením (ES) č. 1987/2006 a rozhodnutím Rady 2007/533/SVV[16] provedla Komise po třech letech od jeho uvedení do provozu celkové hodnocení centrálního systému SIS II a dvoustranné i mnohostranné výměny doplňujících informací mezi členskými státy.

Hodnocení se konkrétně zaměřilo na přezkum uplatňování článku 24 nařízení (ES) č. 1987/2006 se záměrem učinit nezbytné návrhy na změnu ustanovení tohoto článku, aby byla ve větší míře harmonizována kritéria pro vkládání záznamů.

Výsledky hodnocení zdůraznily nutnost změnit právní základ SIS, aby mohl lépe reagovat na nové bezpečnostní a migrační výzvy. Změny zahrnují například návrh na povinné vkládání zákazů vstupu do SIS za účelem jejich lepšího vykonávání, povinné konzultace mezi členskými státy, aby se zamezilo souběžné existenci zákazu vstupu a povolení k pobytu, možnost identifikovat osobu a určit, kde se nachází, na základě jejích otisků prstů s využitím nového automatizovaného systému identifikace otisků prstů, jakož i rozšíření biometrických identifikátorů v systému.

Z výsledků hodnocení rovněž vyplynula potřeba provést změnu právních předpisů, aby se zlepšilo technické fungování systému a racionalizovaly vnitrostátní postupy. Tato opatření zvýší efektivnost a účinnost SIS, neboť zjednoduší jeho používání a omezí zbytečnou zátěž. Další opatření, která jasněji vymezují konkrétní úkoly vypracovávání zpráv uložené členským státům a agentuře eu-LISA, jsou určena ke zvýšení kvality údajů a transparentnosti systému.

---

[15] Agentura byla zřízena nařízením Evropského parlamentu a Rady (EU) č. 1077/2011 ze dne 25. října 2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (Úř. věst. L 286, 1.11.2011, s. 1).

[16] Rozhodnutí Rady 2007/533/SVV ze dne 12. června 2007 o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II) (Úř. věst. L 205, 7.8.2007, s. 63).

Výsledky celkového hodnocení (hodnotící zpráva a související pracovní dokument útvarů Komise, jež byly přijaty 21. prosince 2016[17]) tvoří základ opatření obsažených v tomto návrhu.

Dále v souladu s článkem 19 směrnice o navracení 2008/115/ES zveřejnila Komise v roce 2014 sdělení o návratové politice EU[18], v němž podává zprávu o uplatňování uvedené směrnice. V něm dospěla k závěru, že je třeba dále optimalizovat potenciál systému SIS v oblasti návratové politiky, a uvedla, že přezkum systému SIS II poskytne příležitost zlepšit soudržnost mezi návratovou politikou a systémem SIS II. Dále navrhla, aby byla u zákazů vstupu vydaných podle směrnice o navracení osob uložena členským státům povinnost vložit záznam o odepření vstupu do SIS II.

- **Konzultace se zúčastněnými stranami**

V průběhu svého hodnocení SIS požádala Komise o zpětnou vazbu a návrhy příslušné zúčastněné strany, a to včetně delegátů výboru pro SISVIS postupem stanoveným v článku 51 nařízení (ES) č. 1987/2006. Tento výbor tvoří zástupci členských států pro provozní záležitosti SIRENE (přeshraniční spolupráce v souvislosti se SIS) a pro technické otázky týkající se vývoje a údržby SIS a související aplikace SIRENE.

V rámci procesu hodnocení delegáti výboru vyplnili podrobný dotazník. Pokud bylo třeba odpověď dále objasnit či rozvinout, uskutečnila se výměna e-mailů nebo cílený pohovor.

Tento iterativní proces umožnil nastolení otázek komplexním a transparentním způsobem. V průběhu let 2015 a 2016 delegáti výboru pro SISVIS projednávali tyto otázky na tematických setkáních a seminářích.

Komise rovněž vedla zvláštní konzultace na téma ochrany údajů s národními orgány členských států pro ochranu údajů a s členy koordinační skupiny pro dohled nad SIS II. Členské státy si vyměnily zkušenosti ohledně žádostí subjektů o přístup a činnosti národních orgánů pro ochranu údajů prostřednictvím odpovědi na zvláštní dotazník. Odpovědi na tento dotazník z června 2015 byly zohledněny při vypracovávání tohoto návrhu.

Interně Komise ustavila meziútvarovou řídící skupinu, v níž byl zastoupen Generální sekretariát a Generální ředitelství pro migraci a vnitřní věci, Generální ředitelství pro spravedlnost a spotřebitele, Generální ředitelství pro lidské zdroje a bezpečnost a Generální ředitelství pro informatiku. Tato řídící skupina sledovala proces hodnocení a dle potřeby poskytovala poradenství.

Zjištění v rámci hodnocení zohlednila i podklady shromážděné při kontrolách přímo v členských státech, jejichž cílem bylo podrobně posoudit používání SIS v praxi. Předmětem kontrol byla diskuse a pohovory s odborníky, zaměstnanci centrály SIRENE a příslušnými vnitrostátními orgány.

Orgány členských států odpovědné za navracení mohly vznést své připomínky a návrhy, zejména pokud jde o případné důsledky povinnosti vkládat do SIS záznamy o všech zákazech vstupu vydaných podle směrnice 2008/115/ES, na zasedáních kontaktní skupiny pro směrnici

[17] Zpráva Komise Evropskému parlamentu a Radě o hodnocení Schengenského informačního systému druhé generace (SIS II) v souladu s čl. 24 odst. 5, čl. 43 odst. 3 a čl. 50 odst. 5 nařízení (ES) č. 1987/2006 a čl. 59 odst. 3 a čl. 66 odst. 5 rozhodnutí 2007/533/SVV a průvodní pracovní dokument útvarů Komise.

[18] COM(2014) 199 final.

o navracení osob, zřízené v rámci Komise, která se uskutečnila ve dnech 16. listopadu 2015 a 18. března a 20. června 2016.

Na základě uvedených připomínek stanoví tento návrh opatření ke zlepšení technické a provozní efektivnosti a účinnosti systému.

- **Sběr a využití výsledků odborných konzultací**

Vedle konzultací se zúčastněnými stranami si Komise rovněž vyžádala externí odborné poradenství ve formě čtyř studií, jejichž výsledky byly při vypracovávání tohoto návrhu zohledněny:

- Technický posudek SIS (Kurt Salmon)[19]

V tomto posudku byly vymezeny klíčové otázky pro fungování SIS a budoucí potřeby vyžadující řešení, především problémy v souvislosti s maximalizací kontinuity provozu a zajištěním toho, aby se celková architektura dokázala přizpůsobit rostoucím kapacitním požadavkům.

- Posouzení dopadů možných zlepšení architektury SIS II z hlediska IKT (Kurt Salmon)[20]

Tato studie posoudila běžné náklady na provoz SIS v členských státech a vyhodnotila dva možné technické scénáře zlepšení systému. Oba scénáře obsahují soubor technických návrhů zaměřený na zlepšení centrálního systému a celkové architektury.

- „Posouzení dopadů technických zlepšení architektury SIS II z hlediska IKT – závěrečná zpráva“, 10. listopadu 2016 (Wavestone)[21]

Tato studie posoudila dopady zavedení vnitrostátní kopie na náklady členských států, a to na základě analýzy tří scénářů (plně centralizovaný systém, standardizovaná implementace N.SIS, kterou vyvine a členským státům poskytne agentura eu-LISA, a oddělená implementace N.SIS se společnými technickými normami).

- Studie proveditelnosti a dopadů vytvoření celounijního systému pro výměnu údajů o rozhodnutích o navrácení a sledování jejich dodržování, začleněného do Schengenského informačního systému (PwC)[22]

Tato studie posuzuje proveditelnost navrhovaných změn SIS a jejich technické a provozní dopady s cílem optimalizovat využívání SIS pro účely navracení nelegálních migrantů a zamezení jejich opětovnému vstupu.

---

19 *European Commission FINAL REPORT — SIS II technical assessment* (ZÁVĚREČNÁ ZPRÁVA Evropské komise – Technický posudek SIS II).

20 *European Commission FINAL REPORT — ICT Impact Assessment of Possible Improvements to the SIS II Architecture 2016* (ZÁVĚREČNÁ ZPRÁVA Evropské komise – Posouzení dopadů možných zlepšení architektury SIS II z hlediska IKT 2016).

21 *European Commission FINAL REPORT – „ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report“* (ZÁVĚREČNÁ ZPRÁVA Evropské komise – „Posouzení dopadů technických zlepšení architektury SIS II z hlediska IKT – závěrečná zpráva“), 10. listopadu 2016 (Wavestone).

22 *Study on the feasibility and implications of setting up within the framework of the SIS and EU-wide system for exchanging data on and monitoring compliance with return decisions* (Studie proveditelnosti a dopadů vytvoření celounijního systému pro výměnu údajů o rozhodnutích o navrácení a sledování jejich dodržování, začleněného do Schengenského informačního systému), 4. dubna 2015 (PwC).

- **Posouzení dopadů**

Komise neprovedla posouzení dopadů.

Tři nezávislá posouzení uvedená výše tvořila základ pro vyhodnocení dopadů změn systému z technického hlediska. Od roku 2013, kdy SIS II zahájil dne 9. dubna provoz a stalo se použitelným rozhodnutí 2007/533/SVV, Komise navíc dokončila dva přezkumy příručky SIRENE. Jejich součástí byl přezkum v polovině období, jenž vyústil ve vydání nové příručky SIRENE[23] dne 29. ledna 2015. Komise rovněž přijala katalog osvědčených postupů a doporučení[24]. Agentura eu-LISA a členské státy navíc pravidelně zavádějí technická zlepšení systému. Má se za to, že uvedené možnosti byly nyní vyčerpány a je nutná podstatnější změna právního základu. Jasnosti v oblastech, jako je používání systémů koncových uživatelů a podrobná pravidla pro výmaz záznamu, nelze dosáhnout jen prostřednictvím lepšího provádění a prosazování.

Dále Komise vypracovala celkové hodnocení SIS, jak požaduje čl. 24 odst. 5, čl. 43 odst. 3 a čl. 50 odst. 5 nařízení (ES) č. 1987/2006 a čl. 59 odst. 3 a čl. 66 odst. 5 rozhodnutí 2007/533/SVV, a zveřejnila průvodní pracovní dokument útvarů Komise. Výsledky celkového hodnocení (hodnotící zpráva a související pracovní dokument útvarů Komise přijaté 21. prosince 2016) tvoří základ opatření obsažených v tomto návrhu.

Schengenský hodnotící mechanismus, stanovený v nařízení (EU) č. 1053/2013[25], umožňuje pravidelně posuzovat fungování SIS v členských státech z právního a provozního hlediska. Hodnocení provádějí společně Komise a členské státy. Prostřednictvím tohoto mechanismu vydává Rada na základě hodnocení provedených v rámci víceletých a ročních programů doporučení jednotlivým členským státům. Vzhledem ke své individualizované povaze nemohou tato doporučení nahradit právně závazná pravidla, která jsou současně platná pro všechny členské státy využívající SIS.

Výbor pro SISVIS pravidelně projednává praktické provozní a technické otázky. Ačkoliv tato zasedání mají zásadní význam pro spolupráci mezi Komisí a členskými státy, výsledek těchto jednání (bez změny právních předpisů) nemůže například odstranit problémy vznikající v důsledku odlišných vnitrostátních postupů.

Změny navržené v tomto nařízení nemají žádný významný hospodářský ani environmentální dopad. Měly by však mít výrazně pozitivní sociální dopad tím, že zvyšují bezpečnost: umožňují lepší identifikaci osob používajících falešnou totožnost, pachatelů trestné činnosti, jejichž totožnost je po spáchání závažného trestného činu neznámá, i nelegálních migrantů neoprávněně se pohybujících v prostoru bez kontrol na vnitřních hranicích. Dopad zmíněných

---

[23] Prováděcí rozhodnutí Komise (EU) 2015/219 ze dne 29. ledna 2015, kterým se nahrazuje příloha prováděcího rozhodnutí 2013/115/EU o příručce SIRENE a dalších prováděcích opatřeních k Schengenskému informačnímu systému druhé generace (SIS II) (Úř. věst. L 44, 18.2.2015, s. 75).

[24] Doporučení Komise, kterým se vytváří katalog doporučení a osvědčených postupů pro správné používání Schengenského informačního systému druhé generace (SIS II) a pro výměnu doplňujících informací mezi příslušnými orgány členských států zavádějícími a používajícími SIS II (C(2015) 9169/1).

[25] Nařízení Rady (EU) č. 1053/2013 ze dne 7. října 2013 o vytvoření hodnotícího a monitorovacího mechanismu k ověření uplatňování schengenského *acquis* a o zrušení rozhodnutí výkonného výboru ze dne 16. září 1998, kterým se zřizuje Stálý výbor pro hodnocení a provádění Schengenu (Úř. věst. L 295, 6.11.2013, s. 27).

změn na základní práva a ochranu údajů byl vyhodnocen a podrobněji vysvětlen v následujícím oddíle („Základní práva“).

Tento návrh byl vypracován s využitím velkého souboru podkladů shromážděných pro účely celkového hodnocení SIS druhé generace, které se zaměřilo na jeho fungování a na možné oblasti zlepšení. Aby byl zajištěn výběr nejvhodnější a nejpřiměřenější vnitrostátní architektury, byla dále provedena studie posouzení dopadů z hlediska nákladů.

- **Základní práva a ochrana údajů**

Tento návrh rozvíjí a zlepšuje existující systém namísto vytvoření nového, což znamená, že staví na již zavedených, podstatných a účinných zárukách. Jelikož však SIS nadále zpracovává osobní údaje a bude zpracovávat další kategorie citlivých biometrických údajů, může mít potenciální dopady na základní práva osob. Ty byly důkladně zváženy, a proto byly zavedeny dodatečné záruky s cílem omezit shromažďování a další zpracování údajů na míru nezbytně nutnou a z operativního hlediska potřebnou a poskytnout přístup k těmto údajům pouze osobám, které mají operativní potřebu takové údaje zpracovávat. V tomto návrhu se stanoví jasné lhůty pro uchovávání údajů a výslovně se v něm uznává a zaručuje právo jednotlivců na přístup k údajům, které se jich týkají, jejich opravu a právo požadovat výmaz v souladu se základními právy těchto osob (viz oddíl o ochraně údajů a bezpečnosti).

Návrh kromě toho posiluje opatření na ochranu základních práv, protože právní formou stanoví požadavek na vymazání záznamu a zavádí posouzení přiměřenosti v případě prodloužení platnosti záznamu. Také upravuje rozsáhlé a pevné záruky pro používání biometrických identifikátorů, aby se předešlo nežádoucím důsledkům pro nevinné osoby.

Návrh také vyžaduje komplexní (*end-to-end*) zabezpečení všech prvků systému, které zajistí vyšší ochranu v něm uchovávaných údajů. Tím, že zavádí jasný postup pro řešení incidentů a zajišťuje lepší kontinuitu provozu SIS, je tento návrh plně v souladu s Listinou základních práv Evropské unie[26], a to nejen s ohledem na právo na ochranu osobních údajů. Vývoj a nepřetržité zvyšování efektivity SIS přispějí ke zlepšení bezpečnosti osob ve společnosti.

Návrh obsahuje významné změny z hlediska biometrických identifikátorů. Vedle otisků prstů by se za podmínky splnění právních požadavků měly shromažďovat a uchovávat rovněž otisky dlaní. Záznamy otisků prstů se připojují k alfanumerickým záznamům v SIS, jak stanoví článek 24. V budoucnu by mělo být možné porovnávat tyto daktyloskopické údaje (otisky prstů a otisky dlaní) s otisky prstů nalezenými na místě činu v případě, že se jedná o závažný trestný čin či teroristický trestný čin a s vysokou mírou pravděpodobnosti lze stanovit, že otisky patří pachateli. Vzniknou-li na základě dokladů určité osoby pochybnosti o její totožnosti, měly by příslušné orgány porovnat otisk prstu s otisky prstů uloženými v databázi SIS.

Návrh dále ukládá povinnost shromažďovat a uchovávat další údaje (např. informace o dokladech totožnosti), které pomáhají pracovníkům v praxi zjistit totožnost osob.

Návrh zaručuje právo subjektu údajů na účinnou právní ochranu umožňující napadnout jakékoliv rozhodnutí, které v každém případě zahrnuje právo na účinné prostředky nápravy před soudem podle článku 47 Listiny základních práv EU.

[26] Listina základních práv Evropské unie (2012/C 326/02).

4. ROZPOČTOVÉ DŮSLEDKY

SIS představuje jednotný informační systém. Výdaje plánované ve dvou z návrhů (v tomto návrhu a návrhu nařízení o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech) by proto měly být považovány nikoli za dvě oddělené částky, ale za jedinou. Rozpočtové důsledky změn nutných pro provedení obou návrhů jsou proto uvedeny v jediném legislativním finančním výkaze.

Vzhledem k doplňujícímu charakteru třetího návrhu (o navracení neoprávněně pobývajících státních příslušníků třetích zemí) jsou rozpočtové důsledky řešeny odděleně v samostatném finančním výkazu, který se týká pouze vytvoření této zvláštní kategorie záznamu.

Z posouzení různých aspektů činnosti, která musí být provedena v souvislosti se sítí, v centrálním SIS agenturou eu-LISA a ve vnitrostátních systémech členskými státy, vyplývá, že dva návrhy nařízení budou vyžadovat celkovou částku 64,3 milionu EUR na období 2018–2020.

Tato částka zahrnuje zvýšení šířky pásma sítě TESTA NG, neboť podle dvou uvedených návrhů bude síť přenášet soubory otisků prstů a zobrazení obličeje vyžadující vyšší propustnost a kapacitu (9,9 milionu EUR). Dále zahrnuje náklady agentury eu-LISA na zaměstnance a operační výdaje (17,6 milionu EUR). Agentura eu-LISA informovala Komisi, že v lednu 2018 plánuje přijmout tři nové smluvní zaměstnance, aby mohla včas zahájit fázi vývoje a zajistila zprovoznění aktualizovaných funkcí SIS v roce 2020. Předmětem tohoto návrhu jsou technické změny centrálního SIS za účelem rozšíření některých stávajících kategorií záznamů a vytvoření nových funkcí. Finanční výkaz, jenž tvoří přílohu tohoto návrhu, tyto změny zohledňuje.

Komise dále provedla studii posouzení dopadů na náklady, v níž vyhodnotila náklady na vnitrostátní vývoj požadované tímto návrhem[27]. Odhadované náklady činí 36,8 milionu EUR, které by měly být rozděleny mezi členské státy ve formě jednorázové částky. Každý členský stát tedy obdrží částku 1,2 milionu EUR na modernizaci vnitrostátního systému podle požadavků stanovených v tomto návrhu, která bude určena také na vytvoření částečné vnitrostátní kopie, pokud ještě neexistuje, nebo na záložní systém.

Za účelem modernizace a vytvoření funkcí podle uvedených dvou návrhů se plánuje přerozdělení zbývajícího finančního krytí na inteligentní hranice v rámci Fondu pro vnitřní bezpečnost. Finančním nástrojem, do nějž byl začleněn rozpočet na provedení balíčku týkajícího se inteligentních hranic, je nařízení o nástroji pro podporu v oblasti vnějších hranic v rámci Fondu pro vnitřní bezpečnost[28]. V článku 5 uvedeného nařízení se stanoví, že v rámci provádění programu pro zřizování systémů informačních technologií na podporu řízení migračních toků přes vnější hranice je za podmínek stanovených v článku 15 čerpáno 791 milionů EUR. Z těchto 791 milionů EUR je 480 milionů EUR vyhrazeno na vývoj systému vstupu/výstupu a 210 milionů EUR na vývoj evropského systému pro cestovní informace a povolení (ETIAS). Zbývající prostředky budou částečně použity k uhrazení nákladů na změny uvedené v obou návrzích týkajících se SIS.

---

27 Wavestone, „Posouzení dopadů technických zlepšení architektury SIS II z hlediska IKT – závěrečná zpráva“, 10. listopadu 2016, scénář 3, oddělená implementace N.SIS II.

28 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 (Úř. věst. L 150, 20.5.2014, s. 143).

5. OSTATNÍ PRVKY

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

Komise, členské státy a agentura eu-LISA budou pravidelně přezkoumávat a monitorovat využívání SIS s cílem zajistit jeho nepřetržité efektivní a účelné fungování. Při provádění technických a provozních opatření popsaných v tomto návrhu bude Komisi nápomocen výbor pro SISVIS.

Toto navrhované nařízení navíc v čl. 54 odst. 7 a 8 obsahuje ustanovení o formálním pravidelném přezkumu a procesu hodnocení.

Vždy po dvou letech musí agentura eu-LISA předložit Evropskému parlamentu a Radě zprávu o technickém fungování centrálního SIS, včetně zabezpečení, podpůrné komunikační infrastruktury a dvoustranné a mnohostranné výměny doplňujících informací mezi členskými státy.

Dále vždy po čtyřech letech musí Komise vypracovat celkové hodnocení SIS a výměny informací mezi členskými státy, které postoupí Parlamentu a Radě. Obsahem tohoto hodnocení je:

- přezkoumání dosažených výsledků v porovnání s vytyčenými cíli,
- posouzení, zda platí důvod pro vznik systému,
- uplatňování nařízení v souvislosti s centrálním systémem,
- vyhodnocení zabezpečení centrálního systému,
- zhodnocení dopadů budoucího fungování systému.

Agentura eu-LISA má nyní také za úkol zpracovávat denní, měsíční a roční statistiky týkající se využívání SIS a zajistit nepřetržité monitorování systému a jeho fungování v porovnání s vytyčenými cíli.

- **Podrobné vysvětlení nových ustanovení návrhu**

Ustanovení společná v tomto návrhu a návrhu nařízení o zřízení, provozu a využívání SIS v oblasti policejní spolupráce a justiční spolupráce v trestních věcech:

- Obecná ustanovení (články 1 až 3)
- Technická architektura a způsoby provozování SIS (články 4 až 14)
- Povinnosti agentury eu-LISA (články 15 až 18)
- Právo na přístup a uchovávání záznamů (články 29, 30, 31, 33 a 34)
- Obecná pravidla pro zpracování údajů a ochranu údajů (články 36 až 53)
- Sledování a statistika (článek 54)

Komplexní využívání všech prvků SIS (*end-to-end*)

S více než dvěma miliony koncových uživatelů v rámci příslušných orgánů v celé Evropě je SIS velmi hojně využívaným a účinným nástrojem pro výměnu informací. Tyto návrhy obsahují pravidla pro komplexní provoz všech prvků systému, včetně centrálního SIS provozovaného agenturou eu-LISA, vnitrostátních systémů a aplikací pro koncové uživatele.

Zabývají se nejen centrálním a vnitrostátními systémy jako takovými, ale i technickými a provozními potřebami koncových uživatelů.

V čl. 9 odst. 2 se stanoví, že koncoví uživatelé musí obdržet údaje nezbytné pro plnění svých úkolů (zejména veškeré údaje potřebné k určení totožnosti subjektu údajů a přijetí požadovaného opatření). Článek také obsahuje společný plán pro zavedení SIS v členských státech, čímž zajišťuje harmonizaci všech vnitrostátních systémů. Článek 6 uvádí, že každý členský stát musí zajistit nepřetržitou dostupnost údajů SIS pro koncové uživatele, aby se maximalizoval operativní přínos omezením možnosti výpadku.

Ustanovení čl. 10 odst. 3 zajišťuje, aby se zabezpečení zpracování údajů vztahovalo i na zpracování údajů, které provádí koncový uživatel. Článek 14 ukládá členským státům povinnost zajistit, aby zaměstnanci s přístupem do SIS absolvovali pravidelnou a průběžnou odbornou přípravu týkající se zabezpečení údajů a pravidel o ochraně údajů.

Díky začlenění uvedených opatření tento návrh podrobněji popisuje komplexní fungování všech prvků SIS a stanoví pravidla a povinnosti pro miliony koncových uživatelů v celé Evropě. Aby byl SIS využíván s maximální účinností, měly by členské státy zaručit, že pokaždé, když jsou koncoví uživatelé v dané zemi oprávněni provádět vyhledávání v národní policejní či imigrační databázi, vyhledávají souběžně i v SIS. Tak může SIS splnit svůj cíl fungovat jako hlavní kompenzační opatření v prostoru bez kontrol na vnitřních hranicích a členské státy dokážou lépe reagovat na přeshraniční rozměr trestné činnosti a mobilitu pachatelů. Toto souběžné vyhledávání musí vždy probíhat v souladu s článkem 4 směrnice (EU) 2016/680[29].

Kontinuita provozu

Návrhy posilují ustanovení týkající se kontinuity provozu jak na vnitrostátní úrovni, tak v agentuře eu-LISA (články 4, 6, 7 a 15). Tato ustanovení zajišťují, že bude zachována funkčnost a dostupnost SIS pro pracovníky v terénu i v případě problémů ohrožujících systém.

Kvalita údajů

Návrh zachovává zásadu, že členský stát, který je vlastníkem údajů, nese rovněž odpovědnost za správnost údajů vložených do SIS (článek 39). Je však nezbytné stanovit centrální mechanismus spravovaný agenturou eu-LISA umožňující členským státům pravidelně přezkoumávat záznamy, které obsahují povinná datová pole, jejichž kvalita může budit obavy. Článek 15 návrhu proto zmocňuje agenturu eu-LISA, aby v pravidelných intervalech vypracovávala pro členské státy zprávy o kvalitě údajů. Tuto činnost může usnadnit úložiště údajů pro vypracovávání statistických zpráv a zpráv o kvalitě údajů (článek 54). Tato zlepšení zohledňují prozatímní zjištění expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu.

Fotografie, zobrazení obličeje, daktyloskopické údaje a profily DNA

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

Možnost vyhledávat s pomocí otisků prstů za účelem určení totožnosti osoby je již stanovena v článku 22 nařízení (ES) č. 1987/2006 a rozhodnutí Rady 2007/533/SVV. Návrhy ukládají povinnost provést takovéto vyhledávání, jestliže nelze zjistit totožnost osoby jinými prostředky. V současnosti může být zobrazení obličeje použito pouze k potvrzení totožnosti osoby nalezené na základě alfanumerického vyhledávání, ale nemůže sloužit jako základ pro vyhledávání. Pozměněné články 22 a 28 navíc stanoví, že zobrazení obličeje, fotografie a otisky dlaní mohou být použity k vyhledávání v systému a určení totožnosti osob, jakmile to bude technicky možné. Daktyloskopie je nauka o otiscích prstů, jež jsou využívány jako metoda určení totožnosti. Podle odborníků v oboru daktyloskopie mají otisky dlaní jedinečnou povahu a charakteristické znaky, které umožňují stejně přesné a průkazné srovnání jako otisky prstů. Otisky dlaní lze tedy používat ke zjištění totožnosti osoby stejným způsobem jako otisky prstů. Odebírání otisků dlaní a deseti válených a deseti píchaných otisků prstů je již dlouhá desetiletí běžnou policejní praxí. Otisky dlaní mají hlavní využití pro účely určení totožnosti v případě, že má daná osoba úmyslně či neúmyslně poškozená bříška prstů. Důvodem může být snaha vyhnout se identifikaci či sejmutí otisků nebo poškození způsobené úrazem či těžkou manuální prací. V průběhu jednání o technických pravidlech systému automatizované identifikace otisků prstů (AFIS), začleněného do SIS, členské státy hlásily značný úspěch při zjišťování totožnosti nelegálních migrantů, kteří si bříška prstů poškodili s úmyslem vyhnout se určení totožnosti. Odebírání otisků dlaní by orgánům členských států umožnilo následné určení totožnosti.

Využití zobrazení obličeje k určení totožnosti zajistí větší soudržnost mezi SIS a navrhovaným systémem vstupu/výstupu EU využívajícím elektronické brány a samoobslužné kiosky. Tato funkce bude používána pouze na řádných hraničních přechodech.

Přístup orgánů do SIS – institucionální uživatelé

V tomto pododdíle jsou popsány nové prvky přístupových práv udělených agenturám EU (institucionálním uživatelům). Přístupová práva příslušných vnitrostátních orgánů se nemění.

Přístup do SIS a k údajům v něm uloženým, který potřebují ke své práci, mají Europol (článek 30), Evropská agentura pro pohraniční a pobřežní stráž – jakož i její jednotky, týmy pracovníků, kteří se podílejí na úkolech spojených s navracením, a členové podpůrných týmů pro řízení migrace – a ústřední jednotka ETIAS zřízená v rámci agentury (články 31 a 32). Zavádějí se odpovídající záruky s cílem zabezpečit řádnou ochranu údajů v systému (což zahrnuje i ustanovení v článku 33, podle něhož mají uvedené subjekty přístup pouze k těm údajům, které potřebují k plnění svých úkolů).

Těmito změnami se rozšiřuje přístup Europolu k záznamům v SIS o odepření vstupu, aby Europol mohl optimálně využívat tohoto systému při plnění svých úkolů, a doplňují se nová ustanovení, jimiž se uděluje přístup do tohoto systému Evropské agentuře pro pohraniční a pobřežní stráž a jejím jednotkám při provádění různých operací v rámci jejich mandátu pomáhat členským státům. Podle návrhu nařízení Evropského parlamentu a Rady, kterým se zřizuje evropský systém pro cestovní informace a povolení (ETIAS)[30], předloženého Komisí, bude navíc ústřední jednotka ETIAS v rámci Evropské agentury pro pohraniční a pobřežní stráž prostřednictvím systému ETIAS ověřovat v SIS, zda státní příslušník třetí země, který

[30] COM (2016) 731 final.

žádá o cestovní povolení, není předmětem záznamu v SIS. Proto bude mít ústřední jednotka ETIAS také přístup do SIS[31].

Podle čl. 29 odst. 3 mohou mít vnitrostátní vízové orgány při plnění svých úkolů také právo na přístup k záznamům týkajícím se dokladů, které byly vloženy v souladu s nařízením (EU) 2008/.... o zřízení, provozu a využívání SIS v oblasti policejní spolupráce a justiční spolupráce v trestních věcech.

Uvedené orgány tedy získají přístup do SIS a k údajům v tomto systému, které potřebují k plnění svých úkolů, přičemž se zároveň zavádějí odpovídající záruky s cílem zabezpečit řádnou ochranu údajů v systému (což zahrnuje i ustanovení v článku 35, podle něhož mají uvedené subjekty přístup pouze k těm údajům, které potřebují k plnění svých úkolů).

Odepření vstupu a pobytu

V současnosti může členský stát podle čl. 24 odst. 3 nařízení o SIS II vložit záznam do SIS o osobách, na které se vztahuje zákaz vstupu z důvodu porušení vnitrostátních právních předpisů v oblasti migrace. Revidovaný čl. 24 odst. 3 vyžaduje, aby byl do SIS vložen záznam ve všech případech, kdy byl vydán zákaz vstupu neoprávněně pobývajícímu státnímu příslušníkovi třetí země podle ustanovení v souladu se směrnicí 2008/115/ES. Toto ustanovení upravuje rovněž lhůty a podmínky pro vkládání těchto záznamů poté, co státní příslušník třetí země opustil území členských států na základě povinnosti navrácení. Ustanovení bylo vloženo s cílem zabránit zobrazení zákazů vstupu v SIS, zatímco se dotčený státní příslušník třetí země stále pohybuje na území EU. Protože zákazy vstupu brání opětovnému vstupu na území členských států, mohou nabýt účinku až po navrácení (se) dotčeného státního příslušníka třetí země. Členské státy by zároveň měly přijmout veškerá nezbytná opatření k zajištění toho, že nedojde k žádné prodlevě mezi okamžikem navrácení (se) a aktivací záznamu v SIS.

Tento návrh úzce souvisí s návrhem Komise[32] týkajícím se využívání SIS při navracení neoprávněně pobývajících státních příslušníků třetích zemí, který stanoví podmínky a postupy pro vkládání záznamů o rozhodnutích o navrácení do SIS. Uvedený návrh obsahuje mechanismus pro sledování, zda státní příslušníci třetích zemí, kteří jsou předmětem rozhodnutí o navrácení, skutečně opustili území EU, a mechanismus varování v případě porušení tohoto rozhodnutí. V článku 26 je stanoven postup konzultace, který musí členské státy dodržovat, pokud nalezly záznam o odepření vstupu nebo pobytu – nebo pokud mají v úmyslu takový záznam vložit – který je v rozporu s rozhodnutím jiného členského státu, například platným povolením k pobytu. Tato pravidla by měla zabránit vzniku rozporuplných pokynů, které mohou být v důsledku takových situací vydávány, a případně je odstranit. Zároveň by měla poskytnout jasné pokyny koncovým uživatelům ohledně opatření, která mají být v takové situaci přijata, a orgánům členských států ohledně toho, zda má být záznam vymazán.

Článek 27 (bývalý článek 26 nařízení (ES) č. 1987/2006) je určen k provedení sankčního režimu EU pro státní příslušníky třetích zemí, kterým byl omezen vstup na území EU v souladu s článkem 29 Smlouvy o Evropské unii. Aby bylo možné takové záznamy vkládat, bylo nezbytné stanovit požadavek na minimální údaje nezbytné pro určení totožnosti osoby, tedy příjmení a datum narození. Skutečnost, že nařízením (ES) č. 1987/2006 byl požadavek

[31] Ústřední jednotce ETIAS se uděluje přístup k údajům vloženým podle článků 24 a 27 tohoto nařízení.

[32] COM (2016)…

vkládat datum narození zrušen, způsobila značné problémy, neboť podle technických pravidel a parametrů vyhledávání nelze bez data narození vytvořit záznam v SIS. Jelikož je článek 27 nezbytný pro vytvoření účinného sankčního režimu EU, neuplatňuje se zde požadavek přiměřenosti.

K zajištění většího souladu se směrnicí 2008/115/ES byla terminologie používaná při odkazování na účel záznamu („odepření vstupu a pobytu“) sjednocena se zněním ve směrnici.

Rozlišování osob s podobnými znaky

K zajištění řádného zpracování a uložení údajů a ke snížení rizika duplicity a nesprávného určení totožnosti stanoví článek 41 postup v případě, že se při vkládání nového záznamu zjistí existence staršího záznamu s podobnými znaky.

Ochrana a zabezpečení údajů

Tento návrh vyjasňuje odpovědnost za předcházení incidentům, které by mohly ohrozit bezpečnost či neporušenost infrastruktury SIS, údajů SIS nebo doplňujících informací, a za jejich hlášení a řešení (články 10, 16 a 40).

Článek 12 obsahuje ustanovení o vedení protokolů historie záznamů a nahlížení do nich.

V čl. 15 odst. 3 se zachovává čl. 15 odst. 3 nařízení (ES) č. 1987/2006 a stanoví se, že Komise nadále odpovídá za smluvní řízení komunikační infrastruktury, včetně úkolů souvisejících s plněním rozpočtu, pořizování a obnovy. Tyto úkoly budou přeneseny na agenturu eu-LISA v druhém souboru návrhů o SIS v červnu 2017.

Článek 21 rozšiřuje požadavek, aby členské státy posoudily před pořízením záznamu jeho přiměřenost, i na rozhodnutí o případném prodloužení doby platnosti záznamu. Nově však čl. 24 odst. 2 písm. c) ukládá členským státům povinnost vytvořit za všech okolností záznam o osobách, jejichž činnost spadá do působnosti článků 1, 2, 3 a 4 rámcového rozhodnutí Rady 2002/475/SVV o boji proti terorismu.

Kategorie údajů a zpracování údajů

S cílem poskytnout koncovým uživatelům více informací, které budou zároveň přesnější, usnadnit a urychlit přijetí požadovaného opatření a umožnit lepší identifikaci subjektu záznamu rozšiřuje tento návrh počet druhů informací (článek 20), které mohou být uchovávány o osobách, o nichž byl pořízen záznam, aby zahrnovaly také:

- údaj, zda se dotčená osoba účastní činnosti uvedené v článcích 1, 2, 3 a 4 rámcového rozhodnutí Rady 2002/475/SVV o boji proti terorismu,
- údaj, zda se záznam týká občana EU nebo jiné osoby, která požívá práva na volný pohyb rovnocenného právu občanů EU,
- údaj, zda se rozhodnutí o odepření vstupu zakládá na ustanoveních článků 24 nebo 27,
- druh trestného činu (pro záznamy pořízené podle čl. 24 odst. 2),
- informace z dokladu totožnosti nebo cestovního dokladu,
- barevnou kopii dokladu totožnosti nebo cestovního dokladu,

- fotografie a zobrazení obličeje,
- otisky prstů a otisky dlaní.

Mít k dispozici odpovídající údaje je nezbytnou podmínkou pro správné určení totožnosti osoby, která je kontrolována na hraničním přechodu či uvnitř země nebo která žádá o povolení k pobytu. Nesprávné určení totožnosti může způsobit problémy v oblasti lidských práv a může rovněž vést k situacím, kdy nelze přijmout vhodná následná opatření, protože není známa existence záznamu nebo jeho obsah.

Pokud jde o informace o rozhodnutí zakládajícím záznam, lze rozlišit čtyři důvody: předchozí odsouzení podle čl. 24 odst. 2 písm. a), závažnou bezpečnostní hrozbu podle čl. 24 odst. 2 písm. b), zákaz vstupu podle čl. 24 odst. 3 a omezující opatření podle článku 27. Aby bylo zajištěno přijetí vhodného opatření v případě pozitivního nálezu, je též nezbytné uvést, zda se záznam týká občana EU nebo jiné osoby požívající práva na volný pohyb rovnocenného právům občanů EU. Mít k dispozici odpovídající údaje je nezbytnou podmínkou pro správné určení totožnosti osoby, která je kontrolována na hraničním přechodu či uvnitř země nebo která žádá o povolení k pobytu. Nesprávné určení totožnosti může způsobit problémy v oblasti lidských práv a může rovněž vést k situacím, kdy nelze přijmout vhodná následná opatření, protože není známa existence záznamu nebo jeho obsah.

Rovněž se rozšiřuje seznam osobních údajů (článek 42), které mohou být vloženy do SIS a zpracovány za účelem řešení zneužití totožnosti, protože větší objem údajů usnadňuje určení totožnosti poškozené osoby i osoby, která totožnost zneužila. Rozšíření tohoto ustanovení nepředstavuje žádné riziko, protože všechny tyto údaje mohou být vloženy pouze se souhlasem poškozené osoby, jejíž totožnost byla zneužita. Uvedené ustanovení bude nyní zahrnovat:

- zobrazení obličeje,
- otisky dlaní,
- informace z dokladu totožnosti,
- adresu poškozené osoby,
- jméno otce a matky poškozené osoby.

Článek 20 stanoví podrobnější údaje v záznamech. Jedná se o kategorie záznamů z důvodu odepření vstupu a pobytu a informace z dokladů totožnosti subjektů údajů. Tyto rozšířené údaje umožňují lepší identifikaci dotčené osoby, ale i přijetí informovanějšího rozhodnutí ze strany koncových uživatelů. Na ochranu koncových uživatelů, kteří provádějí kontroly, SIS také zobrazí, zda určitá osoba, o níž byl pořízen záznam, spadá do některé z kategorií uvedených v článcích 1, 2, 3 a 4 rámcového rozhodnutí Rady 2002/475/SVV o boji proti terorismu[33].

Návrh jasně uvádí, že členské státy nesmějí kopírovat údaje vložené jiným členským státem do jiných vnitrostátních souborů údajů (článek 37).

Uchovávání

Článek 34 stanoví lhůtu pro přezkum záznamů. Maximální doba uchovávání záznamů o odepření vstupu a pobytu byla sjednocena s maximální možnou délkou zákazů vstupu

[33] Rámcové rozhodnutí Rady 2002/475/SVV ze dne 13. června 2002 o boji proti terorismu (Úř. věst. L 164, 22.6.2002, s. 3).

vydaných v souladu s článkem 11 směrnice 2008/115/ES. Maximální doba uchovávání záznamů tak bude činit pět let. Členské státy však mohou stanovit kratší lhůty.

Výmaz

Článek 35 vymezuje, za jakých okolností musí být záznamy vymazány, a tak zajišťuje větší harmonizaci vnitrostátních postupů v této oblasti. Tento článek obsahuje zvláštní ustanovení pro pracovníky centrály SIRENE, která se týkají aktivního vymazávání nepotřebných záznamů, pokud centrála neobdrží odpověď od příslušných orgánů.

Práva subjektů údajů na přístup k údajům, opravu nepřesných údajů a výmaz protiprávně uchovávaných údajů

Podrobná pravidla týkající se práv subjektu údajů zůstávají nezměněna, protože současná pravidla již zaručují vysokou úroveň ochrany a jsou v souladu s nařízením (EU) 2016/679[34] a směrnicí 2016/680[35]. Článek 48 navíc stanoví, za jakých podmínek nemusí členské státy subjektům údajů poskytnout informace. Musí se jednat o jeden z důvodů uvedených v tomto článku a zároveň o přiměřené a nezbytné opatření v souladu s vnitrostátním právem.

Statistika

Aby byl zachováván přehled o fungování opravných prostředků, stanoví článek 49 standardní statistický systém, který umožní vypracovávat roční zprávy o těchto údajích:

- počet žádostí subjektů údajů o přístup,
- počet žádostí o opravu nepřesných údajů a výmaz protiprávně uchovávaných údajů,
- počet případů projednávaných u soudů,
- počet případů, kdy soud rozhodl ve prospěch žalobce, a
- počet připomínek k případům vzájemného uznávání konečných rozhodnutí vydaných soudy nebo orgány jiných členských států v souvislosti se záznamy vytvořenými členským státem, jenž záznam pořídil.

Sledování a statistika

Článek 54 stanoví opatření, která musí být zavedena za účelem zajištění řádného monitorování SIS a jeho fungování v porovnání s vytyčenými cíli. Agentura eu-LISA má proto za úkol zpracovávat denní, měsíční a roční statistiky týkající se jeho využívání.

Podle čl. 54 odst. 5 musí agentura eu-LISA postoupit členským státům, Komisi, Europolu a Evropské agentuře pro pohraniční a pobřežní stráž statistické zprávy, které vypracuje, a

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

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

Komise může tuto agenturu požádat o další statistické zprávy a zprávy o kvalitě údajů týkající se SIS a komunikace prostřednictvím central SIRENE.

Podle čl. 54 odst. 6 má být vytvořeno a provozováno centrální úložiště údajů jako součást úkolu agentury eu-LISA sledovat fungování SIS. Oprávnění pracovníci členských států, Komise, Europolu a Evropské agentury pro pohraniční a pobřežní stráž tak získají přístup k údajům vymezeným v čl. 54 odst. 3, což umožní zpracování požadovaných statistik.

2016/0408 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol, o změně nařízení (EU) č. 515/2014 a o zrušení nařízení (ES) č. 1987/2006

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na čl. 77 odst. 2 písm. b) a d) a čl. 79 odst. 2 písm. c) této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Schengenský informační systém (dále jen „SIS“) představuje nezbytný nástroj pro uplatňování ustanovení schengenského *acquis* začleněného do rámce Evropské unie. SIS představuje jedno z hlavních vyrovnávacích opatření přispívajících k udržení vysokého stupně bezpečnosti v prostoru svobody, bezpečnosti a práva Evropské unie prostřednictvím podpory operativní spolupráce mezi příslušníky pohraniční stráže, policejními, celními a dalšími donucovacími orgány, justičními orgány v trestních věcech a imigračními orgány.

(2) SIS byl zřízen podle ustanovení hlavy IV Úmluvy ze dne 19. června 1990 k provedení Schengenské dohody ze dne 14. června 1985 mezi vládami států Hospodářské unie Beneluxu, Spolkové republiky Německo a Francouzské republiky o postupném odstraňování kontrol na společných hranicích[36] (dále jen „Schengenská úmluva“). Vývoj SIS druhé generace (dále jen „SIS II“) byl svěřen Komisi na základě nařízení Rady (ES) č. 2424/2001[37] a rozhodnutí Rady 2001/886/SVV[38] a tento systém byl zřízen nařízením (ES) č. 1987/2006[39] a rozhodnutím Rady 2007/533/SVV[40]. SIS II nahradil SIS vytvořený na základě Schengenské úmluvy.

---

36 Úř. věst. L 239, 22.9.2000, s. 19. Úmluva ve znění nařízení Evropského parlamentu a Rady (ES) č. 1160/2005 (Úř. věst. L 191, 22.7.2005, s. 18).

37 Úř. věst. L 328, 13.12.2001, s. 4.

38 Rozhodnutí Rady 2001/886/SVV ze dne 6. prosince 2001 o vývoji Schengenského informačního systému druhé generace (SIS II) (Úř. věst. L 328, 13.12.2001, s. 1).

39 Nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 ze dne 20. prosince 2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II) (Úř. věst. L 181, 28.12.2006, s. 4).

(3) Po třech letech od uvedení SIS II do provozu provedla Komise vyhodnocení tohoto systému v souladu s čl. 24 odst. 5, čl. 43 odst. 5 a čl. 50 odst. 5 nařízení (ES) č. 1987/2006 a s článkem 59 a čl. 65 odst. 5 rozhodnutí 2007/533/SVV. Hodnotící zpráva a související pracovní dokument útvarů Komise byly přijaty dne 21. prosince 2016[41]. Doporučení uvedená v těchto dokumentech by měla být v tomto nařízení vhodně zohledněna.

(4) Toto nařízení představuje nezbytný právní základ pro řízení SIS v souvislosti se záležitostmi spadajícími do oblasti působnosti hlavy V kapitoly 2 Smlouvy o fungování Evropské unie. Nařízení Evropského parlamentu a Rady (EU) 2018/… o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech[42] představuje nezbytný právní základ pro řízení SIS v souvislosti se záležitostmi spadajícími do oblasti působnosti hlavy V kapitol 4 a 5 Smlouvy o fungování Evropské unie.

(5) Skutečnost, že legislativní základ nezbytný pro řízení SIS sestává ze samostatných nástrojů, nemá dopad na zásadu, že SIS představuje jednotný informační systém, který by měl jako takový fungovat. Proto by určitá ustanovení těchto nástrojů měla být totožná.

(6) Je nezbytné konkrétně vymezit účely SIS, jeho technickou architekturu a financování, stanovit pravidla pro komplexní provoz a využívání všech prvků tohoto systému a vymezit povinnosti, kategorie údajů vkládaných do systému, účely jejich vkládání, kritéria jejich vkládání, orgány oprávněné k přístupu do systému a používání biometrických identifikátorů, jakož i další pravidla týkající se zpracování údajů.

(7) SIS zahrnuje centrální systém (dále jen „centrální SIS“) a vnitrostátní systémy obsahující úplnou nebo částečnou kopii databáze SIS. Vzhledem k tomu, že SIS je nejdůležitějším nástrojem pro výměnu informací v Evropě, je nezbytné zajistit jeho nerušený provoz na centrální i na vnitrostátní úrovni. Každý členský stát by proto měl vytvořit částečnou nebo úplnou kopii databáze SIS a zřídit její záložní systém.

(8) Je nutné udržovat příručku obsahující podrobná pravidla pro výměnu určitých doplňujících informací týkajících se opatření, která záznam vyžaduje. Výměnu těchto informací by měly zajišťovat vnitrostátní orgány jednotlivých členských států (centrály SIRENE).

(9) Aby byla zachována účinná výměna doplňujících informací týkajících se opatření, která mají být podle záznamů přijata, je vhodné posílit fungování centrál SIRENE stanovením požadavků na dostupné zdroje, odbornou přípravu uživatelů a lhůtu pro zodpovězení dotazů obdržených z jiných centrál SIRENE.

(10) Provozní řízení centrálních složek SIS vykonává Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva[43]

---

40 Rozhodnutí Rady 2007/533/SVV ze dne 12. června 2007 o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II) (Úř. věst. L 205, 7.8.2007, s. 63).

41 Zpráva Komise Evropskému parlamentu a Radě o hodnocení Schengenského informačního systému druhé generace (SIS II) v souladu s čl. 24 odst. 5, čl. 43 odst. 3 a čl. 50 odst. 5 nařízení (ES) č. 1987/2006 a čl. 59 odst. 3 a čl. 66 odst. 5 rozhodnutí 2007/533/SVV a průvodní pracovní dokument útvarů Komise.

42 Nařízení (EU) 2018/...

43 Agentura byla zřízena nařízením Evropského parlamentu a Rady (EU) č. 1077/2011 ze dne 25. října 2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (Úř. věst. L 286, 1.11.2011, s. 1).

(dále jen „agentura“). Aby agentura mohla vyčlenit nezbytné finanční a personální zdroje zahrnující všechny aspekty provozního řízení centrálního SIS, mělo by toto nařízení podrobně vymezit její úkoly, zejména pokud jde o technické aspekty výměny doplňujících informací.

(11) Aniž je dotčena odpovědnost členských států za správnost údajů vkládaných do SIS, měla by agentura nést odpovědnost za zlepšování kvality údajů zavedením centrálního nástroje pro sledování kvality údajů a za předkládání zpráv členským státům v pravidelných intervalech.

(12) Aby bylo možno lépe sledovat využívání SIS s cílem analyzovat tendence, pokud jde o migrační tlak a správu hranic, měla by být agentura schopna vytvořit špičkovou kapacitu pro statistické hlášení členským státům, Komisi, Europolu a Evropské agentuře pro pohraniční a pobřežní stráž, aniž by byla ohrožena neporušenost údajů. Mělo by být proto zřízeno centrální úložiště statistických údajů. Žádné vypracované statistiky by neměly obsahovat osobní údaje.

(13) SIS by měl obsahovat další kategorie údajů, aby koncoví uživatelé mohli na základě záznamu činit informovaná rozhodnutí bez ztráty času. Záznamy pro účely odepření vstupu a pobytu by proto měly obsahovat informace o rozhodnutí, na němž se daný záznam zakládá. Za účelem usnadnění identifikace a odhalování vícenásobných identit by měl být v záznamu dále uveden odkaz na doklad totožnosti nebo osobní identifikační číslo včetně kopie takového dokladu, jsou-li k dispozici.

(14) SIS by neměl uchovávat žádné údaje použité k vyhledávání s výjimkou protokolů umožňujících ověřit, zda je vyhledávání zákonné, za účelem sledování zákonnosti zpracovávání údajů, pro vlastní kontrolu, pro zajištění řádného fungování N.SIS, neporušenosti údajů a jejich zabezpečení.

(15) SIS by měl umožnit zpracování biometrických údajů s cílem napomoci spolehlivému určení totožnosti dotyčných osob. Ve stejném smyslu by měl SIS umožňovat rovněž zpracování údajů o osobách, jejichž totožnost byla zneužita (aby se předešlo nežádoucím důsledkům způsobeným chybným určením totožnosti), s výhradou odpovídajících záruk, zejména se souhlasem dotyčné osoby a za přísného omezení účelů, pro něž se tyto údaje mohou zákonným způsobem zpracovávat.

(16) Členské státy by měly provést nezbytná technická opatření, aby pokaždé, když jsou koncoví uživatelé oprávněni provést vyhledávání ve vnitrostátní policejní nebo imigrační databázi, vyhledávali také souběžně v SIS, a to v souladu s článkem 4 směrnice Evropského parlamentu a Rady (EU) 2016/680[44]. To by mělo zajistit, aby SIS fungoval v prostoru bez kontrol na vnitřních hranicích jako hlavní kompenzační opatření a dokázal lépe reagovat na přeshraniční rozměr trestné činnosti a mobilitu pachatelů.

(17) Toto nařízení by mělo stanovit podmínky pro používání daktyloskopických údajů a zobrazení obličeje pro účely určení totožnosti. Používání zobrazení obličeje pro účely určení totožnosti v SIS by též mělo přispět k zajištění jednotnosti postupů hraničních kontrol, jestliže je nezbytné určení a ověření totožnosti na základě daktyloskopických údajů a zobrazení obličeje. V případě jakýchkoli pochybností o totožnosti dané osoby

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

by vyhledávání pomocí daktyloskopických údajů mělo být povinné. Zobrazení obličeje by měla být používána za účelem určení totožnosti pouze v rámci běžných hraničních kontrol prováděných v samoobslužných kioscích a elektronických branách.

(18) Mělo by být umožněno porovnávání otisků prstů nalezených na místě činu s daktyloskopickými údaji uloženými v SIS, pokud lze s vysokou mírou pravděpodobnosti stanovit, že patří pachateli závažné trestné činnosti nebo teroristického trestného činu. Závažnou trestnou činností je třeba rozumět trestné činy vyjmenované v rámcovém rozhodnutí Rady 2002/584/SVV[45] a „teroristickým trestným činem“ je třeba rozumět trestné činy podle vnitrostátního práva uvedené v rámcovém rozhodnutí Rady 2002/475/SVV[46].

(19) Členským státům by mělo být umožněno zavést odkazy mezi záznamy v SIS. Vytvoření odkazů mezi dvěma nebo více záznamy členským státem by nemělo mít dopad na přijímaná opatření, na délku doby uchovávání ani na práva přístupu k záznamům.

(20) Větší míry účinnosti, harmonizace a soudržnosti lze dosáhnout uložením povinnosti vkládat do SIS veškeré zákazy vstupu vydané příslušnými orgány členských států v řízení v souladu se směrnicí 2008/115/ES[47] a stanovením společných pravidel pro vkládání těchto záznamů po navrácení neoprávněně pobývajícího státního příslušníka třetí země. Členské státy by měly přijmout veškerá nezbytná opatření k zajištění toho, že nedojde k žádné prodlevě mezi okamžikem, kdy státní příslušník třetí země opustí schengenský prostor, a aktivací záznamu v SIS. To by mělo zaručit úspěšné vymáhání zákazů vstupu na hraničních přechodech na vnějších hranicích, a účinně tak zabránit opětovnému vstupu do schengenského prostoru.

(21) Toto nařízení by mělo stanovit závazná pravidla pro konzultaci mezi vnitrostátními orgány v případě, že státní příslušník třetí země má nebo může získat platné povolení k pobytu nebo jiné oprávnění nebo právo k pobytu udělované v jednom členském státě, přičemž jiný členský stát má v úmyslu pořídit nebo již vložil záznam pro účely odepření vstupu nebo pobytu tomuto státnímu příslušníkovi třetí země. Takové situace vytvářejí značnou nejistotu jak pro příslušníky pohraniční stráže, tak pro policejní a imigrační orgány. Je proto vhodné stanovit závaznou lhůtu pro rychlou konzultaci s konečným výsledkem, aby se zabránilo případnému vstupu osob představujících hrozbu do schengenského prostoru.

(22) Tímto nařízením by nemělo být dotčeno použití směrnice 2004/38/ES[48].

(23) Záznamy by v SIS měly být uchovávány nanejvýš po dobu nezbytnou pro splnění účelů, pro které byly pořízeny. Aby se snížila administrativní zátěž orgánů zabývajících se za různými účely zpracováním údajů o osobách, je vhodné sjednotit maximální dobu uchování záznamů o odepření vstupu a pobytu s maximální možnou délkou zákazů vstupu vydaných v řízení v souladu se směrnicí 2008/115/ES. Proto by

---

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

46 Rámcové rozhodnutí Rady 2002/475/SVV ze dne 13. června 2002 o boji proti terorismu (Úř. věst. L 164, 22.6.2002, s. 3).

47 Směrnice Evropského parlamentu a Rady 2008/115/ES ze dne 16. prosince 2008 o společných normách a postupech v členských státech při navracení neoprávněně pobývajících státních příslušníků třetích zemí (Úř. věst. L 348, 24.12.2008, s. 98).

48 Směrnice Evropského parlamentu a Rady 2004/38/ES ze dne 29. dubna 2004 o právu občanů Unie a jejich rodinných příslušníků svobodně se pohybovat a pobývat na území členských států (Úř. věst. L 158, 30.4.2004, s. 77).

doba uchovávání záznamů o osobách měla činit nejvýše pět let. Obecnou zásadou je, že záznamy o osobách by měly být ze SIS automaticky vymazány po uplynutí pěti let. Rozhodnutí o uchování záznamů o osobách by měla vycházet z komplexního individuálního posouzení. Členské státy by měly během vymezeného období záznamy o osobách přezkoumat a měly by vést statistiku o počtu záznamů o osobách, u nichž byla doba uchovávání prodloužena.

(24) Na vložení záznamu do SIS a prodloužení doby jeho platnosti by se měl vztahovat nezbytný požadavek přiměřenosti spočívající v posouzení, zda je daný případ dostatečně přiměřený, relevantní a závažný pro vložení záznamu do SIS. V případě trestných činů podle článků 1, 2, 3 a 4 rámcového rozhodnutí Rady 2002/475/SVV o boji proti terorismu[49] by vždy měl být vytvořen záznam o státních příslušnících třetích zemí pro účely odepření vstupu a pobytu, který zohlední vysoký stupeň ohrožení a celkový negativní dopad, jaký může daná činnost mít.

(25) Neporušenost údajů SIS má prvořadý význam. Proto by měly být stanoveny odpovídající záruky pro zpracování údajů SIS na centrální i na vnitrostátní úrovni s cílem zajistit komplexní (*end-to-end*) zabezpečení údajů. Orgány, které se zabývají zpracováním údajů, by měly být vázány bezpečnostními požadavky uvedenými v tomto nařízení a měly by se řídit jednotným postupem hlášení incidentů.

(26) Údaje zpracovávané v SIS za použití tohoto nařízení by neměly být poskytovány ani zpřístupňovány žádným třetím zemím nebo mezinárodním organizacím.

(27) Pro zvýšení účinnosti práce imigračních orgánů rozhodujících o právu státních příslušníků třetích zemí na vstup a pobyt na území členských států a o navracení neoprávněně pobývajících státních příslušníků třetích zemí je vhodné poskytnout jim přístup do SIS podle tohoto nařízení.

(28) Na zpracování osobních údajů orgány členských států podle tohoto nařízení by se mělo použít nařízení (EU) 2016/679[50], ledaže by se použila směrnice (EU) 2016/680[51]. Na zpracování osobních údajů orgány a institucemi Unie při plnění jejich úkolů podle tohoto nařízení by se mělo použít nařízení Evropského parlamentu a Rady (ES) č. 45/2001[52]. Je-li to potřebné, měla by být ustanovení směrnice (EU) 2016/680, nařízení (EU) 2016/679 a nařízení (ES) č. 45/2001 v tomto nařízení blíže upřesněna. Pokud jde o zpracování osobních údajů Europolem, použije se nařízení (EU) 2016/794 o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva[53] (nařízení o Europolu).

---

49 Rámcové rozhodnutí Rady 2002/475/SVV ze dne 13. června 2002 o boji proti terorismu (Úř. věst. L 164, 22.6.2002, s. 3).

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

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

52 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).

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, 25.5.2016, s. 53).

(29) 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.

(30) Členské státy i agentura by měly udržovat bezpečnostní plány s cílem usnadnit provádění bezpečnostních povinností a měly by vzájemně spolupracovat s cílem společně řešit bezpečnostní otázky.

(31) Nezávislé vnitrostátní orgány dozoru by měly v souvislosti s tímto nařízením sledovat zákonnost zpracování osobních údajů členskými státy. Je třeba stanovit práva subjektů údajů na přístup k jejich údajům uchovávaným v SIS a na jejich opravu a výmaz, jakož i následné opravné prostředky u vnitrostátních soudů a vzájemné uznávání rozsudků. Proto je vhodné požadovat od členských států roční statistiky.

(32) Orgány dozoru by měly zajistit, aby alespoň každým čtvrtým rokem byl v souladu s mezinárodními auditorskými standardy proveden audit činností zpracování údajů v N.SIS. Audit by měly provádět orgány dozoru, nebo by si jej vnitrostátní orgány dozoru měly přímo vyžádat od nezávislého auditora pro ochranu údajů. Nezávislý auditor by měl podléhat kontrole a odpovědnosti vnitrostátního orgánu či orgánů dozoru, které by proto měly nařídit audit jako takový a uvést jasně vymezený účel, rozsah a metodiku auditu, jakož i poskytnout vedení a dohled nad auditem a jeho konečnými výsledky.

(33) Nařízení (EU) 2016/794 (nařízení o Europolu) stanoví, že Europol podporuje a posiluje činnost příslušných orgánů členských států, jakož i jejich vzájemnou spolupráci při boji proti terorismu a závažné trestné činnosti a poskytuje analýzy a posouzení hrozeb. Aby mohl Europol plnit své úkoly, zejména v rámci Evropského střediska pro boj proti převaděčství, je vhodné poskytnout této agentuře přístup ke kategoriím záznamů vymezeným v tomto nařízení. Evropské středisko pro boj proti převaděčství, zřízené při Europolu, hraje důležitou strategickou úlohu v boji proti zprostředkovávání nelegální migrace a mělo by získat přístup k záznamům o osobách, kterým byl odepřen vstup a pobyt na území členského státu buď z trestních důvodů, nebo kvůli nedodržení podmínek vstupu a pobytu.

(34) Aby byly odstraněny nedostatky ve sdílení informací týkajících se terorismu, zejména zahraničních teroristických bojovníků – kde je sledování jejich pohybu zásadní – měly by členské státy zároveň s vložením záznamu do SIS sdílet s Europolem informace o činnosti související s terorismem a rovněž by s ním měly sdílet pozitivní nálezy a související informace. To by Evropskému centru pro boj proti terorismu, zřízenému při Europolu, umožnilo ověřovat, zda v databázích Europolu nejsou k dispozici další kontextové informace, poskytovat vysoce kvalitní analýzy přispívající k rozbití teroristických sítí a případně předcházet útokům.

(35) Je rovněž nezbytné stanovit jasná pravidla pro Europol týkající se zpracování a stahování údajů SIS s cílem umožnit co nejrozsáhlejší využívání SIS za podmínky dodržování norem týkajících se ochrany údajů stanovených v tomto nařízení a nařízení (EU) 2016/794. V případech, kdy vyhledávání provedená Europolem v SIS odhalí existenci záznamu pořízeného členským státem, nemůže Europol přijmout požadované opatření. Měl by proto uvědomit dotčený členský stát, aby tento členský stát mohl na případu dále pracovat.

(36) Nařízení Evropského parlamentu a Rady (EU) 2016/1624[54] stanoví pro účely tohoto nařízení, že hostitelský členský stát zmocní příslušníky jednotek Evropské pohraniční a pobřežní stráže nebo týmy pracovníků, kteří se podílejí na úkolech spojených s navracením, vyslané Evropskou agenturou pro pohraniční a pobřežní stráž k tomu, aby mohli nahlížet do evropských databází, je-li to nezbytné pro plnění operačních cílů uvedených v operačním plánu pro hraniční kontrolu, ostrahu hranic a navracení. Další relevantní agentury Unie, zejména Evropský podpůrný úřad pro otázky azylu a Europol, mohou také v rámci podpůrných týmů pro řízení migrace vysílat odborníky, kteří nejsou pracovníky těchto agentur Unie. Cílem vyslání jednotek Evropské pohraniční a pobřežní stráže, týmů pracovníků, kteří se podílejí na úkolech spojených s navracením, a podpůrných týmů pro řízení migrace je poskytnout technickou a operativní posilu žádajícím členským státům, zejména těm, které čelí nepřiměřeným migračním výzvám. Plnění úkolů přidělených jednotkám Evropské pohraniční a pobřežní stráže, týmům pracovníků, kteří se podílejí na úkolech spojených s navracením, a podpůrným týmům pro řízení migrace vyžaduje přístup do SIS prostřednictvím technického rozhraní Evropské agentury pro pohraniční a pobřežní stráž napojeného na centrální SIS. V případech, kdy vyhledávání provedená jednotkou nebo týmy pracovníků v SIS odhalí existenci záznamu pořízeného členským státem, nemůže příslušník jednotky ani pracovník přijmout požadované opatření, ledaže to povolí hostitelský členský stát. Měl by proto uvědomit dotčené členské státy, aby mohly být podniknuty další kroky.

(37) V souladu s nařízením (EU) 2016/1624 Evropská agentura pro pohraniční a pobřežní stráž připravuje analýzy rizik. Tyto analýzy rizik zahrnují všechny aspekty důležité pro evropskou integrovanou správu hranic, především hrozby, které mohou ovlivnit fungování či bezpečnost vnějších hranic. Záznamy vložené do SIS podle tohoto nařízení, zejména záznamy o odepření vstupu a pobytu, jsou relevantní informace z hlediska posuzování možných hrozeb, které mohou ovlivnit vnější hranice, a tudíž by měly být k dispozici za účelem analýzy rizik, které musí Evropská agentura pro pohraniční a pobřežní stráž připravovat. Plnění úkolů svěřených Evropské agentuře pro pohraniční a pobřežní stráž v souvislosti s analýzou rizik vyžaduje přístup do SIS. Podle návrhu nařízení Evropského parlamentu a Rady, kterým se zřizuje evropský systém pro cestovní informace a povolení (ETIAS)[55], předloženého Komisí, bude navíc ústřední jednotka ETIAS v rámci Evropské agentury pro pohraniční a pobřežní stráž provádět v SIS prostřednictvím systému ETIAS ověřování za účelem posouzení žádostí o cestovní povolení, které mimo jiné vyžaduje zjistit, zda státní příslušník třetí země, který žádá o cestovní povolení, není předmětem záznamu v SIS. Za tímto účelem by ústřední jednotka ETIAS v rámci Evropské agentury pro pohraniční a pobřežní stráž také měla mít v rozsahu nezbytném pro plnění svého mandátu přístup do SIS, a to zejména ke všem kategoriím záznamů o státních příslušnících třetích zemí, v souvislosti s nimiž byl pořízen záznam pro účely vstupu a pobytu a na které se vztahují omezující opatření mající zabránit jejich vstupu na území členských států nebo průjezdu přes toto území.

---

54 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 o 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).

55 COM (2016) 731 final.

(38) Z důvodu jejich technické podstaty, podrobného charakteru a potřeby pravidelné aktualizace nelze některé aspekty SIS upravit vyčerpávajícím způsobem ustanoveními tohoto nařízení. Jedná se například o technická pravidla pro vkládání údajů, aktualizace, výmaz a vyhledávání údajů, kvalitu údajů, pravidla vyhledávání týkající se biometrických identifikátorů, pravidla týkající se slučitelnosti a priority záznamů, přidávání označení, odkazy mezi záznamy, stanovení konce platnosti záznamů v rámci maximální lhůty a o výměnu doplňujících informací. Prováděcí pravomoci, pokud jde o tyto aspekty, by proto měly být svěřeny Komisi. Technická pravidla týkající se vyhledávání v záznamech by měla zohledňovat řádné fungování vnitrostátních aplikací.

(39) Za účelem zajištění jednotných podmínek k provedení tohoto nařízení by měly být Komisi svěřeny prováděcí pravomoci. Tyto pravomoci by měly být vykonávány v souladu s nařízením (EU) č. 182/2011[56]. Postup pro přijímání prováděcích opatření podle tohoto nařízení a nařízení (EU) 2018/xxx (policejní a justiční spolupráce) by měl být totožný.

(40) Za účelem zajištění transparentnosti by měla agentura každé dva roky vypracovat zprávu o technickém fungování centrálního SIS a komunikační infrastruktuře, včetně jejího zabezpečení, a o výměně doplňujících informací. Každé čtyři roky by měla Komise předložit celkové vyhodnocení.

(41) Jelikož cílů tohoto nařízení, totiž vytvoření a právní úpravy společného informačního systému a výměny souvisejících doplňujících informací, nemůže být vzhledem k jejich podstatě uspokojivě dosaženo na úrovni členských států, a proto jich může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity, stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení těchto cílů.

(42) Toto nařízení ctí základní práva a zachovává zásady uznané zejména v Listině základních práv Evropské unie. Cílem tohoto nařízení je především zajistit bezpečné prostředí pro všechny osoby žijící na území Evropské unie a ochranu nelegálních migrantů před vykořisťováním a obchodováním s lidmi tím, že umožní určení jejich totožnosti při plném dodržování ochrany osobních údajů.

(43) V souladu s články 1 a 2 Protokolu č. 22 o postavení Dánska, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, se Dánsko neúčastní přijímání tohoto nařízení a toto nařízení pro ně není závazné ani použitelné. Vzhledem k tomu, že toto nařízení navazuje na schengenské *acquis*, rozhodne se Dánsko v souladu s článkem 4 uvedeného protokolu do šesti měsíců ode dne přijetí tohoto nařízení Radou, zda je provede ve svém vnitrostátním právu.

(44) Toto nařízení rozvíjí ta ustanovení schengenského *acquis*, kterých se neúčastní Spojené království v souladu s rozhodnutím Rady 2000/365/ES[57]; Spojené království se tedy nepodílí na jeho přijímání a toto nařízení pro ně není závazné ani použitelné.

---

[56] 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).

[57] Úř. věst. L 131, 1.6.2000, s. 43.

(45) Toto nařízení rozvíjí ta ustanovení schengenského *acquis*, kterých se neúčastní Irsko v souladu s rozhodnutím Rady 2002/192/ES[58]; Irsko se tedy nepodílí na jeho přijímání a toto nařízení pro ně není závazné ani použitelné.

(46) Pokud jde o Island a Norsko, rozvíjí toto nařízení ta ustanovení schengenského *acquis* ve smyslu Dohody uzavřené mezi Radou Evropské unie a Islandskou republikou a Norským královstvím o přidružení těchto dvou států k provádění, uplatňování a rozvoji schengenského *acquis*[59], která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí Rady 1999/437/ES[60] o některých opatřeních pro uplatňování dané dohody.

(47) Pokud jde o Švýcarsko, rozvíjí toto nařízení ta ustanovení schengenského *acquis* ve smyslu dohody podepsané mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis*, která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí 1999/437/ES ve spojení s čl. 4 odst. 1 rozhodnutí Rady 2004/849/ES[61] a rozhodnutí Rady 2004/860/ES[62].

(48) Pokud jde o Lichtenštejnsko, rozvíjí toto rozhodnutí ta ustanovení schengenského *acquis* ve smyslu Protokolu mezi Evropskou unií, Evropským společenstvím, Švýcarskou konfederací a Lichtenštejnským knížectvím o přistoupení Lichtenštejnského knížectví k Dohodě mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis*[63], která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí 1999/437/ES ve spojení s článkem 3 rozhodnutí Rady 2011/349/EU[64] a článkem 3 rozhodnutí Rady 2011/350/EU[65].

(49) Pokud jde o Bulharsko a Rumunsko, představuje toto nařízení akt navazující na schengenské *acquis* nebo s ním jinak související ve smyslu čl. 4 odst. 2 aktu o přistoupení z roku 2005 a je třeba jej vykládat v spojení s rozhodnutím Rady

---

58 Úř. věst. L 64, 7.3.2002, s. 20.

59 Úř. věst. L 176, 10.7.1999, s. 36.

60 Úř. věst. L 176, 10.7.1999, s. 31.

61 Rozhodnutí Rady 2004/849/ES ze dne 25. října 2004 o podpisu Dohody mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis* jménem Evropské unie a o prozatímním provádění některých jejích ustanovení (Úř. věst. L 368, 15.12.2004, s. 26).

62 Rozhodnutí Rady 2004/860/ES ze dne 25. října 2004 o podpisu Dohody mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis* jménem Evropského společenství a o prozatímním provádění některých jejích ustanovení (Úř. věst. L 370, 17.12.2004, s. 78).

63 Úř. věst. L 160, 18.6.2011, s. 21.

64 Rozhodnutí Rady 2011/349/EU ze dne 7. března 2011 o uzavření Protokolu mezi Evropskou unií, Evropským společenstvím, Švýcarskou konfederací a Lichtenštejnským knížectvím o přistoupení Lichtenštejnského knížectví k dohodě mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis* jménem Evropské unie, zejména pokud jde o justiční spolupráci v trestních věcech a policejní spolupráci (Úř. věst. L 160, 18.6.2011, s. 1).

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

2010/365/EU o uplatňování ustanovení schengenského *acquis* týkajících se Schengenského informačního systému v Bulharské republice a Rumunsku[66].

(50) Pokud jde o Kypr a Chorvatsko, představuje toto nařízení akt navazující na schengenské *acquis* nebo s ním jinak související ve smyslu čl. 3 odst. 2 aktu o přistoupení z roku 2003 a čl. 4 odst. 2 aktu o přistoupení z roku 2011.

(51) Odhadované náklady na modernizaci vnitrostátních systémů SIS a na vytvoření nových funkcí stanovené v tomto nařízení jsou nižší než zbývající částka v rozpočtové položce pro inteligentní hranice stanovené v nařízení Evropského parlamentu a Rady (EU) č. 515/2014[67]. Tímto nařízením by tudíž měla být přerozdělena částka přidělená na vývoj systémů informačních technologií na podporu řízení migračních toků přes vnější hranice Unie podle čl. 5 odst. 5 písm. b) nařízení (EU) č. 515/2014.

(52) Nařízení (ES) č. 1987/2006 by proto mělo být zrušeno.

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

[66] Úř. věst. L 166, 1.7.2010, s. 17.

[67] 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 (Úř. věst. L 150, 20.5.2014, s. 143).

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1
Obecný účel SIS

Účelem SIS je zajistit vysokou úroveň bezpečnosti v prostoru svobody, bezpečnosti a práva Unie, včetně udržování veřejné bezpečnosti a veřejného pořádku a zajišťování bezpečnosti na území členských států, a uplatňovat ustanovení části třetí hlavy V kapitoly 2 Smlouvy o fungování Evropské unie, pokud jde o pohyb osob na jejich územích, s využitím informací předávaných prostřednictvím tohoto systému.

Článek 2
Oblast působnosti

1. Toto nařízení zavádí podmínky a postupy pro vkládání a zpracovávání záznamů v SIS o státních příslušnících třetích zemí a pro výměnu doplňujících informací a dalších údajů za účelem odepření vstupu nebo pobytu na území členských států.

2. Toto nařízení též stanoví pravidla o technické architektuře SIS, o povinnostech členských států a Evropské agentury pro provozní řízení rozsáhlých informačních systémů v rámci prostoru svobody, bezpečnosti a práva, o obecném zpracování údajů, o právech dotčených osob a o zákonné odpovědnosti.

Článek 3
Definice

1. Pro účely tohoto nařízení se rozumí:

   (a) „záznamem“ soubor údajů, včetně biometrických identifikátorů uvedených v článku 22, vložených do SIS umožňující příslušným orgánům identifikovat osobu za účelem přijetí konkrétního opatření;

   (b) „doplňujícími informacemi“ informace, které nejsou součástí údajů v záznamech uložených v SIS, ale souvisejí se záznamy SIS, a které se vyměňují:

      (1) s cílem umožnit členským státům vzájemné poskytování konzultací či informací při vkládání záznamu;

      (2) po pozitivním nálezu, aby se umožnilo přijetí vhodného opatření;

      (3) pokud nelze požadované opatření přijmout;

      (4) pokud se jedná o kvalitu údajů SIS;

      (5) pokud se jedná o slučitelnost a prioritu záznamů;

      (6) pokud se jedná o práva přístupu;

   (c) „dalšími údaji“ údaje uložené v SIS a související se záznamy SIS, které jsou okamžitě k dispozici příslušným orgánům, pokud jsou na základě vyhledávání v tomto systému nalezeny osoby, jejichž údaje byly vloženy do SIS;

(d) „státním příslušníkem třetí země“ každá osoba, která není občanem Unie ve smyslu článku 20 Smlouvy o fungování Evropské unie, s výjimkou osob, které na základě dohod mezi Unií nebo dohod mezi Unií a jejími členskými státy na jedné straně a třetími zeměmi na straně druhé požívají práva volného pohybu rovnocenného právu občanů Unie;

(e) „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjektu údajů“);

(f) „identifikovatelnou fyzickou osobou“ osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor, nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

(g) „zpracováním osobních údajů“ jakýkoli úkon nebo soubor úkonů, které jsou prováděny s osobními údaji pomocí automatizovaných postupů nebo bez nich, jako je shromažďování, protokolování, uspořádávání, strukturování, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, nahlížení, používání, sdělování prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

(h) „pozitivním nálezem“ v SIS:

(1) uživatel provádí vyhledávání;

(2) vyhledávání odhalí, že jiný členský stát vložil do SIS záznam;

(3) údaje v záznamu v SIS se shodují s údaji použitými pro vyhledávání a

(4) v důsledku pozitivního nálezu se vyžadují další opatření.

(i) „pořizujícím členským státem“ členský stát, který vložil záznam do SIS;

(j) „vykonávajícím členským státem“ členský stát, který po pozitivním nálezu přijímá vhodná opatření;

(k) „koncovými uživateli“ příslušné orgány přímo vyhledávající v CS-SIS, N.SIS nebo v jejich technické kopii;

(l) „navrácením“ navrácení ve smyslu čl. 3 bodu 3 směrnice 2008/115/ES;

(m) „zákazem vstupu“ zákaz vstupu ve smyslu čl. 3 bodu 6 směrnice 2008/115/ES;

(n) „daktyloskopickými údaji“ údaje o otiscích prstů a otiscích dlaní, které vzhledem ke své jedinečné povaze a charakteristickým znakům umožňují přesné a průkazné srovnání pro účely určení totožnosti osoby;

(o) „závažnou trestnou činností“ trestné činy uvedené v čl. 2 odst. 1 a 2 rámcového rozhodnutí 2002/584/SVV ze dne 13. června 2002[68];

(p) „teroristickými trestnými činy“ trestné činy podle vnitrostátního práva uvedené v článcích 1 až 4 rámcového rozhodnutí 2002/475/SVV ze dne 13. června 2002[69].

---

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

[69] Rámcové rozhodnutí Rady 2002/475/SVV ze dne 13. června 2002 o boji proti terorismu (Úř. věst. L 164, 22.6.2002, s. 3).

Článek 4
Technická architektura a způsoby provozování SIS

1. Schengenský informační systém (SIS) sestává z:

   (a) centrálního systému (dále jen „centrální SIS“) sestávajícího z:

   – technické podpůrné funkce (dále jen „CS-SIS“) obsahující databázi, dále jen „databáze SIS“,

   – jednotného vnitrostátního rozhraní (dále jen „NI-SIS“);

   (b) vnitrostátního systému (dále jen „N.SIS“) v každém členském státě, sestávajícího z vnitrostátních datových systémů, které komunikují s centrálním SIS. Vnitrostátní systém N.SIS obsahuje soubor údajů (dále jen „vnitrostátní kopie“) obsahující úplnou nebo částečnou kopii databáze SIS, jakož i záložní N.SIS; N.SIS a jeho záloha mohou být používány současně, aby byla zajištěna nepřetržitá dostupnost systému pro koncové uživatele;

   (c) komunikační infrastruktury mezi CS-SIS a NI-SIS (dále jen „komunikační infrastruktura“), která poskytuje šifrovanou virtuální síť vyhrazenou pro údaje SIS a výměnu údajů mezi centrálami SIRENE podle čl. 7 odst. 2.

2. Údaje SIS se vkládají, aktualizují, vymazávají a vyhledávají prostřednictvím různých systémů N.SIS. Částečná nebo úplná vnitrostátní kopie je k dispozici za účelem automatizovaného vyhledávání na území každého členského státu, jenž takovou kopii používá. Částečná vnitrostátní kopie obsahuje alespoň údaje uvedené v čl. 20 odst. 2 písm. a) až v) tohoto nařízení. Vyhledávání v souborech údajů N.SIS jiných členských států není umožněno.

3. CS-SIS vykonává funkce technického dohledu a správy, přičemž je jištěn záložním systémem CS-SIS, který je schopen převzít všechny funkce hlavního systému CS-SIS v případě jeho selhání. CS-SIS a záložní CS-SIS jsou umístěny ve dvou technických zařízeních Evropské agentury pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva, zřízené nařízením (EU) č. 1077/2011[70] (dále jen „agentura“). CS-SIS nebo záložní CS-SIS mohou obsahovat další kopii databáze SIS a mohou být používány současně v aktivním provozu, pokud je každý z nich schopen zpracovávat veškeré transakce týkající se záznamů v SIS.

4. Technická podpůrná funkce CS-SIS poskytuje služby nezbytné pro vložení a zpracování údajů SIS, včetně vyhledávání v databázi SIS. CS-SIS zajišťuje:

   (a) on-line aktualizaci vnitrostátních kopií;

   (b) synchronizaci a soulad mezi vnitrostátními kopiemi a databází SIS;

   (c) počáteční nastavení a opětovné zavedení vnitrostátních kopií;

   (d) nepřetržitou dostupnost.

[70] Agentura byla zřízena nařízením Evropského parlamentu a Rady (EU) č. 1077/2011 ze dne 25. října 2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (Úř. věst. L 286, 1.11.2011, s. 1).

Článek 5
Náklady

1. Náklady na provoz, údržbu a další rozvoj centrálního SIS a komunikační infrastruktury se hradí ze souhrnného rozpočtu Evropské unie.

2. Tyto náklady zahrnují práci vykonávanou v souvislosti s CS-SIS, která zajišťuje poskytování služeb uvedených v čl. 4 odst. 4.

3. Náklady na zřízení, provoz a údržbu a další rozvoj jednotlivých N.SIS nese dotyčný členský stát.

KAPITOLA II

POVINNOSTI ČLENSKÝCH STÁTŮ

Článek 6
Vnitrostátní systémy

Každý členský stát je povinen zřídit, provozovat, udržovat a dále rozvíjet svůj N.SIS a připojit svůj N.SIS k NI-SIS.

Každý členský stát je odpovědný za zajištění nepřetržitého provozu N.SIS, jeho připojení k NI-SIS a za nepřetržitou dostupnost údajů SIS pro koncové uživatele.

Článek 7
Úřad N.SIS a centrála SIRENE

1. Každý členský stát určí orgán (dále jen „úřad N.SIS“), jenž ponese hlavní odpovědnost za jeho N.SIS.

   Tento orgán je odpovědný za plynulý provoz a zabezpečení N.SIS, zajišťuje přístup příslušných orgánů k SIS a přijímá nezbytná opatření pro dodržování ustanovení tohoto nařízení. Je odpovědný za zajištění toho, že veškeré funkce SIS jsou odpovídajícím způsobem zpřístupněny koncovým uživatelům.

   Každý členský stát předává své záznamy prostřednictvím úřadu N.SIS.

2. Každý členský stát určí centrálu, která zajistí výměnu a dostupnost veškerých doplňujících informací (dále jen „centrála SIRENE“), v souladu s ustanoveními příručky SIRENE, jak je uvedeno v článku 8.

   Tyto centrály též koordinují ověřování kvality informací vkládaných do SIS. Pro tyto účely mají přístup k údajům zpracovávaným v SIS.

3. Členské státy uvědomí agenturu o svém úřadu N.SIS II a o své centrále SIRENE. Agentura zveřejní jejich seznam spolu se seznamem uvedeným v čl. 36 odst. 8.

Článek 8
Výměna doplňujících informací

1. Doplňující informace se vyměňují v souladu s ustanoveními příručky SIRENE a prostřednictvím komunikační infrastruktury. Členské státy poskytnou nezbytné technické a personální zdroje pro zajištění nepřetržité dostupnosti a výměny doplňujících informací. V případě, že komunikační infrastruktura není dostupná,

členské státy mohou k výměně doplňujících informací použít jiné náležitě zabezpečené technické prostředky.

2. Doplňující informace se použijí v souladu s článkem 43 pouze pro účely, pro které byly předány, ledaže by byl získán předchozí souhlas pořizujícího členského státu.

3. Centrály SIRENE plní své úkoly rychlým a účinným způsobem, zejména co nejrychleji, nejpozději však do 12 hodin od jejího obdržení, odpovídají na žádost.

4. Podrobná pravidla pro výměnu doplňujících informací se přijímají prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 55 odst. 2, a to formou příručky nazvané „Příručka SIRENE“.

Článek 9
Technický a funkční soulad

1. K zajištění okamžitého a účinného přenosu údajů dodržuje každý členský stát při zřizování svého N.SIS společné normy, protokoly a technické postupy stanovené pro zajištění souladu mezi N-SIS a CS-SIS. Tyto společné normy, protokoly a technické postupy se stanoví a vypracují prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 55 odst. 2.

2. Členské státy zajistí prostřednictvím služeb, které poskytuje CS-SIS, aby údaje uložené ve vnitrostátní kopii byly prostřednictvím automatické aktualizace podle čl. 4 odst. 4 totožné a shodné s databází SIS a aby vyhledávání v jeho vnitrostátní kopii poskytovalo rovnocenný výsledek jako vyhledávání v databázi SIS. Koncoví uživatelé obdrží údaje nezbytné pro plnění jejich úkolů, zejména veškeré údaje potřebné k určení totožnosti subjektu údajů a přijetí požadovaného opatření.

Článek 10
Bezpečnost – členské státy

1. Každý členský stát přijme, ve vztahu ke svému N.SIS, nezbytná opatření, včetně bezpečnostního plánu, plánu kontinuity provozu a plánu pro obnovení provozu po havárii, aby:

   (a) údaje fyzicky chránil, mimo jiné vypracováním plánů pro mimořádné situace pro ochranu kritické infrastruktury;

   (b) zabránil neoprávněným osobám v přístupu k zařízení na zpracování údajů využívanému pro zpracování osobních údajů (kontrola přístupu k zařízení);

   (c) zabránil neoprávněnému čtení, kopírování, pozměňování nebo odstraňování nosičů údajů (kontrola nosičů údajů);

   (d) zabránil neoprávněnému vkládání údajů a neoprávněnému prohlížení, pozměňování či výmazu uložených osobních údajů (kontrola uchovávání);

   (e) zabránil neoprávněným osobám v užívání automatizovaných systémů zpracování údajů pomocí zařízení pro přenos údajů (kontrola uživatelů);

   (f) zajistil, aby osoby oprávněné k využívání automatizovaného systému zpracování údajů měly přístup pouze k údajům, na které se vztahuje jejich oprávnění k přístupu, a pouze s pomocí individuálních a jedinečných totožností uživatele a chráněných režimů přístupu k informacím (kontrola přístupu k údajům);

(g) zajistil, aby všechny orgány s oprávněním přístupu do SIS nebo k zařízením pro zpracování údajů vytvořily profily popisující funkce a povinnosti osob, jež jsou oprávněny k údajům přistupovat a údaje zadávat, aktualizovat, mazat a vyhledávat, a aby tyto profily bezodkladně na základě žádosti zpřístupnily vnitrostátním orgánům dozoru uvedeným v čl. 50 odst. 1 (profily pracovníků);

(h) zajistil, aby bylo možné ověřit a zjistit, kterým orgánům se mohou osobní údaje předávat prostřednictvím zařízení pro přenos údajů (kontrola předávání);

(i) zajistil, aby bylo možné dodatečně ověřit a zjistit, které osobní údaje byly vloženy do automatizovaných systémů zpracování údajů, a kdo, kdy a za jakým účelem je vložil (kontrola vkládání);

(j) zabránil neoprávněnému čtení, kopírování, pozměňování nebo výmazu osobních údajů během přenosů osobních údajů nebo přepravy nosičů dat, zejména prostřednictvím vhodných technik šifrování (kontrola přepravy);

(k) sledoval účinnost bezpečnostních opatření uvedených v tomto odstavci a přijal nezbytná organizační opatření související s interním sledováním (interní kontrola).

2. Členské státy přijmou opatření rovnocenná opatřením uvedeným v odstavci 1, pokud jde o zabezpečení v souvislosti se zpracováním a výměnou doplňujících informací, včetně zabezpečení prostor centrály SIRENE.

3. Členské státy přijmou opatření rovnocenná opatřením uvedeným v odstavci 1, pokud jde o bezpečnost v souvislosti se zpracováním údajů SIS orgány uvedenými v článku 29.

Článek 11
Důvěrnost – členské státy

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

Článek 12
Vedení protokolů na vnitrostátní úrovni

1. Členské státy zajistí, aby každý přístup k osobním údajům v CS-SIS a všechny výměny osobních údajů s CS-SIS byly zaprotokolovány v jejich N.SIS za účelem kontroly, zda je vyhledávání zákonné, či nikoli, za účelem sledování zákonnosti zpracování údajů, pro vlastní kontrolu, pro zajištění řádného fungování N.SIS, neporušenosti údajů a jejich zabezpečení.

2. Protokoly obsahují zejména historii záznamu, datum a čas zpracování údajů, druh údajů použitých pro provedení vyhledávání; odkaz na druh předávaných údajů a jak název příslušného orgánu, tak jméno osoby odpovědné za zpracování údajů.

3. Pokud je vyhledávání provedeno pomocí daktyloskopických údajů nebo zobrazení obličeje v souladu s článkem 22, obsahují protokoly zejména druh údajů použitých pro provedení vyhledávání, odkaz na druh předávaných údajů a jak název příslušného orgánu, tak jméno osoby odpovědné za zpracování údajů.

4. Protokoly lze použít pouze k účelu uvedenému v odstavci 1 a vymažou se nejdříve po uplynutí jednoho roku a nejpozději po třech letech od jejich vytvoření.

5. Protokoly lze uchovat déle, jsou-li potřebné pro postupy kontroly, které již započaly.

6. Příslušné vnitrostátní orgány pověřené kontrolou, zda je vyhledávání zákonné, či nikoli, sledováním zákonnosti zpracování údajů, vlastní kontrolou a zajištěním řádného fungování N.SIS, neporušenosti údajů a jejich zabezpečení mají v rozsahu své pravomoci a na základě žádosti k těmto protokolům přístup, aby mohly plnit své úkoly.

Článek 13
Vlastní kontrola

Členské státy zajistí, aby každý orgán s oprávněním k přístupu k údajům SIS učinil opatření nezbytná k zajištění dodržování tohoto nařízení a spolupracoval, je-li to nutné, s vnitrostátním orgánem dozoru.

Článek 14
Odborná příprava zaměstnanců

Dříve než zaměstnanci orgánů s právem přístupu do SIS obdrží povolení zpracovávat údaje uložené v SIS a pravidelně poté, co jim byl přístup do SIS udělen, absolvují odpovídající odbornou přípravu týkající se zabezpečení údajů, pravidel o ochraně údajů a postupů pro zpracování údajů uvedených v příručce SIRENE. Zaměstnanci jsou informováni o jakýchkoliv příslušných trestných činech a sankcích.

KAPITOLA III

POVINNOSTI AGENTURY

Článek 15
Provozní řízení

1. Za provozní řízení centrálního SIS odpovídá agentura. Agentura ve spolupráci s členskými státy zajistí, aby se pro centrální SIS vždy využívaly nejlepší dostupné technologie určené na základě analýzy nákladů a přínosů.

2. Agentura odpovídá rovněž za následující úkoly týkající se komunikační infrastruktury:

   (a) dohled;

   (b) zabezpečení;

   (c) koordinaci vztahů mezi členskými státy a poskytovatelem.

3. Komise odpovídá za všechny ostatní úkoly spojené s komunikační infrastrukturou, zejména:

   (a) úkoly související s plněním rozpočtu;

   (b) pořizování a obnovu;

   (c) smluvní záležitosti.

4. Agentura odpovídá též za následující úkoly spojené s centrálami SIRENE a komunikací mezi centrálami SIRENE:

   (a) koordinaci a vedení testování;

   (b) údržbu a aktualizaci technických specifikací pro výměnu doplňujících informací mezi centrálami SIRENE a pro komunikační infrastrukturu a za řízení vlivu technických změn, pokud mají dopad na SIS i na výměnu doplňujících informací mezi centrálami SIRENE.

5. Agentura vytvoří a spravuje mechanismus a postupy pro provádění kontrol kvality údajů v CS-SIS a pravidelně předkládá zprávy členským státům. Agentura pravidelně předkládá Komisi zprávy o zjištěných problémech a o tom, kterých členských států se týkají. Tento mechanismus, postupy a výklad dodržování norem kvality údajů se stanoví a vypracují prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 55 odst. 2.

6. Provozní řízení centrálního SIS sestává ze všech úkolů nezbytných pro zachování funkčnosti centrálního SIS 24 hodiny denně sedm dní v týdnu v souladu s tímto nařízením, zejména z údržby a technického rozvoje nezbytného pro plynulý chod systému. Mezi tyto úkoly patří také testování, které má zajistit, aby centrální SIS a vnitrostátní systémy fungovaly podle technických a funkčních požadavků v souladu s článkem 9 tohoto nařízení.

Článek 16
Bezpečnost

1. Agentura přijme pro centrální SIS a komunikační infrastrukturu nezbytná opatření, včetně bezpečnostního plánu, plánu kontinuity provozu a plánu pro obnovení provozu po havárii, aby:

   (a) údaje fyzicky chránila, mimo jiné vypracováním plánů pro mimořádné situace pro ochranu kritické infrastruktury;

   (b) zabránila neoprávněným osobám v přístupu k zařízení na zpracování údajů využívanému pro zpracování osobních údajů (kontrola přístupu k zařízení);

   (c) zabránila neoprávněnému čtení, kopírování, pozměňování nebo odstraňování nosičů údajů (kontrola nosičů údajů);

   (d) zabránila neoprávněnému vkládání údajů a neoprávněnému prohlížení, pozměňování či výmazu uložených osobních údajů (kontrola uchovávání);

   (e) zabránila neoprávněným osobám v užívání automatizovaných systémů zpracování údajů pomocí zařízení pro přenos údajů (kontrola uživatelů);

   (f) zajistila, aby osoby oprávněné k využívání automatizovaného systému zpracování údajů měly přístup pouze k údajům, na které se vztahuje jejich oprávnění k přístupu, a pouze s pomocí individuálních a jedinečných totožností uživatele a chráněných režimů přístupu k informacím (kontrola přístupu k údajům);

   (g) vytvořila profily popisující funkce a povinnosti osob, jež jsou oprávněny k údajům nebo k zařízením pro zpracování údajů přistupovat, a aby tyto profily na žádost bezodkladně zpřístupnila evropskému inspektorovi ochrany údajů uvedenému v článku 51 (profily pracovníků);

(h) zajistila, aby bylo možné ověřit a zjistit, kterým orgánům se mohou osobní údaje předávat prostřednictvím zařízení pro přenos údajů (kontrola předávání);

(i) zajistila, aby bylo možné dodatečně ověřit a zjistit, které osobní údaje byly vloženy do automatizovaných systémů zpracování údajů, kdy a kým byly vloženy (kontrola vkládání);

(j) zabránila neoprávněnému čtení, kopírování, pozměňování nebo výmazu osobních údajů během přenosů osobních údajů nebo přepravy nosičů dat, zejména prostřednictvím vhodných technik šifrování (kontrola přepravy);

(k) sledovala účinnost bezpečnostních opatření uvedených v tomto odstavci a přijala nezbytná organizační opatření související s interním sledováním pro zajištění souladu s tímto nařízením (interní kontrola).

2. Agentura přijme opatření rovnocenná opatřením uvedeným v odstavci 1, pokud jde o zabezpečení při zpracování a výměně doplňujících informací prostřednictvím komunikační infrastruktury.

Článek 17
Důvěrnost – agentura

1. Aniž je dotčen článek 17 služebního řádu úředníků Evropské unie a pracovního řádu ostatních zaměstnanců Unie, agentura použije odpovídající pravidla služebního tajemství nebo jiné srovnatelné povinnosti zachování důvěrnosti na všechny své zaměstnance, kteří musí pracovat s údaji SIS s použitím norem srovnatelných s normami stanovenými v článku 11 tohoto nařízení. Tato povinnost trvá i poté, co dotyčné osoby opustí svůj úřad nebo zaměstnanecký poměr, nebo poté, co ukončí svou činnost.

2. Agentura přijme opatření rovnocenná opatřením uvedeným v odstavci 1, pokud jde o důvěrnost při výměně doplňujících informací prostřednictvím komunikační infrastruktury.

Článek 18
Vedení protokolů na centrální úrovni

1. Agentura zajistí, aby každý přístup k osobním údajům a všechny výměny osobních údajů v rámci CS-SIS byly zaprotokolovány pro účely uvedené v čl. 12 odst. 1.

2. Protokoly obsahují zejména historii záznamů, datum a čas přenosu údajů, druh údajů použitých pro vyhledávání, odkaz na druh předávaných údajů a název příslušného orgánu odpovědného za zpracování údajů.

3. Pokud je vyhledávání provedeno s pomocí daktyloskopických údajů nebo zobrazení obličeje v souladu s článkem 22 a 28, obsahují protokoly zejména druh údajů použitých pro provedení vyhledávání, odkaz na druh předávaných údajů a název jak příslušného orgánu, tak osoby odpovědné za zpracování údajů.

4. Protokoly lze použít pouze k účelům uvedeným v odstavci 1 a vymažou se nejdříve po uplynutí jednoho roku a nejpozději po třech letech od jejich vytvoření. Protokoly obsahující historii záznamů musí být smazány po uplynutí jednoho roku až tří let od výmazu záznamů.

5. Protokoly lze uchovat déle, jsou-li potřebné pro postupy kontroly, které již započaly.

6. Příslušné orgány pověřené kontrolou, zda je vyhledávání zákonné, či nikoli, sledováním zákonnosti zpracování údajů, vlastní kontrolou a zajištěním řádného fungování CS-SIS, neporušenosti údajů a jejich zabezpečení mají v rozsahu své pravomoci a na základě žádosti k těmto protokolům přístup, aby mohly plnit své úkoly.

KAPITOLA IV

INFORMOVÁNÍ VEŘEJNOSTI

Článek 19
Informační kampaně o SIS

Komise, ve spolupráci s vnitrostátními orgány dozoru a s evropským inspektorem ochrany údajů, pravidelně vede kampaně, které informují veřejnost o účelech SIS, o údajích, které se v něm ukládají, o orgánech, které k němu mají přístup, a o právech subjektů údajů. Členské státy, ve spolupráci se svými vnitrostátními orgány dozoru, navrhnou a provedou nezbytné politiky s cílem obecně informovat své občany o SIS.

KAPITOLA V

ZÁZNAMY POŘÍZENÉ O STÁTNÍCH PŘÍSLUŠNÍCÍCH TŘETÍCH ZEMÍ ZA ÚČELEM ODEPŘENÍ VSTUPU A ZÁKAZU POBYTU

Článek 20
Kategorie údajů

1. Aniž je dotčen čl. 8 odst. 1 nebo ustanovení tohoto nařízení, jež stanoví uchovávání dalších údajů, obsahuje SIS pouze ty kategorie údajů, které dodává každý z členských států a které jsou potřebné pro účely uvedené v článku 24.

2. Informace o osobách, o kterých byl pořízen záznam, obsahují pouze tyto údaje:

   (a) příjmení;

   (b) jméno (jména);

   (c) rodné příjmení (rodná příjmení);

   (d) dříve užívaná jména, případně alias;

   (e) jakékoli zvláštní objektivní a nezměnitelné tělesné znaky;

   (f) místo narození;

   (g) datum narození;

   (h) pohlaví;

   (i) státní příslušnost (příslušnosti);

   (j) zda je dotčená osoba ozbrojená, má sklon k násilí, jde o uprchlou osobu nebo se účastní činnosti uvedené v článcích 1, 2, 3 a 4 rámcového rozhodnutí Rady 2002/475/SVV o boji proti terorismu;

(k) důvod záznamu;

(l) orgán pořizující záznam;

(m) odkaz na rozhodnutí, na jehož základě byl záznam pořízen;

(n) opatření, která je třeba přijmout;

(o) odkaz (odkazy) podle článku 38 na další záznamy pořízené v SIS;

(p) zda je dotčená osoba rodinným příslušníkem občana EU nebo jiné osoby, která požívá práva na volný pohyb, podle článku 25;

(q) zda se rozhodnutí o odepření vstupu zakládá na:

– předchozím odsouzení podle čl. 24 odst. 2 písm. a),

– závažné bezpečnostní hrozbě podle čl. 24 odst. 2 písm. b),

– zákazu vstupu podle čl. 24 odst. 3 nebo

– omezujícím opatření podle článku 27;

(r) druh trestného činu (pro záznamy pořízené podle čl. 24 odst. 2 tohoto nařízení);

(s) kategorie dokladu totožnosti;

(t) země, kde byl doklad totožnosti vydán;

(u) číslo (čísla) dokladu totožnosti;

(v) datum vydání dokladu totožnosti;

(w) fotografie a zobrazení obličeje;

(x) daktyloskopické údaje;

(y) barevná kopie dokladu totožnosti.

3. Technická pravidla pro vkládání, aktualizaci, výmaz a vyhledávání údajů uvedených v odstavci 2 se stanoví a vypracují prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 55 odst. 2.

4. Technická pravidla pro vyhledávání údajů uvedených v odstavci 2 se stanoví a vypracují přezkumným postupem uvedeným v čl. 55 odst. 2. Tato technická pravidla jsou podobná pro vyhledávání v CS-SIS, v národních kopiích a technických kopiích, jak je uvedeno v článku 36, a vycházejí ze společných norem stanovených a vypracovaných prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 55 odst. 2.

Článek 21
Proporcionalita

1. Členský stát před pořízením záznamu a při prodlužování doby platnosti záznamu ověří, zda je daný případ dostatečně přiměřený, relevantní a závažný pro vložení záznamu do SIS.

2. Při uplatňování čl. 24 odst. 2 vytvoří členské státy takový záznam o státním příslušníkovi třetí země za všech okolností, jestliže se jedná o trestný čin spadající do

působnosti článků 1 až 4 rámcového rozhodnutí Rady 2002/475/SVV o boji proti terorismu[71].

Článek 22

Zvláštní pravidla pro vkládání fotografií, zobrazení obličeje a daktyloskopických údajů

1. Údaje uvedené v čl. 20 odst. 2 písm. w) a x) se vloží do SIS pouze po provedení kontroly kvality s cílem zjistit, zda jsou splněny minimální normy kvality údajů.

2. Pro uchovávání údajů uvedených v odstavci 1 se stanoví normy kvality. Specifikace těchto norem se stanoví prostřednictvím prováděcích opatření a aktualizují přezkumným postupem uvedeným v čl. 55 odst. 2.

Článek 23

Požadavek na vložení záznamu

1. Záznam nesmí být vložen bez údajů uvedených v čl. 20 odst. 2 písm. a), g), k), m), n) a q). Jestliže se záznam zakládá na rozhodnutí přijatém podle čl. 24 odst. 2, vloží se rovněž údaje uvedené v čl. 20 odst. 2 písm. r).

2. Dále se vloží všechny další údaje uvedené v čl. 20 odst. 2, jsou-li k dispozici.

Článek 24

Podmínky pořizování záznamů o odepření vstupu a pobytu

1. Údaje týkající se státních příslušníků třetích zemí, o kterých byl pořízen záznam pro účely odepření vstupu a pobytu, se vloží do SIS na základě vnitrostátního záznamu vyplývajícího z rozhodnutí přijatého příslušnými správními nebo justičními orgány v souladu s procesními předpisy, které stanoví vnitrostátní právo, a učiněného pouze na základě posouzení jednotlivých případů. Odvolání proti těmto rozhodnutím se podávají v souladu s vnitrostátním právem.

2. Záznam se vloží, pokud se rozhodnutí uvedené v odstavci 1 zakládalo na tom, že přítomnost státního příslušníka třetí země na území členského státu může představovat ohrožení veřejného pořádku, veřejné bezpečnosti nebo bezpečnosti státu. Tato situace nastane zejména v případě:

   (a) státního příslušníka třetí země, který byl v členském státě odsouzen pro trestný čin, na který se vztahuje trest odnětí svobody ve výši nejméně jednoho roku;

   (b) státního příslušníka třetí země, proti kterému existuje důvodné podezření, že spáchal závažný trestný čin, nebo ohledně kterého existují zjevné náznaky o úmyslu páchat takové trestné činy na území členského státu.

3. Záznam se vloží, pokud rozhodnutí uvedené v odstavci 1 představuje zákaz vstupu vydaný v souladu s řízením v souladu se směrnicí 2008/115/ES. Pořizující členský stát zajistí, že záznam nabude účinku v SIS v okamžiku navrácení dotčeného státního příslušníka třetí země. Potvrzení o navrácení je sděleno pořizujícímu členskému státu v souladu s článkem 6 nařízení (EU) 2018/xxx [nařízení o navracení].

[71] Rámcové rozhodnutí Rady 2002/475/SVV ze dne 13. června 2002 o boji proti terorismu (Úř. věst. L 164, 22.6.2002, s. 3).

Článek 25
Podmínky vkládání záznamů o státních příslušnících třetích zemí, kteří požívají práva na volný pohyb v rámci Unie

1. Záznam týkající se státního příslušníka třetí země, který požívá práva na volný pohyb v Unii ve smyslu směrnice Evropského parlamentu a Rady 2004/38/ES[72], se vloží v souladu s ustanoveními přijatými za účelem provedení uvedené směrnice.

2. V případě pozitivního nálezu záznamu podle článku 24 týkajícího se státního příslušníka třetí země, který požívá práva na volný pohyb v Unii, členský stát, který záznam používá, okamžitě konzultuje prostřednictvím výměny doplňujících informací pořizující členský stát s cílem neprodleně rozhodnout o opatření, které má být přijato.

Článek 26
Postup konzultace

1. Pokud členský stát hodlá vydat povolení k pobytu nebo jiné povolení zakládající oprávnění k pobytu státnímu příslušníku třetí země, na nějž se vztahuje záznam pro účely odepření vstupu a pobytu vložený jiným členským státem, nejprve prostřednictvím výměny doplňujících informací konzultuje s pořizujícím členským státem, přičemž zohlední zájmy tohoto členského státu. Pořizující členský stát poskytne konečnou odpověď do sedmi dnů. Pokud členský stát, který hodlá vydat povolení k pobytu nebo jiné povolení zakládající oprávnění k pobytu, rozhodne o jeho vydání, záznam pro účely odepření vstupu a pobytu se vymaže.

2. Pokud členský stát hodlá vložit záznam pro účely odepření vstupu a pobytu, jenž se vztahuje na státního příslušníka třetí země, který je držitelem platného povolení k pobytu či jiného povolení zakládajícího oprávnění k pobytu vydaného jiným členským státem, nejprve prostřednictvím výměny doplňujících informací konzultuje členský stát, který povolení vydal, přičemž zohlední zájmy tohoto členského státu. Členský stát, který povolení vydal, poskytne konečnou odpověď do sedmi dnů. Pokud členský stát, který povolení vydal, rozhodne o jeho zachování, záznam pro účely odepření vstupu a pobytu se nevloží.

3. V případě pozitivního nálezu záznamu pro účely odepření vstupu a pobytu, jenž se vztahuje na státního příslušníka třetí země, který je držitelem platného povolení k pobytu nebo jiného povolení zakládajícího oprávnění k pobytu, konzultuje vykonávající členský stát prostřednictvím výměny doplňujících informací neprodleně členský stát, který povolení k pobytu vydal, a členský stát, který záznam vložil, aby mohl urychleně rozhodnout, zda je třeba přijmout dané opatření. Pokud je přijato rozhodnutí o zachování povolení k pobytu, záznam se vymaže.

4. Členské státy poskytují agentuře každoročně statistické údaje o konzultacích, které se uskutečnily podle odstavců 1 až 3.

[72] Úř. věst. L 158, 30.4.2004, s. 77.

Článek 27

Podmínky pro pořizování záznamů o státních příslušnících třetích zemí, na které se vztahují omezující opatření

1. Do SIS se za účelem odepření vstupu a zákazu pobytu vkládají záznamy o státních příslušnících třetích zemí, na které se vztahují omezující opatření zaměřená na zamezení vstupu na území členských států nebo tranzitu přes něj, učiněná podle právních aktů přijatých Radou, včetně opatření, kterými se provádí zákaz cestování vydaný Radou bezpečnosti Organizace spojených národů, pokud jsou dodrženy požadavky na kvalitu údajů.

2. Členský stát, který je odpovědný za vkládání, aktualizaci a výmaz těchto údajů jménem všech členských států, se určí v okamžiku přijetí příslušného opatření přijatého podle článku 29 Smlouvy o EU. Postup pro určení tohoto odpovědného členského státu se stanoví a vypracuje prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 55 odst. 2.

KAPITOLA VI

VYHLEDÁVÁNÍ S POUŽITÍM BIOMETRICKÝCH ÚDAJŮ

Článek 28

Zvláštní pravidla pro ověřování nebo vyhledávání s použitím fotografií, zobrazení obličeje a daktyloskopických údajů

1. Fotografie, zobrazení obličeje a daktyloskopické údaje se získávají ze SIS k potvrzení totožnosti osob, které byly nalezeny na základě alfanumerického vyhledávání v SIS.

2. Daktyloskopické údaje lze též použít k určení totožnosti osoby. Daktyloskopické údaje uložené v SIS se použijí pro účely určení totožnosti, jestliže nelze zjistit totožnost osoby jinými prostředky.

3. Jestliže příslušné orgány nemohou zjistit totožnost osoby s využitím jiné vnitrostátní, evropské či mezinárodní databáze, lze daktyloskopické údaje uložené v SIS týkající se záznamů pořízených podle článku 24 vyhledávat též s použitím úplných či neúplných souborů otisků prstů či otisků dlaní zajištěných na místě vyšetřovaného činu, u nichž lze s vysokou mírou pravděpodobnosti stanovit, že patří pachateli trestné činnosti.

4. Fotografie a zobrazení obličeje lze použít k určení totožnosti osoby, jakmile to bude z technického hlediska možné a bude-li zajištěna vysoká míra spolehlivosti určení totožnosti. Určení totožnosti na základě fotografií nebo zobrazení obličeje lze provádět pouze na řádných hraničních přechodech, kde se používají samoobslužné systémy a systémy automatizované hraniční kontroly.

KAPITOLA VII

PRÁVO PŘÍSTUPU K ZÁZNAMŮM A JEJICH UCHOVÁVÁNÍ

Článek 29
Orgány mající právo přístupu k záznamům

1. Přístup k údajům vloženým do SIS a právo v těchto údajích vyhledávat přímo nebo v kopii údajů SIS je vyhrazeno orgánům odpovědným za určení totožnosti státních příslušníků třetích zemí pro:

   (a) ochranu hranic, v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/399 ze dne 9. března 2016, kterým se stanoví kodex Unie o pravidlech upravujících přeshraniční pohyb osob (Schengenský hraniční kodex);

   (b) provádění policejních a celních kontrol v dotyčném členském státě, jakož i pro jejich koordinaci určenými orgány;

   (c) jiné činnosti v oblasti prosazování práva prováděné za účelem prevence, vyšetřování, odhalování trestných činů na území dotčeného členského státu;

   (d) posuzování podmínek a přijímání rozhodnutí týkajících se vstupu a pobytu státních příslušníků třetích zemí na území členských států, včetně povolení k pobytu a dlouhodobých víz, a navracení státních příslušníků třetích zemí;

   (e) posuzování žádostí o víza a přijímání rozhodnutí o těchto žádostech, včetně o prohlášení víza za neplatné nebo jeho zrušení anebo prodloužení jeho platnosti, v souladu s nařízením Evropského parlamentu a Rady (EU) č. 810/2009[73].

2. Pro účely čl. 24 odst. 2 a 3 a článku 27 mohou právo na přístup k údajům vloženým do SIS a právo v těchto údajích přímo vyhledávat při plnění svých úkolů vykonávat i vnitrostátní justiční orgány, včetně těch, které odpovídají za zahájení trestního stíhání a za vyšetřování před podáním obžaloby, jak je stanoveno vnitrostátními právními předpisy, jakož i jejich koordinační orgány.

3. Právo na přístup k údajům týkajícím se osobních dokladů vloženým podle čl. 38 odst. 2 písm. j) a k) nařízení (EU) 2018/xxx [policejní spolupráce a justiční spolupráce v trestních věcech] a právo v těchto údajích vyhledávat mohou též vykonávat orgány uvedené v odst. 1 písm. d). Přístup těchto orgánů k údajům se řídí právem každého členského státu.

4. Orgány uvedené v tomto článku se zahrnou do seznamu uvedeného v čl. 36 odst. 8.

Článek 30
Přístup Europolu k údajům SIS

1. Agentura Evropské unie pro spolupráci v oblasti prosazování práva (Europol) má v rámci svého mandátu právo na přístup k údajům vloženým do SIS a právo v těchto údajích vyhledávat.

[73] Nařízení Evropského parlamentu a Rady (ES) č. 810/2009 ze dne 13. července 2009 o kodexu Společenství o vízech (vízový kodex) (Úř. věst. L 243, 15.9.2009, s. 1).

2. Pokud vyhledávání provedené Europolem odhalí existenci záznamu v SIS, Europol o tom informuje způsobem vymezeným v nařízení (EU) 2016/794 pořizující členský stát.

3. Použití informací získaných vyhledáváním v SIS podléhá souhlasu dotyčného členského státu. Pokud členský stát povolí použití takové informace, Europol s ní nakládá v souladu s nařízením (EU) 2016/794. Europol může takovou informaci sdělit třetím zemím a třetím subjektům pouze se souhlasem dotyčného členského státu.

4. Europol může od dotyčného členského státu požadovat další informace v souladu s ustanoveními nařízení (EU) 2016/794.

5. Europol:

   (a) aniž jsou dotčena ustanovení odstavců 3, 4 a 6, nepropojí části SIS s jakýmkoli počítačovým systémem pro sběr a zpracování údajů provozovaným Europolem nebo na jeho pracovištích, ani do takového systému nepřenese údaje obsažené v SIS, k nimž má přístup, ani nestáhne nebo jinak nezkopíruje jakékoli části SIS;

   (b) omezí přístup k údajům vloženým do SIS na konkrétně oprávněné zaměstnance Europolu;

   (c) přijme a bude uplatňovat opatření stanovená v článcích 10 a 11;

   (d) umožní evropskému inspektorovi ochrany údajů, aby kontroloval činnost Europolu při výkonu jeho práva na přístup k údajům vloženým do SIS a práva v těchto údajích vyhledávat.

6. Kopie údajů se mohou pořizovat pouze pro technické účely, pokud jsou potřebné k tomu, aby pracovníci Europolu vybavení náležitým oprávněním mohli provádět přímé vyhledávání. Na tyto kopie se použijí ustanovení tohoto nařízení. Technická kopie se použije pro účely uchovávání údajů SIS v průběhu vyhledávání údajů. Po dokončení vyhledávání se údaje vymažou. Tato použití nejsou považována za protiprávní stahování nebo kopírování údajů SIS. Europol nesmí kopírovat údaje v záznamech nebo další údaje pořízené členskými státy nebo získané z CS-SIS do jiných systémů Europolu.

7. Kopie podle odstavce 6, které vedou ke vzniku off-line databází, lze uchovávat pouze na dobu nepřesahující 48 hodin. Tato doba může být prodloužena při mimořádné situaci, dokud tato situace neskončí. Europol oznámí každé takové prodloužení evropskému inspektorovi ochrany údajů.

8. Europol může přijímat a zpracovávat doplňující informace k příslušným záznamům SIS, pokud jsou řádně uplatněna pravidla pro zpracování údajů uvedená v odstavcích 2 až 7.

9. Za účelem ověření zákonnosti zpracování údajů, pro vlastní kontrolu a pro zajištění řádného zabezpečení údajů a jejich neporušenosti by měl Europol vést protokoly o každém přístupu do SIS a vyhledávání v tomto systému. Tyto protokoly a dokumentace nejsou považovány za protiprávní stahování nebo kopírování jakékoli části SIS.

Článek 31

Přístup jednotek Evropské pohraniční a pobřežní stráže, týmů pracovníků, kteří se podílejí na úkolech spojených s navracením, a členů podpůrných týmů pro řízení migrace k údajům SIS

1. V souladu s čl. 40 odst. 8 nařízení (EU) 2016/1624 mají příslušníci jednotek Evropské pohraniční a pobřežní stráže nebo týmy pracovníků, kteří se podílejí na úkolech spojených s navracením, a členové podpůrných týmů pro řízení migrace v rámci svého mandátu právo na přístup k údajům vloženým do SIS a právo v těchto údajích vyhledávat.

2. Příslušníci jednotek Evropské pohraniční a pobřežní stráže nebo týmy pracovníků, kteří se podílejí na úkolech spojených s navracením, a členové podpůrných týmů pro řízení migrace mají v souladu s odstavcem 1 přístup k údajům vloženým do SIS a mohou v těchto údajích vyhledávat prostřednictvím technického rozhraní vytvořeného a spravovaného Evropskou agenturou pro pohraniční a pobřežní stráž podle čl. 32 odst. 2.

3. Pokud vyhledávání provedené příslušníkem jednotky Evropské pohraniční a pobřežní stráže nebo týmy pracovníků, kteří se podílejí na úkolech spojených s navracením, nebo členem podpůrného týmu pro řízení migrace odhalí existenci záznamu v SIS, je o tom informován pořizující členský stát. V souladu s článkem 40 nařízení (EU) 2016/1624 mohou příslušníci jednotek a členové týmů jednat v reakci na záznam v SIS pouze pod velením a zpravidla za přítomnosti příslušníků pohraniční stráže hostitelského členského státu, v němž působí, nebo pracovníků, kteří se podílejí na úkolech spojených s navracením, tohoto státu. Hostitelský členský stát může příslušníky jednotek zmocnit k tomu, aby jednali jeho jménem.

4. Každý vstup a každé vyhledávání provedené příslušníkem jednotek Evropské pohraniční a pobřežní stráže nebo týmy pracovníků, kteří se podílejí na úkolech spojených s navracením, nebo členy podpůrných týmů pro řízení migrace se zaprotokoluje v souladu s článkem 12 a každé jejich použití údajů, k nimž získali přístup, se zaeviduje.

5. Přístup k údajům vloženým do SIS se omezuje na příslušníky jednotek Evropské pohraniční a pobřežní stráže nebo týmy pracovníků, kteří se podílejí na úkolech spojených s navracením, nebo členy podpůrných týmů pro řízení migrace a nelze jej rozšířit na jiné členy týmů.

6. Za účelem zajištění důvěrnosti a bezpečnosti se přijmou a budou uplatňovat opatření stanovená v článcích 10 a 11.

Článek 32

Přístup Evropské agentury pro pohraniční a pobřežní stráž k údajům SIS

1. Evropská agentura pro pohraniční a pobřežní stráž má za účelem analýzy hrozeb, které mohou ovlivnit fungování či bezpečnost vnějších hranic, právo na přístup k údajům vloženým do SIS a právo v těchto údajích vyhledávat, a to v souladu s články 24 a 27.

2. Pro účely čl. 31 odst. 2 a odstavce 1 tohoto článku Evropská agentura pro pohraniční a pobřežní stráž vytvoří a spravuje technické rozhraní, které umožňuje přímé propojení s centrálním SIS.

3. Pokud vyhledávání provedené Evropskou agenturou pro pohraniční a pobřežní stráž odhalí existenci záznamu v SIS, informuje o tom tato agentura pořizující členský stát.

4. Evropská agentura pro pohraniční a pobřežní stráž má za účelem plnění úkolů, které jí byly svěřeny nařízením, kterým se zřizuje evropský systém pro cestovní informace a povolení (ETIAS), právo na přístup k údajům vloženým do SIS a právo tyto údaje ověřovat, a to v souladu s články 24 a 27.

5. Pokud ověření provedené Evropskou agenturou pro pohraniční a pobřežní stráž pro účely odstavce 2 odhalí existenci záznamu v SIS, použije se postup podle článku 22 nařízení, kterým se zřizuje evropský systém pro cestovní informace a povolení (ETIAS).

6. Žádné ustanovení tohoto článku se nedotýká ustanovení nařízení (EU) 2016/1624 týkajících se ochrany údajů a odpovědnosti za neoprávněné nebo nesprávné zpracování takových údajů Evropskou agenturou pro pohraniční a pobřežní stráž.

7. Každý vstup a každé vyhledávání provedené Evropskou agenturou pro pohraniční a pobřežní stráž se zaprotokoluje v souladu s článkem 12 a každé použití údajů, k nimž Evropská agentura pro pohraniční a pobřežní stráž získala přístup, se zaeviduje.

8. Ledaže by to bylo nezbytné k plnění úkolů pro účely nařízení, kterým se zřizuje evropský systém pro cestovní informace a povolení (ETIAS), se žádné části SIS nepropojí s jakýmkoli počítačovým systémem pro sběr a zpracování údajů provozovaným Evropskou agenturou pro pohraniční a pobřežní stráž nebo na jejích pracovištích ani se do takového systému nepřenesou údaje v SIS obsažené, k nimž má Evropská agentura pro pohraniční a pobřežní stráž přístup. Žádná část SIS se nestáhne. Protokolování přístupu a vyhledávání není považováno za stahování nebo kopírování údajů SIS.

9. Za účelem zajištění důvěrnosti a bezpečnosti se přijmou a budou uplatňovat opatření stanovená v článcích 10 a 11.

Článek 33
Rozsah přístupu

Koncoví uživatelé, včetně Europolu a Evropské agentury pro pohraniční a pobřežní stráž, mají přístup pouze k údajům, které jsou nezbytné k plnění jejich úkolů.

Článek 34
Doba uchovávání záznamů

1. Záznamy vložené do SIS podle tohoto nařízení se uchovávají pouze po dobu nezbytnou pro splnění účelů, pro které byly vloženy.

2. Do pěti let od vložení záznamu do SIS přezkoumá členský stát, jenž záznam pořídil, nutnost jej uchovávat.

3. Každý členský stát ve vhodných případech stanoví kratší doby pro přezkum v souladu se svým vnitrostátním právem.

4. V případech, kdy je pracovníkům centrály SIRENE odpovědným za koordinaci a ověřování kvality údajů zřejmé, že záznam o určité osobě splnil svůj účel a měl být ze SIS vymazán, upozorní pracovníci na uvedenou skutečnost orgán, který záznam vytvořil. Daný orgán má 30 kalendářních dní od obdržení tohoto oznámení, aby

sdělil, zda záznam byl či má být vymazán, nebo uvedl důvody pro uchování záznamu. Pokud tato třicetidenní lhůta uplyne bez odpovědi, pracovníci centrály SIRENE záznam vymažou. Centrály SIRENE hlásí veškeré opakující se problémy v této oblasti svému vnitrostátnímu orgánu dozoru.

5. Členský stát, jenž záznam pořídil, může v době pro přezkum na základě souhrnného individuálního posouzení, které zaznamená, rozhodnout o delším zachování záznamu, je-li to nezbytné pro účely, pro něž byl záznam pořízen. V tomto případě se použije odstavec 2 také na toto delší zachování. Jakékoliv prodloužení záznamu musí být sděleno CS-SIS.

6. Záznamy se automaticky vymazávají po uplynutí doby pro přezkum uvedené v odstavci 2 s výjimkou případu, kdy členský stát, jenž záznam pořídil, informoval CS-SIS o prodloužení záznamu podle odstavce 5. CS-SIS automaticky čtyři měsíce předem uvědomí členské státy o plánovaném výmazu údajů ze systému.

7. Členské státy uchovávají statistiky o počtu záznamů, u nichž byla doba uchovávání prodloužena v souladu s odstavcem 5.

Článek 35
Výmaz záznamů

1. Záznamy o odepření vstupu a pobytu podle článku 24 jsou vymazány, jakmile je rozhodnutí, na jehož základě byl záznam založen, příslušným orgánem odvoláno nebo zrušeno, a to v případě potřeby po postupu konzultace uvedeném v článku 26.

2. Záznamy o státních příslušnících třetích zemí, na které se vztahují omezující opatření podle článku 27, se vymažou, pokud bylo opatření provádějící zákaz cestování ukončeno, pozastaveno nebo zrušeno.

3. Záznamy pořízené o osobě, která získala občanství státu, jehož státní příslušníci požívají práva na volný pohyb v Unii, se vymažou, jakmile je pořizující členský stát, informován podle článku 38 nebo se jinak dozví o tom, že dotyčná osoba získala takovéto občanství.

KAPITOLA VIII

OBECNÁ PRAVIDLA PRO ZPRACOVÁNÍ ÚDAJŮ

Článek 36
Zpracování údajů v SIS

1. Členské státy mohou zpracovávat údaje uvedené v článku 20 za účelem odepření vstupu a pobytu na svých územích.

2. Kopie údajů se mohou pořizovat pouze pro technické účely, pokud jsou potřebné k přímému vyhledávání orgány uvedenými v článku 29. Na tyto kopie se použijí ustanovení tohoto nařízení. Členské státy nesmějí kopírovat údaje v záznamech nebo další údaje pořízené jiným členským státech ze svého N.SIS nebo z CS-SIS do jiných vnitrostátních souborů údajů.

3. Technické kopie podle odstavce 2, které vedou ke vzniku off-line databází, lze uchovávat pouze na dobu nepřesahující 48 hodin. V mimořádných situacích může být tato doba prodloužena až do konce mimořádné situace.

Bez ohledu na první pododstavec nejsou povoleny technické kopie vedoucí ke vzniku off-line databází, které mají být využívány orgány vydávajícími víza, s výjimkou pořízených kopií, které mají být použity pouze při mimořádných situacích v důsledku nedostupnosti sítě po dobu delší než 24 hodin.

Členské státy uchovávají aktuální soupis těchto kopií, zpřístupňují tento soupis svým vnitrostátním orgánům dozoru a zajišťují, že se na tyto kopie použijí ustanovení tohoto nařízení, zejména článku 10.

4. Přístup k takovým údajům se povoluje pouze v mezích pravomoci vnitrostátních orgánů uvedených v článku 29 a pouze pracovníkům vybaveným náležitým oprávněním.

5. Jakékoli zpracování informací uvedených v SIS pro jiné účely než účely, pro které byly do něj vloženy, musí být spojeno s konkrétním případem a odůvodněno nezbytností předcházet bezprostřednímu vážnému ohrožení veřejného pořádku a veřejné bezpečnosti, a to z vážných důvodů národní bezpečnosti nebo s cílem předejít závažné trestné činnosti. Za tím účelem musí být předem získáno povolení členského státu, jenž záznam pořídil.

6. Údaje týkající se osobních dokladů vložené podle čl. 38 odst. 2 písm. j) a k) nařízení (EU) 2018/xxx mohou být používány orgány uvedenými v čl. 29 odst. 1 písm. d) v souladu s právem každého členského státu.

7. Jakékoli využití údajů, které není v souladu s odstavci 1 až 6, je podle práva každého členského státu považováno za zneužití.

8. Každý členský stát zašle agentuře seznam příslušných orgánů, které jsou podle tohoto nařízení oprávněny přímo vyhledávat v údajích obsažených v SIS, a případné změny tohoto seznamu. V tomto seznamu je u každého orgánu uvedeno, v jakých údajích může vyhledávat a za jakými účely. Agentura zajistí každoroční zveřejnění seznamu v *Úředním věstníku Evropské unie*.

9. Neobsahuje-li právo Unie zvláštní ustanovení, použije se pro údaje vložené do N.SIS právo každého příslušného členského státu.

Článek 37
Údaje SIS a vnitrostátní soubory

1. Ustanovením čl. 36 odst. 2 není dotčeno právo členského státu uchovávat ve svých vnitrostátních souborech údaje SIS, ve spojitosti s nimiž bylo učiněno opatření na jeho území. Takové údaje se uchovávají ve vnitrostátních souborech nanejvýš po dobu tří let s výjimkou případů, kdy konkrétní ustanovení vnitrostátního práva upravují delší období uchovávání.

2. Ustanovením čl. 36 odst. 2 není dotčeno právo členského státu uchovávat ve svých vnitrostátních souborech údaje obsažené v konkrétním záznamu, který dotyčný členský stát do SIS vložil.

Článek 38
Informování v případě nepoužití záznamu

Nemohou-li být požadovaná opatření provedena, uvědomí o tom dožádaný členský stát neprodleně členský stát, jenž záznam pořídil.

Článek 39
Kvalita údajů zpracovávaných v SIS

1. Členský stát pořizující záznam odpovídá za zajištění toho, že údaje jsou správné, aktuální a jsou vložené v SIS v souladu se zákonem.

2. Pouze členský stát, jenž záznam pořídil, je oprávněn měnit, doplňovat, opravovat, aktualizovat nebo mazat údaje, které vložil.

3. Má-li některý z členských států, jenž nepořídil záznam, důkazy naznačující, že položka údaje je věcně nesprávná nebo je uchovávána protiprávně, uvědomí o tom co nejdříve a nejpozději do deseti dnů poté, co se o uvedeném důkazu dozvěděl, pořizující členský stát prostřednictvím výměny doplňujících informací. Pořizující členský stát sdělení prověří a v případě potřeby dotyčnou položku neprodleně opraví nebo vymaže.

4. Nemohou-li se členské státy dohodnout ve lhůtě dvou měsíců od okamžiku, kdy se důkazy poprvé objevily, jak je popsáno v odstavci 3, předloží členský stát, jenž nepořídil záznam, věc příslušnému vnitrostátnímu orgánu dozoru k rozhodnutí.

5. Členské státy si vymění doplňující informace v případě, že si dotyčná osoba stěžuje, že není osobou, k níž se má záznam vztahovat. Prokáže-li kontrola, že se skutečně jedná o dvě odlišné osoby, bude osoba, která si stěžuje, informována o ustanoveních uvedených v článku 42.

6. Pokud je určitá osoba již předmětem záznamu v SIS, dohodne se o vložení dalšího záznamu členský stát, který vkládá tento záznam, s členským státem, který vložil první záznam. Dohody je dosaženo na základě výměny doplňujících informací.

Článek 40
Bezpečnostní incidenty

1. Každou událost, která má nebo může mít dopad na bezpečnost SIS a může údajům SIS způsobit škodu nebo újmu, je nutno považovat za bezpečnostní incident, zejména v případě, mohlo-li dojít k přístupu k údajům nebo pokud byla či mohla být ohrožena dostupnost, neporušenost a důvěrnost údajů.

2. Bezpečnostní incidenty se řeší tak, aby byla zajištěna rychlá, účinná a náležitá odezva.

3. Členské státy oznamují bezpečnostní incidenty Komisi, agentuře a evropskému inspektorovi ochrany údajů. Agentura oznamuje bezpečnostní incidenty Komisi a evropskému inspektorovi ochrany údajů.

4. Informace o bezpečnostním incidentu, který má nebo může mít dopad na provoz SIS v členském státě či v rámci agentury, nebo na dostupnost, neporušenost a důvěrnost údajů vložených či zaslaných jinými členskými státy, jsou předány členským státům a nahlášeny v souladu s plánem pro řešení incidentů vypracovaným agenturou.

Článek 41
Rozlišování osob s podobnými znaky

Pokud se při vkládání nového záznamu ukáže, že v SIS již existuje záznam o osobě se stejnými prvky popisu totožnosti, postupuje se takto:

(a) centrála SIRENE kontaktuje žádající orgán s cílem objasnit, zda se záznam týká stejné osoby, či nikoli;

(b) prokáže-li kontrola, že osoba, jež je předmětem nového záznamu, a osoba, o níž již existuje záznam v SIS, je ve skutečnosti tatáž osoba, centrála SIRENE použije postup vkládání vícenásobných záznamů uvedený v čl. 39 odst. 6. Prokáže-li kontrola, že se ve skutečnosti jedná o dvě různé osoby, centrála SIRENE schválí požadavek na vložení dalšího záznamu a to tak, že doplní potřebné prvky, které zabrání jakýmkoli chybným určením totožnosti.

Článek 42
Další údaje pro účely řešení zneužití totožnosti

1. Může-li dojít k záměně mezi osobou, která má být ve skutečnosti předmětem záznamu, a osobou, jejíž totožnost byla zneužita, doplní pořizující členský stát tento záznam o údaje týkající se osoby, jejíž totožnost byla zneužita, za podmínky jejího výslovného souhlasu, aby se předešlo nežádoucím důsledkům chybného určení totožnosti.

2. Údaje týkající se osoby, jejíž totožnost byla zneužita, se použijí pouze pro tyto účely:

   (a) umožnit příslušnému orgánu odlišit osobu, jejíž totožnost byla zneužita, od osoby, jež je ve skutečnosti předmětem záznamu;

   (b) umožnit osobě, jejíž totožnost byla zneužita, prokázat svoji totožnost a dokázat, že její totožnost byla zneužita.

3. Za účelem naplnění tohoto článku lze vložit a dále zpracovávat v SIS pouze tyto osobní údaje:

   (a) příjmení;

   (b) jméno (jména);

   (c) rodné příjmení (rodná příjmení);

   (d) dříve užívaná jména, případně alias, která mohou být vedena zvlášť;

   (e) jakékoli zvláštní objektivní a nezměnitelné tělesné znaky;

   (f) místo narození;

   (g) datum narození;

   (h) pohlaví;

   (i) zobrazení obličeje;

   (j) otisky prstů;

   (k) státní příslušnost (příslušnosti);

   (l) kategorie dokladu totožnosti;

   (m) země, kde byl doklad totožnosti vydán;

   (n) číslo (čísla) dokladu totožnosti;

   (o) datum vydání dokladu totožnosti;

   (p) adresa poškozené osoby;

   (q) jméno otce poškozené osoby;

   (r) jméno matky poškozené osoby.

4. Technická pravidla potřebná pro vkládání a další zpracování údajů uvedených v odstavci 3 se zavedou prostřednictvím prováděcích opatření stanovených a vypracovaných přezkumným postupem podle čl. 55 odst. 2.

5. Údaje uvedené v odstavci 3 se vymažou současně s odpovídajícím záznamem nebo dříve, pokud o to osoba požádá.

6. K údajům uvedeným v odstavci 3 mohou přistupovat pouze orgány mající právo přístupu k odpovídajícímu záznamu. Mohou tak učinit pouze za účelem předcházení chybnému určení totožnosti.

Článek 43
Odkazy mezi záznamy

1. Členský stát může vytvořit odkaz mezi jím vloženými záznamy v SIS. Smyslem takového odkazu je zavést souvislost mezi dvěma nebo více záznamy.

2. Vytvoření odkazu nemá dopad na konkrétní opatření, které má být provedeno na základě jednotlivého záznamu opatřeného odkazem, nebo na dobu uchovávání jednotlivých záznamů propojených odkazy.

3. Vytvoření odkazu nemá dopad na práva přístupu upravená tímto nařízením. Orgánům bez práva přístupu k některým kategoriím záznamů není umožněno vidět odkaz na záznam, ke kterému nemají přístup.

4. Členský stát vytvoří odkaz mezi záznamy, je-li to z operativního hlediska potřebné.

5. Domnívá-li se členský stát, že vytvoření odkazu mezi záznamy jiným členským státem je neslučitelné s jeho vnitrostátními právními předpisy nebo mezinárodními závazky, může přijmout nezbytná opatření, která znemožní přístup k příslušnému odkazu z jeho území nebo jeho orgánům nacházejícím se vně jeho území.

6. Technická pravidla pro odkazování mezi záznamy se stanoví a vypracují v souladu s přezkumným postupem uvedeným v čl. 55 odst. 2.

Článek 44
Účel a doba uchovávání doplňujících informací

1. S cílem podporovat výměnu doplňujících informací uchovávají členské státy v centrále SIRENE odkaz na rozhodnutí, na jejichž základě byl záznam pořízen.

2. Osobní údaje vedené v souborech centrálou SIRENE v důsledku výměny informací se uchovávají pouze po dobu potřebnou pro dosažení účelů, pro něž byly tyto údaje poskytnuty. Výmaz těchto údajů se v každém případě provede nejpozději do jednoho roku po výmazu záznamu týkajícího se dotyčné osoby ze SIS.

3. Odstavcem 2 není dotčeno právo členského státu uchovávat ve vnitrostátních souborech údaje týkající se konkrétního záznamu, který členský stát pořídil, nebo záznamu, ve spojení s nímž bylo učiněno opatření na jeho území. Období, po které mohou být takové údaje vedeny v takových souborech, se řídí vnitrostátním právem.

Článek 45
Předávání osobních údajů třetím stranám

Údaje zpracovávané v SIS a související doplňující informace podle tohoto nařízení se neposkytují ani nezpřístupňují žádné třetí zemi nebo mezinárodní organizaci.

KAPITOLA IX

OCHRANA ÚDAJŮ

Článek 46
Platné právní předpisy

1. Na zpracování osobních údajů agenturou podle tohoto nařízení se vztahuje nařízení (ES) č. 45/2001.
2. Na zpracování osobních údajů orgány uvedenými v článku 29 tohoto nařízení se vztahuje nařízení (EU) 2016/679, ledaže by se na ně vztahovaly vnitrostátní předpisy provádějící směrnici (EU) 2016/680.
3. Na zpracování osobních údajů příslušnými vnitrostátními orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, se vztahují vnitrostátní předpisy provádějící směrnici (EU) 2016/680.

Článek 47
Přístupové právo, oprava nepřesných údajů a výmaz protiprávně uchovávaných údajů

1. Právo subjektů údajů na přístup k údajům vloženým o nich v SIS a na opravu či výmaz těchto údajů se vykonává v souladu s právními předpisy členského státu, u kterého toto právo uplatňují.
2. Pokud to stanoví vnitrostátní právní předpisy, rozhoduje o tom, zda a jakým způsobem se tyto informace poskytují, vnitrostátní orgán dozoru.
3. Členský stát, jenž záznam nepořídil, může poskytnout informace o těchto údajích pouze tehdy, pokud předem poskytl členskému státu, jenž záznam pořídil, příležitost zaujmout postoj. Toto se provádí prostřednictvím výměny doplňujících informací.
4. Členský stát přijme rozhodnutí neposkytnout subjektu údajů v souladu s vnitrostátním právem žádné nebo některé informace v takovém rozsahu a po takovou dobu, po jakou takové částečné nebo úplné omezení představuje s přihlédnutím k lidským právům a oprávněným zájmům dotčené fyzické osoby nutné a přiměřené opatření v demokratické společnosti:
   (a) aby se zabránilo maření úředních nebo právních šetření, vyšetřování nebo řízení;
   (b) aby se zabránilo ovlivňování prevence, odhalování, vyšetřování a stíhání trestných činů nebo výkonu trestů;
   (c) pro ochranu veřejné bezpečnosti;
   (d) pro ochranu národní bezpečnosti;
   (e) k ochraně práv a svobod druhých.
5. Dotčená osoba je vyrozuměna co nejdříve a v každém případě do 60 dnů ode dne, kdy požádala o přístup, nebo dříve, stanoví-li tak vnitrostátní právo.
6. Dotčená osoba je o činnostech v návaznosti na výkon svých práv na opravu a vymazání vyrozuměna co nejdříve a v každém případě do tří měsíců ode dne, kdy požádala o opravu nebo vymazání, nebo dříve, stanoví-li tak vnitrostátní právo.

Článek 48
Právo na informace

1. Státní příslušníci třetích zemí, kteří jsou předmětem záznamů pořízených v souladu s tímto nařízením, jsou vyrozuměni v souladu s články 10 a 11 směrnice 95/46/ES. Informace se poskytnou písemně, společně s kopií vnitrostátního rozhodnutí, na jehož základě byl záznam pořízen, nebo s odkazem na ně podle čl. 24 odst. 1.

2. Tyto informace se neposkytnou:

(f) pokud

i) osobní údaje nebyly získány od dotyčného státního příslušníka třetí země

a

ii) poskytnutí informací se ukáže jako nemožné nebo by vyžadovalo nepřiměřené úsilí;

(g) pokud dotyčný státní příslušník třetí země již informace má;

(h) pokud vnitrostátní právo umožňuje omezení práva na informace, zejména za účelem zajištění národní bezpečnosti, obrany, veřejné bezpečnosti a pro předcházení, vyšetřování, odhalování a stíhání trestných činů.

Článek 49
Opravné prostředky

1. Každý má právo podat žalobu u soudu nebo orgánu příslušného podle právních předpisů kteréhokoliv členského státu, zejména ve věci přístupu, opravy, výmazu či poskytnutí informace nebo odškodnění v souvislosti se záznamem, který se ho týká.

2. Aniž jsou dotčena ustanovení článku 53, zavazují se členské státy navzájem vymáhat konečná rozhodnutí vydaná soudy nebo orgány uvedenými v odstavci 1 tohoto článku.

3. K získání uceleného přehledu o fungování opravných prostředků se vnitrostátní orgány dozoru vyzývají, aby vypracovaly standardní statistický systém za účelem každoročního podávání zpráv o:

(a) počtu žádostí subjektů o přístup, které byly podány správci údajů, a počtu případů, kdy byl přístup k údajům poskytnut;

(b) počtu žádostí subjektů o přístup, které byly podány vnitrostátnímu orgánu dozoru, a počtu případů, kdy byl přístup k údajům poskytnut;

(c) počtu žádostí o opravu nepřesných údajů a výmaz protiprávně uchovávaných údajů, které byly podány správci údajů, a počtu případů, kdy byly údaje opraveny nebo vymazány;

(d) počtu žádostí o opravu nepřesných údajů a výmaz protiprávně uchovávaných údajů, které byly podány vnitrostátnímu orgánu dozoru;

(e) počtu případů, které jsou projednávány u soudů;

(f) počtu případů, kdy soud rozhodl ve prospěch žalobce v jakémkoli aspektu případu;

(g) jakýchkoli připomínkách k případům vzájemného uznávání konečných rozhodnutí vydaných soudy nebo orgány jiných členských států v souvislosti se záznamy vytvořenými pořizujícím členským státem.

Vnitrostátní orgány dozoru předávají tyto zprávy prostřednictvím mechanismu spolupráce stanoveného v článku 52.

Článek 50
Dohled nad N.SIS

1. Každý členský stát zajistí, aby nezávislý vnitrostátní orgán dozoru nebo orgány dozoru, které byly v každém členském státě určeny a které mají pravomoci uvedené v kapitole VI směrnice (EU) 2016/680 nebo kapitole VI nařízení (EU) 2016/679, sledovaly nezávisle zákonnost zpracování osobních údajů v SIS na svých územích a jejich předávání mimo svá území, včetně výměny a dalšího zpracování doplňujících informací.

2. Vnitrostátní orgán dozoru zajistí, aby alespoň každým čtvrtým rokem byl v souladu s mezinárodními auditorskými standardy proveden audit činností zpracování údajů v N.SIS. Audit provádí přímo vnitrostátní orgán dozoru či orgány dozoru, nebo si jej vnitrostátní orgán dozoru či orgány dozoru přímo vyžádají od nezávislého auditora pro ochranu údajů. Vnitrostátní orgán dozoru si za všech okolností zachová kontrolu nad nezávislým auditorem a přebírá za něj odpovědnost.

3. Členské státy zajistí, aby vnitrostátní orgán dozoru měl dostatečné zdroje pro plnění úkolů, které mu byly podle tohoto nařízení svěřeny.

Článek 51
Dohled nad agenturou

1. Evropský inspektor ochrany údajů zajistí, aby byly činnosti agentury související se zpracováváním osobních údajů prováděny v souladu s tímto nařízením. Odpovídajícím způsobem se použijí povinnosti a pravomoci uvedené v článcích 46 a 47 nařízení (ES) č. 45/2001.

2. Evropský inspektor ochrany údajů zajistí, aby byl alespoň každým čtvrtým rokem v souladu s mezinárodními auditorskými standardy proveden audit činností agentury souvisejících se zpracováváním osobních údajů. Zpráva o tomto auditu se zasílá Evropskému parlamentu, Radě, agentuře, Komisi a vnitrostátním orgánům dozoru. Agentura má možnost se k zprávě před jejím přijetím vyjádřit.

Článek 52
Spolupráce mezi vnitrostátními orgány dozoru a evropským inspektorem ochrany údajů

1. Vnitrostátní orgány dozoru a evropský inspektor ochrany údajů, každý z nich v rozsahu svých příslušných pravomocí, aktivně spolupracují v rámci svých povinností a zajistí koordinovaný dohled nad SIS.

2. Vyměňují si příslušné informace, každý z nich v rozsahu svých příslušných pravomocí, pomáhají si navzájem při provádění auditů a kontrol, přezkoumávají obtíže týkající se výkladu nebo použití tohoto nařízení nebo jiných platných právních aktů Unie, zabývají se problémy zjištěnými při výkonu nezávislého dohledu nebo při výkonu práv subjektů údajů, vypracovávají harmonizované návrhy společných řešení případných problémů a podle potřeby zvyšují povědomí o právech na ochranu údajů.

3. Pro účely stanovené v odstavci 2 se vnitrostátní orgány dozoru a evropský inspektor ochrany údajů setkávají nejméně dvakrát ročně v rámci Evropského sboru pro ochranu osobních údajů, zřízeného nařízením (EU) 2016/679. Náklady na tato setkání nese a jejich organizaci zajišťuje uvedený sbor zřízený nařízením (EU) 2016/679. Na prvním setkání se přijme jednací řád. Další pracovní metody se vypracují společně podle potřeby.

4. Sbor zřízený nařízením (EU) 2016/679 zasílá Evropskému parlamentu, Radě a Komisi každé dva roky společnou zprávu o činnosti.

KAPITOLA X

ODPOVĚDNOST

Článek 53
Odpovědnost

1. Každý členský stát odpovídá za škodu způsobenou kterékoli osobě při využívání N.SIS. To platí i v případě škody způsobené pořizujícím členským státem tím, že tento členský stát vložil věcně nepřesné údaje nebo údaje protiprávně uchovával.

2. Pokud není členský stát, proti němuž je podána žaloba, členským státem pořizujícím záznam, je členský stát pořizující záznam povinen uhradit na žádost částky vyplacené jako náhrada, ledaže členský stát, který žádá o náhradu, použil údaje v rozporu s tímto nařízením.

3. Pokud nesplnění povinností plynoucích z tohoto nařízení členským státem způsobí SIS škodu, je daný členský stát za tuto škodu odpovědný, ledaže agentura nebo jiný členský stát účastnící se SIS neučinily přiměřené kroky s cílem předejít této škodě nebo zmírnit její následky.

KAPITOLA XI

ZÁVĚREČNÁ USTANOVENÍ

Článek 54
Sledování a statistika

1. Agentura zajistí zavedení postupů pro sledování, jak SIS funguje v porovnání s vytyčenými cíli, které se týkají výstupů, nákladové efektivnosti, bezpečnosti a kvality služeb.

2. Pro účely technické údržby, vypracovávání zpráv a statistik má agentura přístup k nezbytným informacím, které se týkají zpracovávání údajů v centrálním SIS.

3. Agentura zpracovává denní, měsíční a roční statistiky udávající počet evidovaných vstupů podle kategorie záznamů, počet pozitivních nálezů podle kategorie záznamů za rok, počet vyhledávání v SIS a počet přístupů do SIS za účelem vložení, aktualizace nebo výmazu záznamu, a to pro každý z těchto počtů celkem a pro každý členský stát jednotlivě, včetně statistik o postupu konzultace uvedeném v článku 26.

Vypracované statistiky nesmí obsahovat osobní údaje. Roční statistická zpráva se zveřejní.

4. Členské státy, jakož i Europol a Evropská agentura pro pohraniční a pobřežní stráž poskytnou agentuře a Komisi informace nezbytné pro vypracování zpráv uvedených v odstavcích 7 a 8.

5. Agentura postoupí členským státům, Komisi, Europolu a Evropské agentuře pro pohraniční a pobřežní stráž všechny statistické zprávy, které vypracuje. Za účelem sledování toho, jak jsou prováděny právní akty Unie, může Komise požádat agenturu o předložení dalších konkrétních statistických zpráv, pravidelných nebo účelových, o výkonnosti nebo využívání SIS a komunikaci prostřednictvím center SIRENE.

6. Pro účely odstavců 3 až 5 tohoto článku a čl. 15 odst. 5 agentura zřídí, realizuje a provozuje ve svých technických prostorách centrální úložiště obsahující údaje uvedené v odstavci 3 tohoto článku a v čl. 15 odst. 5, které neumožní individuální identifikaci a dovolí Komisi a agenturám uvedeným v odstavci 5 získat konkrétní zprávy a statistiky. Agentura udělí členským státům, Komisi, Europolu a Evropské agentuře pro pohraniční a pobřežní stráž přístup do centrálního úložiště přes zabezpečený přístup prostřednictvím komunikační infrastruktury, s kontrolovaným přístupem a specifickými uživatelskými profily, a to výhradně pro účely hlášení a statistiky.

Podrobná pravidla týkající se fungování centrálního úložiště a pravidla pro ochranu údajů a bezpečnost týkající se úložiště se stanoví a vypracují prostřednictvím prováděcích opatření přijatých přezkumným postupem uvedeným v čl. 55 odst. 2.

7. Dva roky po spuštění provozu SIS a poté vždy po dvou letech předloží agentura Evropskému parlamentu a Radě zprávu o technickém fungování centrálního SIS a komunikační infrastruktury, včetně jejich zabezpečení, a o dvoustranné a mnohostranné výměně doplňujících informací mezi členskými státy.

8. Tři roky po spuštění provozu SIS a poté vždy po čtyřech letech vypracuje Komise celkové hodnocení centrálního SIS a dvoustranné i mnohostranné výměny doplňujících informací mezi členskými státy. Toto celkové hodnocení zahrnuje přezkoumání dosažených výsledků v porovnání s vytyčenými cíli, posouzení trvající platnosti důvodu pro vznik systému, použití tohoto nařízení ve vztahu k centrálnímu SIS, zabezpečení centrálního SIS, jakož i všech dopadů jeho budoucího provozování. Komise předá hodnotící zprávy Evropskému parlamentu a Radě.

Článek 55
Postup projednávání ve výborech

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 56

Změny nařízení (EU) 515/2014

Nařízení (EU) 515/2014[74] se mění takto:

V článku 6 se doplňuje nový odstavec, který zní:

„6. Ve fázi vývoje členské státy obdrží další příspěvek ve výši 36,8 milionu EUR, který se přidělí ve formě jednorázové částky k jejich základnímu příspěvku, a všechny tyto finanční prostředky vyhradí na vnitrostátní systém SIS s cílem zajistit jeho rychlou a účinnou modernizaci v souladu se zavedením centrálního SIS podle nařízení (EU) 2018/…[*] a nařízení (EU) 2018/…[**].

[*]Nařízení o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech (Úř. věst. …..).

[**]Nařízení (EU) 2018/... o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol (Úř. věst. ….).“

Článek 57
Zrušení

Nařízení (ES) č. 1987/2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace

Rozhodnutí Komise 2010/261/EU ze dne 4. května 2010 o bezpečnostním plánu pro centrální SIS II a komunikační infrastrukturu[75]

Článek 25 Úmluvy k provedení Schengenské dohody[76]

Článek 58
Vstup v platnost a použitelnost

1. Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.
2. Použije se ode dne stanoveného Komisí potom, co:
   (a) byla přijata nezbytná prováděcí opatření;
   (b) členské státy Komisi oznámí, že přijaly nezbytná technická a právní opatření pro zpracovávání údajů SIS a výměnu doplňujících informací podle tohoto nařízení;
   (c) agentura oznámí Komisi ukončení veškerého testování v souvislosti s CS-SIS a s interakcí mezi CS-SIS a N.SIS.
3. Toto nařízení je závazné v celém rozsahu a přímo použitelné v členských státech v souladu se Smlouvou o fungování Evropské unie.

[74] 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 (Úř. věst. L 150, 20.5.2014, s. 143).

[75] Rozhodnutí Komise 2010/261/EU ze dne 4. května 2010 o bezpečnostním plánu pro centrální SIS II a komunikační infrastrukturu (Úř. věst. L 112, 5.5.2010, s. 31).

[76] Úř. věst. L 239, 22.9.2000, s. 19.

V Bruselu dne

Za Evropský parlament
předseda

Za Radu
předseda

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1 Název návrhu/podnětu

1.2 Příslušné oblasti politik podle členění ABM/ABB

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, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol a o zrušení nařízení (ES) č. 1987/2006.

1.2 Příslušné oblasti politik podle členění ABM/ABB[77]

Oblast politiky: Migrace a vnitřní věci (hlava 18)

1.3 Povaha návrhu/podnětu

☐ Návrh/podnět se týká **nové akce**

☐ Návrh/podnět se týká **nové akce následující po pilotním projektu / přípravné akci**[78]

☑ 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

Cíl – „Na cestě k nové migrační politice“

Nutnost přezkoumat právní základ SIS za účelem řešení nových výzev v oblasti bezpečnosti a migrace zdůraznila Komise již při mnoha příležitostech. V „Evropském programu pro migraci“[79] například Komise uvedla, že má-li být správa hranic účinnější, je také třeba lépe využívat příležitostí, které nabízejí systémy IT a technologie. V „Evropském programu pro bezpečnost“[80] Komise oznámila svůj záměr vyhodnotit SIS v letech 2015 a 2016 a prozkoumat možnosti, jak členským státům pomoci při uplatňování zákazů cestování vydaných na vnitrostátní úrovni. V „Akčním plánu EU proti pašování migrantů“[81] Komise uvedla, že zváží, zda pro orgány členských států zavede povinnost evidovat všechny zákazy vstupu v SIS, aby se umožnila jejich vymahatelnost na celém území EU. Dále Komise prohlásila, že bude zabývat tím, zda je možné a přiměřené evidovat rozhodnutí o navrácení vydaná orgány členských států s cílem zjistit, zda se na zadrženého nelegálního migranta nevztahuje rozhodnutí o navrácení vydané jiným členským státem. A konečně, ve sdělení „Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost“[82] Komise vysvětlila, že v současnosti zkoumá možné další funkce systému SIS s cílem předložit návrhy na revizi jeho právního základu.

---

77 ABM: řízení podle činností (activity-based management) – ABB: sestavování rozpočtu podle činností (activity-based budgeting).

78 Uvedené v čl. 54 odst. 2 písm. a) nebo b) finančního nařízení.

79 COM(2015) 240 final.

80 COM(2015) 185 final.

81 COM(2015) 285 final.

82 COM(2016) 205 final.

Jakožto výsledek celkového hodnocení tohoto systému a plně v souladu s víceletými cíli Komise, vymezenými ve výše zmíněných sděleních a ve strategickém plánu GŘ pro migraci a vnitřní věci 2016–2020[83], má tento návrh za cíl reformovat strukturu, provoz a využívání Schengenského informačního systému v oblasti hraničních kontrol.

1.4.2 Specifické cíle a příslušné aktivity ABM/ABB

Specifický cíl č.

GŘ pro migraci a vnitřní věci – plán řízení na rok 2017 – specifický cíl č. 1.2:

Účinná správa hranic – záchrana životů a zabezpečení vnějších hranic EU

Příslušné aktivity ABM/ABB

Kapitola 18 02 – Vnitřní bezpečnost

[83] Ares(2016)2231546 – 12. května 2016.

1.4.3 Očekávané výsledky a dopady

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

K hlavním cílům politiky patří:

1) Přispět k zajištění vysokého stupně bezpečnosti v rámci prostoru svobody, bezpečnosti a práva EU.

2) Zvýšit efektivnost a účinnost hraničních kontrol.

GŘ HOME doporučilo na základě celkového hodnocení SIS, které provedlo v letech 2015 a 2016, technická zlepšení tohoto systému a harmonizaci vnitrostátních postupů v oblasti správy odepření vstupu a pobytu. Stávající nařízení o SIS II například členským státům pouze umožňuje pořizovat v tomto systému záznamy pro účely odepření vstupu a pobytu, avšak neukládá to jako povinnost. Některé členské státy systematicky vkládají do SIS všechny zákazy vstupu, zatímco jiné nikoli. Předmětný návrh proto přispěje k dosažení vyšší úrovně harmonizace v této oblasti, neboť zavede povinnost vkládat do SIS všechny zákazy vstupu, stanoví společná pravidla pro vkládání záznamů do tohoto systému včetně povinnosti záznam zdůvodnit.

Nový návrh zavádí opatření, jež řeší provozní a technické potřeby koncových uživatelů. Zejména jsou to nová datová pole ve stávajících záznamech, která poskytnou příslušníkům pohraniční stráže všechny informace nezbytné k účinnému plnění úkolů. Návrh také výslovně zdůrazňuje význam nepřetržité dostupnosti SIS, protože jeho výpadky mohou podstatně ohrozit schopnost provádět ochranu vnějších hranic. Návrh tak bude mít velmi pozitivní dopad na účinnost hraničních kontrol.

Po přijetí a provedení zlepší uvedené návrhy také kontinuitu provozu, neboť členské státy budou povinny mít úplnou nebo částečnou vnitrostátní kopii a její zálohu. Pracovníkům v terénu tak bude vždy k dispozici plně funkční a provozuschopný systém.

1.4.4 Ukazatele výsledků a dopadů

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

Během modernizace systému

Po schválení předlohy návrhu a přijetí technických specifikací bude SIS modernizován za účelem důkladnější harmonizace vnitrostátních postupů pro využívání systému, za účelem rozšíření oblasti působnosti systému zvýšením míry informací dostupných koncovým uživatelům v zájmu zlepšení informovanosti pracovníků provádějících kontroly, jakož i za účelem zavedení technických změn ke zvýšení bezpečnosti a snížení administrativní zátěže. Řízení projektu týkajícího se modernizace systému bude koordinovat agentura eu-LISA. Agentura vytvoří strukturu projektového řízení a poskytne podrobný harmonogram s milníky pro provedení navrhovaných změn, jež Komisi umožní podrobně sledovat provádění návrhu.

Specifický cíl – spuštění aktualizovaných funkcí SIS v roce 2020

Ukazatel – úspěšné dokončení komplexního testování revidovaného systému před uvedením do provozu

Po uvedení systému do provozu

Po uvedení systému do provozu agentura eu-LISA zajistí zavedení postupů pro sledování, jak funguje SIS v porovnání s vytyčenými cíli, které se týkají výstupů,

nákladové efektivnosti, bezpečnosti a kvality služeb. Dva roky po spuštění provozu SIS a poté vždy po dvou letech má agentura eu-LISA předkládat Evropskému parlamentu a Radě zprávu o technickém fungování centrálního SIS a komunikační infrastruktuře, včetně jejich zabezpečení, a o dvoustranné a mnohostranné výměně doplňujících informací mezi členskými státy. Agentura eu-LISA také zpracovává denní, měsíční a roční statistiky udávající počet protokolů podle kategorie záznamů, počet pozitivních nálezů podle kategorie záznamů za rok, počet vyhledávání v SIS a počet přístupů do SIS za účelem vložení, aktualizace nebo výmazu záznamu, a to pro každý z těchto počtů celkem a pro každý členský stát jednotlivě.

Tři roky po spuštění provozu SIS a poté vždy po čtyřech letech vypracuje Komise celkové hodnocení centrálního SIS a dvoustranné i mnohostranné výměny doplňujících informací mezi členskými státy. Toto celkové hodnocení zahrnuje přezkoumání dosažených výsledků v porovnání s vytyčenými cíli, posouzení trvající platnosti důvodu pro vznik systému, použití tohoto nařízení ve vztahu k centrálnímu SIS, bezpečnost centrálního SIS, jakož i všech dopadů jeho budoucího provozování. Komise předává hodnotící zprávy Evropskému parlamentu a Radě.

1.5 Odůvodnění návrhu/podnětu

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

1. Přispět k zajištění vysokého stupně bezpečnosti v rámci prostoru svobody, bezpečnosti a práva EU.

2. Zesílit boj proti mezinárodní trestné činnosti, terorismu a dalším bezpečnostním hrozbám.

3. Rozšířit oblast působnosti SIS zavedením nových prvků v záznamech o odepření vstupu a pobytu.

4. Zvýšit efektivnost hraničních kontrol.

5. Zvýšit účinnost činnosti příslušníků pohraniční stráže a imigračních orgánů.

6. Dosáhnout větší míry efektivnosti a harmonizace vnitrostátních postupů a zajistit vymahatelnost zákazů vstupu v celém schengenském prostoru.

7. Přispět k boji proti nelegální migraci.

1.5.2 Přidaná hodnota ze zapojení EU

SIS je hlavní bezpečnostní databáze v Evropě. Při neexistenci kontrol na vnitřních hranicích získal účinný boj proti trestné činnosti a terorismu evropský rozměr. SIS je proto nezbytný jako podpůrný nástroj při ochraně vnějších hranic a kontrolách nelegálních migrantů zjištěných na území jednotlivých zemí. Cílem tohoto návrhu jsou technická zlepšení za účelem zefektivnění a zlepšení účinnosti systému a harmonizace jeho využívání ve všech zúčastněných členských státech. Nadnárodní povaha těchto cílů spolu s výzvami při zajišťování účinné výměny informací, která by zabránila stále různorodějším hrozbám, znamenají, že EU má nejlepší předpoklady k tomu, aby navrhovala řešení těchto problémů. Cílů zvýšení efektivity a harmonizovaného využívání SIS, konkrétně zvýšení objemu, kvality a rychlosti výměny informací prostřednictvím centralizovaného rozsáhlého informačního systému spravovaného regulační agenturou (eu-LISA), nemohou dosáhnout členské státy samotné, a proto jsou zapotřebí opatření na úrovni EU. Nebudou-li stávající problémy řešeny, bude SIS nadále fungovat podle pravidel platných v současné době,

což znamená ignorovat příležitost k maximalizaci efektivity a přidané hodnoty EU zjištěné při hodnocení SIS a jeho využívání členskými státy.

Jen v roce 2015 provedly vnitrostátní orgány v SIS téměř 2,9 miliardy vyhledávání a vyměnily si přes 1,8 milionu doplňujících informací, což představuje jasný důkaz zásadního podílu tohoto systému na ochraně vnějších hranic. Decentralizovaná řešení by takovouto vysokou úroveň výměny informací mezi členskými státy nezajistila a na národní úrovni by uvedených výsledků nebylo možno dosáhnout. SIS se také ukázal jako nejúčinnější nástroj pro výměnu informací za účelem boje proti terorismu a poskytuje přidanou hodnotu EU, neboť vnitrostátním bezpečnostním službám umožňuje spolupracovat rychlým a účinným způsobem zaručujícím důvěrnost. Nové návrhy ještě zjednoduší výměnu informací a spolupráci mezi orgány členských států EU pro ochranu hranic. Europol a Evropská pohraniční a pobřežní stráž získají v neposlední řadě v rámci svých pravomocí plný přístup do tohoto systému, což je jasná známka přidané hodnoty ze zapojení EU.

1.5.3 Závěry vyvozené z podobných zkušeností v minulosti

Hlavní závěry vyvozené z vývoje Schengenského informačního systému druhé generace jsou tyto:

1. Fáze vývoje by měla být zahájena až po přesném definování technických a provozních požadavků. Vývoj lze provádět až poté, co byly s konečnou platností přijaty právní nástroje, které stanoví účel, oblast působnosti, funkce a technické specifikace systému.

2. Komise vedla (a nadále vede) časté konzultace s příslušnými zúčastněnými stranami, mimo jiné s delegáty výboru pro SISVIS postupem projednávání ve výborech. Tento výbor tvoří zástupci členských států jak pro provozní záležitosti SIRENE (přeshraniční spolupráce v souvislosti se SIS), tak pro technické otázky týkající se vývoje a údržby SIS a související aplikace SIRENE. Změny navržené v tomto nařízení byly transparentně a komplexně projednány na zvláštních setkáních a pracovních seminářích. Dále Komise interně ustavila meziútvarovou řídící skupinu, v níž byl zastoupen Generální sekretariát a Generální ředitelství pro migraci a vnitřní věci, Generální ředitelství pro spravedlnost a spotřebitele, Generální ředitelství pro lidské zdroje a bezpečnost a Generální ředitelství pro informatiku. Tato řídící skupina sledovala proces hodnocení a dle potřeby poskytovala poradenství.

3. Komise si rovněž vyžádala externí odborné poradenství ve formě tří studií, jejichž výsledky byly při vypracovávání tohoto návrhu zohledněny:

– Technický posudek SIS (Kurt Salmon) – v tomto posudku byly vymezeny klíčové otázky pro fungování SIS a budoucí potřeby, které by měly být zváženy. Také byly identifikovány problémy v souvislosti s maximalizací kontinuity provozu a zajištěním toho, aby se celková architektura dokázala přizpůsobit rostoucím kapacitním požadavkům.

– Posouzení dopadů možných zlepšení architektury SIS II z hlediska IKT (Kurt Salmon) – tato studie posoudila běžné náklady na provoz SIS v členských státech a vyhodnotila tři možné technické scénáře zlepšení systému. Všechny scénáře obsahují soubor technických návrhů zaměřený na zlepšení centrálního systému a celkové architektury.

– Studie proveditelnosti a dopadů vytvoření celounijního systému pro výměnu údajů o rozhodnutích o navrácení a sledování jejich dodržování, začleněného do

Schengenského informačního systému (PwC) – tato studie posuzuje proveditelnost navrhovaných změn SIS a jejich technické a provozní dopady s cílem optimalizovat využívání SIS pro účely navracení nelegálních migrantů a zamezení jejich opětovnému vstupu.

1.5.4 Soulad a možná synergie s dalšími vhodnými nástroji:

Tento návrh je třeba považovat za realizaci opatření uvedených ve sdělení ze dne 6. dubna 2016 s názvem „Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost“[84], které zdůrazňuje, že EU musí posílit a zlepšit své informační systémy, datovou architekturu a výměnu informací v oblasti prosazování práva, boje proti terorismu a správy hranic.

Návrh je navíc v souladu s řadou politik Unie v této oblasti:

a) vnitřní bezpečnost ve vztahu k úloze SIS bránit vstupu státních příslušníků třetích zemí, kteří představují bezpečnostní hrozbu;

b) ochrana údajů v rozsahu, v jakém tento návrh musí zajistit ochranu základních práv, aby byl respektován soukromý život fyzických osob, jejichž osobní údaje jsou zpracovávány v SIS.

Návrh je také slučitelný se stávajícími právními předpisy Evropské unie. Konkrétně to jsou:

a) účinná návratová politika EU, která zlepší a posílí systém EU pro odhalování a předcházení opětovného vstupu státních příslušníků třetích zemí po jejich navrácení. To by pomohlo snížit motivaci k nelegální migraci do EU, což je jeden z hlavních cílů Evropského programu pro migraci[85]; b) **Evropská pohraniční a pobřežní stráž[86]**, pokud jde o možnost, aby pracovníci agentury prováděli analýzy rizik a o právo příslušníků jednotek Evropské pohraniční a pobřežní stráže, týmů pracovníků, kteří se podílejí na úkolech spojených s navracením, a členů podpůrných týmů pro řízení migrace na přístup v rámci jejich mandátu k údajům vloženým do SIS a právo v těchto údajích vyhledávat;

c) **ochrana vnějších hranic** v rozsahu, v jakém toto nařízení napomáhá členským státům chránit jejich úsek vnějších hranic EU a budovat důvěru v účinnost systému EU pro správu hranic;

d) Europol v rozsahu, v jakém tento návrh uděluje Europolu v rámci jeho mandátu další práva na přístup a vyhledávání v údajích vložených do SIS.

Návrh je také slučitelný s budoucími právními předpisy Evropské unie. Konkrétně to jsou:

84 COM(2016) 205 final.

85 COM(2015) 240 final.

86 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 o 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).

a) **systém vstupu/výstupu**[87] (EES) – pro účely jeho provozu se navrhuje kombinace otisku prstu a zobrazení obličeje jako biometrických identifikátorů, což je přístup, který tento návrh zohledňuje;

b) **ETIAS** – navrhuje se důkladné posuzování státních příslušníků třetích zemí osvobozených od vízové povinnosti, kteří mají v úmyslu cestovat do EU, z bezpečnostního hlediska, včetně jejich ověření v SIS.

87 Návrh nařízení Evropského parlamentu a Rady, 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 Evropské unie, kterým se stanoví podmínky přístupu do systému EES pro účely vymáhání práva a kterým se mění nařízení (ES) č. 767/2008 a nařízení (EU) č. 1077/2011 (COM(2016) 194 final).

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

– Provádění s obdobím rozběhu od roku 2018 do roku 2020,

– poté plné fungování.

1.7 Předpokládaný způsob řízení[88]

☑ **Přímé řízení** Komisí

– ☑ 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

Komise bude odpovědná za celkové řízení politiky a agentura eu-LISA bude odpovědná za vývoj, provoz a údržbu systému.

SIS představuje jednotný informační systém. Výdaje stanovené ve dvou z návrhů (v tomto návrhu a návrhu nařízení o zřízení, provozu a využívání Schengenského informačního systému v oblasti policejní spolupráce a justiční spolupráce v trestních věcech) by proto měly být považovány nikoli za dvě oddělené částky, ale za jedinou. Rozpočtové důsledky změn vyžadovaných pro provedení obou návrhů jsou proto uvedeny v jediném legislativním finančním výkazu.

[88] Vysvětlení způsobů řízení spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. SPRÁVNÍ OPATŘENÍ

2.1 Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Komise, členské státy a agentura budou pravidelně přezkoumávat a sledovat využívání SIS s cílem zajistit, že nadále funguje efektivně a účelně. Komisi bude při provádění technických a provozních opatření popsaných v tomto návrhu nápomocen výbor.

Toto navrhované nařízení navíc v čl. 54 odst. 7 a 8 obsahuje ustanovení o formálním pravidelném přezkumu a procesu hodnocení.

Vždy po dvou letech musí agentura eu-LISA předložit Evropskému parlamentu a Radě zprávu o technickém fungování centrálního SIS, včetně jeho zabezpečení, podpůrné komunikační infrastruktuře a o dvoustranné a mnohostranné výměně doplňujících informací mezi členskými státy.

Dále vždy po čtyřech letech musí Komise vypracovat celkové hodnocení SIS a výměny informací mezi členskými státy, které postoupí Parlamentu a Radě. To bude znamenat:

a) přezkoumání dosažených výsledků v porovnání s vytyčenými cíli;

b) posouzení, zda stále platí důvod pro vznik systému;

c) přezkoumání uplatňování nařízení v souvislosti s centrálním systémem;

d) vyhodnocení zabezpečení centrálního systému;

e) zhodnocení dopadů budoucího fungování systému.

2.2 Agentura eu-LISA má nyní také povinnost zpracovávat denní, měsíční a roční statistiky týkající se využívání SIS a zajistit nepřetržité monitorování systému a jeho fungování v porovnání s vytyčenými cíli. Systém řízení a kontroly

2.2.1 Zjištěná rizika

Byla zjištěna tato rizika:

1. Možné problémy agentury eu-LISA při řízení změn uvedených v tomto návrhu současně s jinými probíhajícími změnami (např. zavedení AFIS v rámci SIS) a budoucím vývojem (např. systém vstupu/výstupu, ETIAS a modernizace Eurodacu). Toto riziko lze snížit zajištěním toho, aby měla agentura eu-LISA dostatečný počet pracovníků a zdroje potřebné pro plnění těchto úkolů, a průběžným řízením dodavatele zajišťujícího údržbu provozního stavu (MWO).

2. Problémy členských států:

2.1 Tyto problémy jsou zejména finančního rázu. Legislativní návrhy například obsahují povinný vývoj částečné vnitrostátní kopie v každém N.SIS II. Členské státy, které takovou kopii již nevyvinuly, budou muset vynaložit finanční prostředky. Obdobně platí, že na vnitrostátní úrovni by měl být v úplném rozsahu zaveden dokument pro ovládání rozhraní. Členské státy, které tak dosud neučinily, na to budou muset vyčlenit finanční prostředky v rozpočtu příslušných ministerstev. Toto riziko lze snížit poskytnutím finančních prostředků EU členským státům, například ze složky Fondu pro vnitřní bezpečnost týkající se vnějších hranic (ISF).

2.2 Vnitrostátní systémy je nutno přizpůsobit centrálním požadavkům a diskuse s členskými státy na toto téma mohou způsobit prodlevy při vývoji. Toto riziko lze snížit včasným zapojením členských států do řešení této záležitosti s cílem zajistit možnost přijetí opatření v příslušné době.

2.2.2 Informace o zavedeném systému vnitřní kontroly

Povinnosti týkající se centrálních složek SIS vykonává agentura eu-LISA. Aby bylo možno lépe sledovat využívání SIS s cílem analyzovat tendence, pokud jde o migrační tlak, správu hranic a trestné činy, měla by být agentura schopna vytvořit špičkovou kapacitu pro statistické hlášení členským státům a Komisi.

Účetní závěrky agentury eu-LISA podléhají schválení Účetním dvorem a postupu udělování absolutoria. Útvar interního auditu Komise bude provádět audity ve spolupráci s interním auditorem agentury.

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

N/A

2.3 Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření.

Plánovaná opatření na 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. Agentura přistoupí k interinstitucionální dohodě o vnitřním vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF) a neprodleně vydá odpovídající předpisy platné pro všechny její 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 agentury 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

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			
	Okruh 3 – Bezpečnost a občanství	RP/NRP[89]	zemí ESVO[90]	kandidátských zemí[91]	třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení
	18 02 08 – Schengenský informační systém	RP	NE	NE	ANO	NE
	18 02 01 01 – Podpora správy hranic a společné vízové politiky na usnadnění legálního cestování	RP	NE	NE	ANO	NE
	18 02 07 – Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva („eu-LISA“)	RP	NE	NE	ANO	NE

89 RP = rozlišené prostředky / NRP = nerozlišené prostředky.
90 ESVO: Evropské sdružení volného obchodu.
91 Kandidátské země a případně potenciální kandidátské země západního Balkánu.

3.2 Odhadovaný dopad na výdaje

3.2.1 Odhadovaný souhrnný dopad na výdaje

Okruh víceletého finančního rámce	3	Bezpečnost a občanství

GŘ HOME			Rok **2018**	Rok **2019**	Rok **2020**	**CELKEM**
• Operační prostředky						
18 02 08 – Schengenský informační systém	Závazky	(1)	6,234	1,854	1,854	**9,942**
	Platby	(2)	6,234	1,854	1,854	**9,942**
18 02 01 01 (Hranice a víza)	Závazky	(1)		18,405	18,405	**36,810**
	Platby	(2)		18,405	18,405	**36,810**
CELKEM prostředky pro GŘ HOME	Závazky	=1+1a +3	6,234	20,259	20,259	**46,752**
	Platby	=2+2a +3	6,234	20,259	20,259	**46,752**

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce	3	Bezpečnost a občanství

eu-LISA			Rok **2018**	Rok **2019**	Rok **2020**	**CELKEM**
• Operační prostředky						
Hlava 1: Výdaje na zaměstnance	Závazky	(1)	0,210	0,210	0,210	**0,630**
	Platby	(2)	0,210	0,210	0,210	**0,630**
Hlava 2: Výdaje na infrastrukturu a provoz	Závazky	(1a)	0	0	0	**0**
	Platby	(2a)	0	0	0	**0**
Hlava 3: Operační výdaje	Závazky	(1a)	12,893	2,051	1,982	**16,926**
	Platby	(2a)	2,500	7,893	4,651	**15,044**
CELKEM prostředky pro eu-LISA	Závazky	=1+1a +3	13,103	2,261	2,192	**17,556**
	Platby	=2+2a +3	2,710	8,103	4,861	**15,674**

3.2.2 Odhadovaný dopad na operační prostředky

• Operační prostředky CELKEM	Závazky	(4)								
	Platby	(5)								
• Prostředky správní povahy financované z rámce na zvláštní programy CELKEM		(6)								
CELKEM prostředky	Závazky	=4+ 6								

na OKRUH <….> víceletého finančního rámce	Platby	=5+ 6								

Má-li návrh/podnět dopad na více okruhů:

• Operační prostředky CELKEM	Závazky	(4)							
	Platby	(5)							
• Prostředky správní povahy financované z rámce na zvláštní programy CELKEM		(6)							
CELKEM prostředky z OKRUHU 1 až 4 víceletého finančního rámce (referenční částka)	Závazky	=4+ 6	19,337	22,520	22,451				**64,308**
	Platby	=5+ 6	8,944	28,362	25,120				**62,426**

3.2.3 Odhadovaný dopad na prostředky správní povahy

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

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			**CELKEM**
GŘ: <…….>									
• Lidské zdroje									
• Ostatní správní výdaje									
GŘ <….> CELKEM	Prostředky								

CELKEM prostředky na OKRUH 5 víceletého finančního rámce	(Závazky celkem = platby celkem)								

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **N**[92]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			**CELKEM**
CELKEM prostředky z OKRUHU 1 až 5 víceletého finančního rámce	Závazky								
	Platby								

[92] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět.

3.2.3.1 Odhadovaný dopad na operační prostředky eu-LISA

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

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

Uveďte cíle a výstupy ⇩			Rok **2018**		Rok **2019**		Rok **2020**		Vložit počet let podle trvání finančního dopadu (viz bod 1.6)						**CELKEM**			
	VÝSTUPY																	
	Druh[93]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 1[94] Vývoj centrálního systému																		
– Externí smluvní			1	5,013														5,013
– Programové vybavení (software)			1	4,050														4,050
– Technické vybavení (hardware)			1	3,692														3,692
Mezisoučet za specifický cíl č. 1				12,755														12,755
SPECIFICKÝ CÍL Č. 2 Údržba centrálního systému																		
– Externí smluvní strana			1	0	1	0,365	1	0,365										0,730

[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…“.

Programové vybavení (software)			1	0	1	0,810	1	0,810										1,620
Technické vybavení (hardware)			1	0	1	0,738	1	0,738										1,476
Mezisoučet za specifický cíl č. 2						1,913		1,913										3,826
SPECIFICKÝ CÍL Č. 3 Zasedání / školicí kurzy																		
Školení			1	0,138	1	0,138	1	0,069										0,345
Mezisoučet za specifický cíl č. 3				0,138		0,138		0,069										0,345
NÁKLADY CELKEM				12,893		2,051		1,982										16,926

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

3.2.3.2 Odhadovaný dopad na operační prostředky GŘ HOME

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

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

Uveďte cíle a výstupy ⇩			Rok **2018**		Rok **2019**		Rok **2020**		Vložit počet let podle trvání finančního dopadu (viz bod 1.6)						**CELKEM**			
	VÝSTUPY																	
	Druh[95]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 1[96] Vývoj vnitrostátního systému			1		1	1,221	1	1,221										2,442
SPECIFICKÝ CÍL Č. 2 Infrastruktura			1		1	17,184	1	17,184										34,368
NÁKLADY CELKEM						18,405		18,405										36,810

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

96 Popsaný v bodě 1.4.2 „Specifické cíle…“

3.2.3.3 Odhadovaný dopad na lidské zdroje eu-LISA – souhrn

– ☐ 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 **2018**	Rok **2019**	Rok **2020**	**CELKEM**
Úředníci (AD)				
Úředníci (AST)				
Smluvní zaměstnanci	0,210	0,210	0,210	0,630
Dočasní zaměstnanci				
Vyslaní národní odborníci				
CELKEM	**0,210**	**0,210**	**0,210**	**0,630**

Nábor pracovníků je naplánován na leden 2018. Všichni pracovníci musí být k dispozici na začátku roku 2018, aby bylo možné včas začít s vývojem s cílem zajistit, aby byl provoz přepracovaného SIS zahájen v roce 2020. Zapotřebí jsou tři noví smluvní zaměstnanci (SZ), kteří pokryjí potřeby jak v souvislosti s prováděním projektu, tak ohledně provozní podpory a údržby po uvedení do provozu. Tyto zdroje budou využity na:

- podporu provádění projektu jako členové týmu projektu, včetně činností, které zahrnují definování požadavků a technických specifikací, spolupráci s členskými státy a poskytování podpory členským státům při provádění, aktualizaci dokumentu pro ovládání rozhraní (ICD), monitorování smluvních dodávek, poskytování a aktualizaci dokumentace atd.,
- podporu činností souvisejících s přechodem, jejichž cílem je zprovoznit systém ve spolupráci s dodavatelem (sledování verzí, aktualizace operačního procesu, odborná příprava (včetně odborné přípravy v členských státech)) atd.,
- podporu dlouhodobějších činností, definice specifikací, vypracování smluv v případě změny systému (např. kvůli rozpoznávání zobrazení) nebo v případě, že bude zapotřebí upravit smlouvu o údržbě provozního stavu (MWO) nového SIS II tak, aby zahrnovala dodatečné změny (technické a rozpočtové),
- zvýšení podpory druhé úrovně po zahájení provozu, během průběžné údržby a provozu.

Je třeba uvést, že tyto tři nové zdroje (smluvní zaměstnanci na plný pracovní úvazek) budou pracovat nad rámec zdrojů interních týmů, jež budou vyhrazeny i na jiné činnosti, které souvisejí s projektem a s kontrolou plnění smluvních závazků, finanční kontrolou a provozem. Využitím smluvních zaměstnanců se zabezpečí dostatečná doba trvání a kontinuita smluv tak, aby se zajistila kontinuita provozu a uplatnění týchž odborníků pro operativní podpůrné

činnosti po dokončení projektu. Operativní podpůrné činnosti kromě toho vyžadují přístup k produkčnímu prostředí, který nelze poskytnout smluvním dodavatelům nebo externím pracovníkům.

3.2.3.4 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 **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)		
• **Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)**							
XX 01 01 01 (v ústředí a v zastoupeních Komise)							
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)**[97]							
XX 01 02 01 (SZ, VNO, ZAP z celkového rámce)							
XX 01 02 02 (SZ, MZ, VNO, ZAP a MOD při delegacích)							
XX 01 04 **yy** [98] – v ústředí							
– 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							

XX 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:

Úředníci a dočasní zaměstnanci	
Externí zaměstnanci	

97 SZ = smluvní zaměstnanec; MZ = místní zaměstnanec; VNO = vyslaný národní odborník; ZAP = zaměstnanec agentury práce; MOD = mladý odborník při delegaci.

98 Dílčí strop na externí zaměstnance financované z operačních prostředků (bývalé položky „BA“).

3.2.4 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.

Za účelem vytvoření funkcí a provedení změn podle uvedených dvou návrhů se plánuje přerozdělení zbývajícího finančního krytí na inteligentní hranice v rámci Fondu pro vnitřní bezpečnost. Finančním nástrojem, do nějž byl začleněn rozpočet na provedení balíčku týkajícího se inteligentních hranic, je nařízení o nástroji pro podporu v oblasti vnějších hranic v rámci Fondu pro vnitřní bezpečnost. V článku 5 uvedeného nařízení se stanoví, že v rámci provádění programu pro zřizování systémů informačních technologií na podporu řízení migračních toků přes vnější hranice je za podmínek stanovených v článku 15 čerpáno 791 milionů EUR. Z výše uvedených 791 milionů EUR je 480 milionů EUR vyhrazeno na vývoj systému vstupu/výstupu a 210 milionů EUR na vývoj evropského systému pro cestovní informace a povolení (ETIAS). Zbývající prostředky, tedy 100,828 milionu EUR, budou částečně použity k uhrazení nákladů na změny uvedené v obou návrzích týkajících se SIS.

– ☐ Návrh/podnět vyžaduje použití nástroje pružnosti nebo změnu víceletého finančního rámce.

Upřesněte potřebu, příslušné okruhy a rozpočtové položky a odpovídající částky.

3.2.5 Příspěvky třetích stran

– ☑ Návrh/podnět nepočítá se spolufinancováním od třetích stran.

– Návrh/podnět počítá se spolufinancováním podle následujícího odhadu:

prostředky v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			Celkem
Upřesněte spolufinancující subjekt								
Spolufinancované prostředky CELKEM								

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[99]						
		2018	2019	2020	2021	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)		
Článek 6313 – Příspěvky zemí přidružených k Schengenu (CH, NO, LI, IS)		p.m	p.m	p.m	p.m			

U účelově vázaných různých příjmů upřesněte dotčené výdajové rozpočtové položky.

18 02 08 (Schengenský informační systém), 18 02 07 (eu-LISA)

Upřesněte způsob výpočtu dopadu na příjmy.

Rozpočet zahrnuje příspěvek od zemí přidružených k provádění, uplatňování a rozvoji schengenského *acquis*.

[99] Pokud jde o tradiční vlastní zdroje (cla, dávky z cukru), je třeba uvést čisté částky, tj. hrubé částky po odečtení 25 % nákladů na výběr.