EVROPSKÁ
KOMISE

V Bruselu dne 21.12.2016
COM(2016) 883 final

2016/0409 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, o změně nařízení (EU) č. 515/2014 a o zrušení nařízení (ES) č. 1986/2006, rozhodnutí Rady 2007/533/SVV a rozhodnutí Komise 2010/261/EU

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

V průběhu minulých dvou letech 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 nejúspěšnější nástroj 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 představuje 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 souvisle 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 tímto účelem provádí Komise přezkum stávající informační architektury, který umožní identifikovat mezery a slepá místa, 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 případně předloží druhý soubor návrhů s cílem ještě 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.

Tento návrh je součástí prvního souboru návrhů[6] na zlepšení fungování systému SIS a jeho provozu a využívání v oblasti policejní spolupráce a justiční spolupráce v trestních věcech. Zahrnuje:

1) záměr Komise zvýšit přidanou hodnotu SIS pro účely prosazování práva[7] v reakci na nové hrozby;

2) 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;

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

---

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 (EU) 2018/xxx [hraniční kontroly] a nařízení (EU) 2018/xxx [navracení neoprávněně pobývajících státních příslušníků třetích zemí].

7 Viz sdělení Komise o „Naplňování Evropského programu pro bezpečnost v zájmu boje proti terorismu a položení základů účinné a skutečné bezpečnostní unie“, COM(2016) 230 final ze dne 20.4.2016, s. 4.

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.

4) zohlednění žádostí koncových uživatelů SIS o provedení technických zlepšení a

5) 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 Komisí navrhovaným nařízením o zřízení, provozu a využívání SIS v oblasti hraničních kontrol, 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].

Základem stávajícího právního rámce druhé generace SIS – týkajícího se využívání SIS pro účely policejní spolupráce a justiční spolupráce v trestních věcech – je nástroj bývalého třetího pilíře: rozhodnutí Rady 2007/533/SVV[11], jakož i nástroj bývalého prvního pilíře: nařízení (ES) č. 1986/2006[12].Tento návrh konsoliduje obsah stávajících nástrojů a doplňuje nová ustanovení s cílem:

- lépe harmonizovat vnitrostátní postupy pro využívání SIS, zejména s ohledem na teroristické trestné činy, jakož i na děti, u nichž hrozí únos jejich rodičem;
- rozšířit oblast působnosti SIS zavedením nových prvků biometrických identifikátorů do stávajících záznamů;
- zavést technické změny ke zlepšení bezpečnosti a pomoci snížit administrativní zátěž tím, že se stanoví povinné vnitrostátní kopie a společné technické normy pro provádění;
- vyřešit komplexní využívání všech prvků SIS (*end-to-end*), které by nejen pokrývalo centrální a vnitrostátní systémy, ale také zajistilo, že koncoví uživatelé obdrží veškeré údaje potřebné k plnění úkolů a budou při zpracování údajů SIS dodržovat všechna bezpečnostní pravidla.

• Soulad s ostatními politikami Unie a rovněž se stávajícími a budoucími právními nástroji

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

1) **Vnitřní bezpečnost**, jak zdůrazňuje Evropský program pro bezpečnost[13], a úsilí Komise o účinnou a efektivní bezpečnostní unii[14], jejichž cílem je prevence, odhalování, vyšetřování a stíhání teroristických trestných činů a jiných závažných trestných činů tím, že se umožní donucovacím orgánům zpracovávat osobní údaje osob, u nichž existuje podezření, že se podílejí na teroristických činech nebo závažných trestných činech.

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 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).

12 Nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 ze dne 20. prosince 2006 o přístupu subjektů odpovědných za vydávání osvědčení o registraci vozidel v členských státech k Schengenskému informačnímu systému druhé generace (SIS II) (Úř. věst. L 381, 28.12.2006, s. 1).

13 COM(2015) 185 final.

14 COM(2016) 230 final.

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

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

3) **Evropská pohraniční a pobřežní stráž**, pokud jde o její přístup do SIS pro účely navrhovaného evropského systému pro cestovní informace a povolení (ETIAS)[15] a 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 podpůrného týmu 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;

4) **Europol,** neboť tento návrh uděluje Europolu v rámci jeho mandátu další práva na přístup k údajům, které byly vloženy do SIS, a vyhledávání v nich.

5) Prümské rozhodnutí, neboť nová ustanovení tohoto návrhu umožňující určení totožnosti osob na základě otisků prstů (jakož i zobrazení obličeje a profilů DNA) doplňují stávající prümská ustanovení[16] o vzájemném přeshraničním on-line přístupu k určeným vnitrostátním databázím DNA a automatizovaných systémech pro identifikaci otisků prstů.

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

6) **Správa vnějších hranic**. Návrh doplňuje navrhovanou novou zásadu pro Schengenský hraniční kodex spočívající v systematických kontrolách všech cestujících, včetně občanů EU, na základě příslušných databází při vstupu do schengenského prostoru a výstupu z něj, která byla zavedena jako reakce na činnost zahraničních teroristických bojovníků.

7) **Systém vstupu/výstupu.** Návrh se snaží odrážet navrhované použití kombinace otisků prstů a zobrazení obličeje jako biometrických identifikátorů pro provoz systému vstupu/výstupu (EES).

8) **ETIAS.** Návrh zohledňuje navrhovaný systém ETIAS, jehož cílem je důkladné posouzení státních příslušníků třetích zemí, kteří chtějí do EU cestovat, z hlediska bezpečnosti, včetně jejich kontroly v SIS.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právní základ

Právním základem ustanovení tohoto návrhu, která se týkají policejní spolupráce a justiční spolupráce v trestních věcech, jsou čl. 82 odst. 1 písm. d), čl. 85 odst. 1, čl. 87 odst. 2 písm. a) a čl. 88 odst. 2 písm. a) Smlouvy o fungování Evropské unie.

---

15 COM(2016) 731 final.

16 Rozhodnutí Rady 2008/615/SVV ze dne 23. června 2008 o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti (Úř. věst. L 210, 6.8.2008, s. 1); rozhodnutí Rady 2008/616/SVV ze dne 23. června 2008 o provádění rozhodnutí 2008/615/SVV o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti (Úř. věst. L 210, 6.8.2008, s. 12).

- **Proměnná geometrie**

Tento návrh rozvíjí ustanovení schengenského *acquis* týkající se policejní spolupráce a justiční spolupráce v trestních věcech. 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: Podle článku 5 Protokolu o schengenském *acquis* začleněném do rámce Evropské unie, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, a podle čl. 8 odst. 2 rozhodnutí Rady 2000/365/ES ze dne 29. května 2000 o žádosti Spojeného království Velké Británie a Severního Irska, aby se na ně vztahovala některá ustanovení schengenského *acquis*[17], je toto nařízení pro Spojené království závazné.

Irsko: V souladu s článkem 5 Protokolu o schengenském *acquis* začleněném do rámce Evropské unie, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, a s čl. 6 odst. 2 rozhodnutí Rady 2002/192/ES ze dne 28. února 2002 o žádosti Irska, aby se na ně vztahovala některá ustanovení schengenského *acquis*[18], je toto nařízení pro Irsko závazné.

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

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

[18] Úř. věst. L 64, 7.3.2002, s. 20.

[19] 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).

Vysoké 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 týkající se policejní spolupráce a justiční spolupráce v trestních věcech.

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. Na základě posouzení operačních požadavků tento návrh omezuje dobu uchovávání záznamů o věcech a uvádí je do souladu se záznamy o osobách (neboť se často týkají osobních údajů, například osobních identifikačních dokladů nebo poznávacích značek). Policejní zkušenosti ukazují, že odcizený majetek lze vrátit během poměrně krátké doby, a desetiletá platnost záznamů o věcech je tudíž nepřiměřeně dlouhá.

Záznamy v SIS obsahují pouze údaje, které jsou potřebné pro určení totožnosti a nalezení osoby nebo věci a pro přijetí vhodného operativního opatření. Všechny další informace jsou poskytovány prostřednictvím center 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 podobu nařízení a nahradí rozhodnutí Rady 2007/533/JHA, přičemž velká část obsahu tohoto rozhodnutí zůstane zachována. 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 návrh 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[20] (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 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.

Výsledky hodnocení zdůraznily nutnost změnit právní základ SIS, aby mohl lépe reagovat na nové bezpečnostní a migrační výzvy. Sem patří například návrh na řešení komplexního (*end-to-end*) využívání SIS regulací jeho využití koncovými uživateli a stanovením norem pro ochranu údajů použitelných i na aplikace pro koncové uživatele, dále posílení systému pro účely boje proti terorismu prostřednictvím nových opatření, která mají být přijata, vyjasnění situace dětí, kterým hrozí únos jejich rodiči, jakož i rozšíření biometrických identifikátorů, které jsou v systému dostupné.

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.

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

---

[20] 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).

[21] 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.

- **Konzultace se zúčastněnými stranami**

V průběhu svého hodnocení SIS požádala Komise o zpětnou vazbu a návrhy příslušné zúčastněné strany, a to včetně členů výboru pro SISVIS postupem stanoveným v článku 67 rozhodnutí Rady 2007/533/SVV. 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 členové 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 členové 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 využívání SIS v praxi. Předmětem kontrol byla diskuse a pohovory s odborníky, zaměstnanci centrály SIRENE a příslušnými vnitrostátními orgány.

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 tří studií, jejichž výsledky byly při vypracovávání tohoto návrhu zohledněny:

- Technický posudek SIS (Kurt Salmon)[22]

  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)[23]

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

[23] *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).

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)[24]

  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).

- **Posouzení dopadů**

Komise neprovedla posouzení dopadů.

Tři nezávislá posouzení uvedená výše (v oddíle „Sběr a využití výsledků odborných konzultací“) 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[25] dne 29. ledna 2015. Komise rovněž přijala katalog osvědčených postupů a doporučení[26]. 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[27], 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

---

24 *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).

25 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).

26 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).

27 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).

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 pohřešovaných nezletilých. Dopad zmíněných 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 byly stanoveny jasné časové rámce pro uchovávání údajů, včetně zkrácení doby uchovávání záznamů o věcech. 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. Bude možné spolehlivěji určovat totožnost osob s využitím biometrických údajů pro pohřešované osoby, které potřebují ochranu, přičemž bude zajištěno, že jsou osobní údaje přesné a náležitě chráněné. Návrh také vymezuje rozsáhlé a pevné záruky pro používání biometrických identifikátorů, aby se předešlo nežádoucím důsledkům pro nevinné osoby.

Dále 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[28], pokud jde o 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 články 26, 32, 34 a 36. V budoucnu by mělo být možné porovnávat tyto

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

daktyloskopické údaje (otisky prstů a otisky dlaní) s otisky prstů nalezenými na místě činu v případě, že se jedná o závažný trestný čin či terorismus a s vysokou mírou pravděpodobnosti lze stanovit, že otisky patří pachateli. Návrh navíc stanoví uchovávání otisků prstů pro tzv. „neznámé hledané osoby“ (podmínky jsou podrobně popsány v oddílu 5 pododdílu „Fotografie, zobrazení obličeje, daktyloskopické údaje a profily DNA“). 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.

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 hraničních kontrol) 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 jeho 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[29]. 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

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

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[30]. 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.

5. OSTATNÍ PRVKY

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

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

Toto navrhované nařízení navíc v čl. 71 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 konkrétních ustanovení návrhu**

Ustanovení společná v tomto návrhu a návrhu nařízení o zřízení, provozu a využívání SIS v oblasti hraničních kontrol:

- Obecná ustanovení (články 1 až 3)
- Technická architektura a způsoby provozování SIS (články 4 až 14)
- Povinnosti agentury eu-LISA (články 15 až 18)

[30] 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).

- Právo na přístup a uchovávání záznamů (články 43, 46, 48, 50 a 51)
- Obecná pravidla pro zpracování údajů a ochranu údajů (články 53 až 70)
- Sledování a statistika (článek 71)

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, 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[31].

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 56). 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

[31] 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).

vypracovávala pro členské státy zprávy o kvalitě údajů. Tuto činnost může usnadnit úložiště údajů pro vypracovávání statistických zpráv a zpráv o kvalitě údajů (článek 71). Tato zlepšení zohledňují prozatímní zjištění expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu.

Fotografie, zobrazení obličeje, daktyloskopické údaje a profily DNA

Možnost vyhledávání s pomocí otisků prstů za účelem určení totožnosti určité osoby je již stanovena v článku 22 nařízení (ES) č. 1987/2006 a v rozhodnutí Rady 2007/533/SVV. Návrhy ukládají povinnost provést takovéto vyhledávání, jestliže nelze zjistit totožnost osoby jinými prostředky. Kromě toho změny článku 22 a nové články 40, 41 a 42 umožní použít k určení totožnosti osoby kromě otisků prstů i zobrazení obličeje, otisky dlaní a profily DNA . V současnosti může být zobrazení obličeje použito pouze k potvrzení totožnosti osoby nalezené na základě alfanumerického vyhledávání, ale nemůže sloužit jako základ pro vyhledávání. 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. Zde jsou dvě hlavní použití otisků dlaní:

i) identifikační účely v případě, že si subjekt úmyslně nebo neúmyslně poškodil konce prstů. Důvodem může být snaha vyhnout se určení totožnosti 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, hlásila Itálie značný úspěch při zjišťování totožnosti nelegálních migrantů, kteří si bříška prstů poškodili s úmyslem vyhnout se určení totožnosti. Odebírání otisků dlaní italským orgánům umožnilo následné určení totožnosti.

ii) Latentní otisky z místa činu. Podezřelý často zanechá na místě činu stopy, které se ukáží být otisky dlaní rukou. Pouze díky rutinnímu odebírání otisků dlaní, když jsou osobě oprávněně odebírány otisky prstů, lze určit totožnost podezřelého. Otisk dlaně také obvykle obsahuje detailní otisk prstu v celé délce, který často chybí u válených a píchaných otisků prstů, neboť ty se zpravidla zaměřují na konce a poslední články prstů.

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.

V případech, kdy otisky prstů nebo dlaní nejsou k dispozici, čl. 22 odst. 1 písm. b) umožňuje použití profilů DNA pro pohřešované osoby, které musí být umístěny pod ochranu, zejména děti. Tato funkce se použije pouze při neexistenci otisků prstů a bude k dispozici pouze oprávněným uživatelům. Toto ustanovení tedy umožňuje použití profilů DNA pohřešované osoby/dítěte prostřednictvím jejích rodičů nebo sourozenců, což vnitrostátním orgánům umožní určit totožnost dané osoby a vyhledat ji. Členské státy si již tyto informace mezi sebou na operační úrovni vyměňují, a to prostřednictvím výměny doplňujících informací. Tento návrh vytváří právní rámec pro tuto praxi tím, že ji vkládá do vlastního právního základu pro provoz a využívání SIS a že zavádí jasné postupy s ohledem na podmínky, za kterých mohou být tyto profily použity.

Navrhované změny umožní pořizovat záznamy do SIS pro neznámé osoby hledané v souvislosti s trestným činem na základě otisků prstů nebo dlaní (články 40–42). Tyto záznamy mohou být vytvořeny, pokud byly například na místě závažného trestného činu

nalezeny latentní otisky prstů nebo dlaní a pokud existují pádné důvody se domnívat, že tyto otisky patří pachateli uvedeného trestného činu. Například v případě, že jsou otisky prstů nalezeny na zbrani použité při spáchání trestného činu nebo na jakémkoli jiném předmětu, který pachatel při spáchání trestného činu použil. Tato nová kategorie záznamů doplňuje prümská ustanovení, jež umožňují propojení vnitrostátních systémů identifikace podle otisků prstů v oblasti vyšetřování trestné činnosti. Prostřednictvím prümského mechanismu může členský stát podat žádost, aby zjistil, zda je pachatel trestného činu, jehož otisky prstů byly nalezeny, znám v jakémkoli jiném členském státě (obvykle pro účely vyšetřování). Totožnost určité osoby lze určit prostřednictvím prümského mechanismu pouze tehdy, pokud jí byly sejmuty otisky prstů v jiném členském státě pro účely trestního řízení. Totožnost pachatelů, kteří nikdy předtím trestný čin nespáchali, tak nelze určit. Změna obsažená v tomto návrhu, tedy uchovávání otisků prstů neznámé hledané osoby, umožní vložit otisky prstů neznámého pachatele do SIS, tak aby tento pachatel mohl být identifikován jako hledaná osoba, pokud bude nalezen v jiném členském státě. Použití této funkce předpokládá, že členské státy předběžně konzultovaly všechny dostupné vnitrostátní a mezinárodní zdroje, ale totožnost dotčené osoby nezjistily. Tento návrh obsahuje dostatečné záruky, které zajistí, že do SIS budou vloženy pouze otisky prstů osob, které jsou důvodně podezřelé ze spáchání závažného trestného činu nebo teroristického trestného činu. Proto je použití této nové kategorie záznamů přípustné pouze v případech, kdy neznámý pachatel představuje závažnou hrozbu pro veřejnou bezpečnost, která odůvodňuje porovnání těchto otisků s otisky prstů cestujících, aby se například zabránilo tomu, že dotčená osoba opustí prostor bez kontrol na vnitřních hranicích.

Toto ustanovení neumožňuje koncovým uživatelům vložit otisky prstů v této kategorii, u nichž nelze zjistit vztah k pachateli. Další podmínkou je, že totožnost osoby nemůže být určena za použití jiné vnitrostátní, evropské nebo mezinárodní databáze, ve které jsou uloženy otisky prstů. Jakmile budou tyto otisky prstů vloženy do SIS, budou použity k určení totožnosti osob, jejichž totožnost nelze určit jiným způsobem. Pokud by se na základě této kontroly zjistila možná shoda, měl by daný členský stát provést další kontrolu s jejich otisky prstů, případně se zapojením odborníků na otisky prstů, s cílem zjistit, zda je daná osoba vlastníkem otisků uložených v SIS, a měl by určit totožnost osoby. Příslušné postupy jsou upraveny vnitrostátními právními předpisy. Určení totožnosti osoby odpovídající „neznámé hledané osobě“ v SIS může vést k jejímu zatčení.

Přístup k SIS

Tento pododdíl popisuje nové prvky, pokud jde přístupová práva do SIS týkající se příslušných vnitrostátních orgánů a agentur EU (institucionálních uživatelů).

Vnitrostátní orgány – imigrační orgány

Aby bylo zajištěno co nejefektivnější využití SIS, návrh umožňuje přístup do systému SIS vnitrostátním orgánům odpovědným za přezkoumávání podmínek a přijímání rozhodnutí týkajících se vstupu a pobytu státních příslušníků třetích zemí na území členských států a jejich navracení. Toto doplnění umožní nahlédnout do SIS, pokud jde o nelegální migranty, kteří nebyli zkontrolováni při pravidelných hraničních kontrolách. Tento návrh zajišťuje stejné zacházení se státními příslušníky třetích zemí, kteří přecházejí vnější hranice na řádných hraničních přechodech (a podléhají tedy kontrolám ve vztahu ke státním příslušníkům třetích zemí) i se státními příslušníky třetích zemí, kteří se dostali do schengenského prostoru nelegálně.

Tento návrh nadto zaručuje, že orgány příslušné pro registraci vozidel (článek 44), plavidel a letadel budou mít omezený přístup do systému, aby mohly plnit své úkoly, za předpokladu, že jsou státními subjekty. To pomůže zabránit registracím uvedených dopravních prostředků,

pokud byly odcizeny a hledají se v jiných členských státech. Tato iniciativa není nová, pokud jde o subjekty příslušné pro registraci vozidel, neboť ty mají přístup do SIS již podle článku 102a Schengenské úmluvy a podle nařízení (ES) č. 1986/2006[32]. Podle stejné logiky návrh stanoví přístup k záznamům v SIS týkajícím se plavidel a letadel pro orgány příslušné pro registraci lodí a letadel.

Institucionální uživatelé

Přístup do SIS a k údajům v něm uloženým, který potřebují ke své práci, mají Europol (článek 46), Eurojust (článek 47) a Evropská agentura pro pohraniční a pobřežní stráž, jakož i její jednotky, týmy pracovníků, kteří se podílejí na úkolech spojených s navracením, a členové podpůrného týmu pro řízení migrace (články 48 a 49). Zavádějí se odpovídající záruky s cílem zabezpečit řádnou ochranu údajů v systému (což zahrnuje i ustanovení v článku 50, 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 pohřešovaných osobách, 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. V rámci činnosti expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu a s cílem dále posílit sdílení informací týkajících se terorismu Komise posoudí, zda by měl Europol automaticky dostávat oznámení ze systému SIS, je-li vytvořen záznam týkající se činnosti související s terorismem.

Podle návrhu nařízení Evropského parlamentu a Rady, kterým se zřizuje evropský systém pro cestovní informace a povolení (ETIAS)[33], předloženého Komisí, bude navíc ústřední jednotka ETIAS v rámci Evropské agentury pro pohraniční a pobřežní stráž vyhledávat v SIS prostřednictvím ETIAS, aby zjistila, zda státní příslušník třetí země, který žádá o cestovní povolení, není předmětem záznamu v SIS. K tomuto účelu bude mít ústřední jednotka ETIAS také plný přístup do SIS.

Zvláštní změny záznamů

Článek 26 stanoví, že členské státy mají pozastavit platnost záznamů za účelem zatčení (v případě probíhajícího policejního vyšetřování nebo operace), takže budou během omezeného časového období viditelné pouze pro centrály SIRENE, avšak nikoli pro pracovníky v terénu. Toto ustanovení umožňuje zabránit tomu, aby důvěrnou policejní operaci vedoucí k zatčení intenzivně hledaného pachatele trestné činnosti ohrozil policista, který do ní není zapojen.

Články 32 a 33 upravují záznamy o pohřešovaných osobách. Jejich změny umožňují pořídit preventivní záznamy v případech, kdy je vysoké riziko únosu dítěte rodičem, a stanoví přesněji vymezenou kategorizaci záznamů o pohřešovaných osobách. K rodičovským únosům často dochází za podrobně naplánovaných okolností s úmyslem rychle opustit členský stát, kde byla dohodnuta ujednání o péči o dítě. Tyto změny řeší případnou mezeru ve stávající právní úpravě, podle níž mohou být záznamy o dětech pořízeny až v okamžiku, kdy se

[32] Nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 ze dne 20. prosince 2006 o přístupu subjektů odpovědných za vydávání osvědčení o registraci vozidel v členských státech k Schengenskému informačnímu systému druhé generace (SIS II) (Úř. věst. L 381, 28.12.2006, s. 1).

[33] COM (2016) 731 final.

pohřešují. Orgánům členských států tak bude umožněno určit vysoce ohrožené děti. Tyto změny budou znamenat, že tam, kde je bezprostřední vysoké riziko rodičovského únosu, budou pohraniční stráž a donucovací orgány o tomto riziku informovány, budou moci důkladněji přezkoumat okolnosti, za nichž ohrožené dítě cestuje, a v případě potřeby vezmou dítě do ochranné péče. Doplňující informace, včetně informací o rozhodnutí příslušného soudního orgánu, který požadoval pořízení záznamu, budou poskytnuty prostřednictvím centrál SIRENE. Příručka SIRENE bude příslušným způsobem upravena. Tento záznam bude vyžadovat odpovídající rozhodnutí soudních orgánů o poskytnutí péče pouze jednomu z rodičů. Další podmínkou bude bezprostřední riziko únosu. Status záznamu o pohřešovaném dítěti se bude automaticky aktualizovat tak, aby odrážel dosažení jejich případné zletilosti.

Článek 34 umožňuje doplnit do záznamu údaje o vozidlech, jestliže existuje důvodné podezření, že souvisejí s hledanou osobou.

Článek 37 zavádí nový druh kontroly, „vyšetřovací kontrolu“. Ta je zamýšlena zejména jako podpora pro opatření v boji proti terorismu a závažné trestné činnosti. Umožňuje orgánům zadržet a vyslechnout dotyčnou osobu. Je podrobnější než stávající skrytá kontrola, ale nezahrnuje hledání osoby a jejím výsledkem není zatčení dotyčné osoby. Může však poskytnout dostatek informací k rozhodnutí o dalších krocích, které je třeba podniknout. Článek 36 se rovněž mění tak, aby odrážel tento další druh kontroly.

Tento návrh obsahuje ustanovení o záznamech v SIS týkajících se nevyplněných úředních dokladů a vydaných dokladů totožnosti (článek 36) a vozidel, včetně plavidel a letadel (články 32, 34), jestliže souvisejí se záznamy o lidech pořízenými podle těchto článků. Článek 37 se mění s cílem stanovit opatření, která mají být přijata na základě těchto záznamů. Účel je čistě vyšetřovací, neboť to umožní orgánům řešit situace, kdy několik osob používá pravé doklady podobného vzhledu, avšak nejsou jejich zákonnými držiteli.

Článek 38 stanoví rozšířený seznam věcí, pro které lze pořídit záznam, a doplňuje padělané doklady, vozidla bez ohledu na systém pohonu (například elektrický, jakož i benzinový/naftový atd.), padělané bankovky, vybavení IT a identifikovatelné součásti vozidel a průmyslových zařízení. Neobsahuje již záznamy o platebních nástrojích, jelikož účinnost těchto záznamů byla vždy velmi nízká a málokdy vedla k pozitivním nálezům.

S cílem zpřesnit postup, kterým je třeba se řídit po nalezení věci, jež je předmětem záznamu, se mění článek 39 v tom smyslu, že kromě kontaktování orgánu, který záznam pořídil, musí být věci zabaveny.

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 57).

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

Článek 12 také zahrnuje ustanovení týkající se automatizovaného skenovacího vyhledávání registračních značek motorových vozidel, s použitím systémů automatického rozpoznávání registračních značek, která členským státům ukládají povinnost uchovávat protokoly těchto vyhledávání v souladu s vnitrostátními právními předpisy.

V čl. 15 odst. 3 se zachovává čl. 15 odst. 3 rozhodnutí Rady 2007/533/SVV 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 posoudit, zda je případ dostatečně relevantní, odpovídající a důležitý, i na rozhodnutí o prodloužení či neprodloužení doby platnosti záznamu. Nově tento článek ukládá členským státům také povinnost vytvořit za všech okolností záznam podle článků 34, 36 a 38 (podle situace) o osobách či s nimi souvisejících věcech, 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

Tento návrh rozšiřuje druhy informací (článek 20), které mohou být uchovávány o osobách, o kterých byl pořízen záznam, a to o tyto druhy:

- údaj, zda se dotčená osoba účastní činnosti uvedené v článcích 1, 2, 3 a 4 rámcového rozhodnutí Rady 2002/475/SVV,
- ostatní poznámky o dané osobě; důvody pořízení záznamu,
- podrobné údaje o vnitrostátním registračním čísle osoby a místě registrace,
- kategorizaci typu případu pohřešované osoby (pouze záznamy podle článku 32),
- informace z dokladu totožnosti nebo cestovního dokladu,
- barevnou kopii dokladu totožnosti nebo cestovního dokladu,
- profily DNA (pouze pokud nejsou k dispozici otisky prstů vhodné pro určení totožnosti).

Článek 59 rozšiřuje seznam osobních údajů, které mohou být vloženy a zpracovány v SIS pro účely řešení zneužití totožnosti. Tyto údaje mohou být vloženy pouze se souhlasem oběti zneužití totožnosti. 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. Patří mezi ně podrobnosti o dokladech totožnosti subjektů údajů, včetně možnosti kategorizovat pohřešované děti podle jejich zmizení, jako jsou nezletilé osoby bez doprovodu, rodičovský únos, útěky atd. To je zásadní pro koncové uživatele, aby mohli neprodleně přijmout potřebná opatření na ochranu takových dětí. Rozšířené údaje umožňují lepší určování totožnosti dotčených osob, 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[34].

Návrh jasně uvádí, že členské státy nesmějí kopírovat údaje vložené jiným členským státem do jiných vnitrostátních souborů údajů (článek 53).

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

Uchovávání

Maximální doba uchování záznamu o osobách bude prodloužena na pět let, s výjimkou záznamů pro účely skrytých, vyšetřovacích nebo zvláštních kontrol, kde tato doba zůstává jeden rok. Členské státy mohou kdykoli stanovit kratší doby platnosti. Prodloužení maximální délky platnosti se řídí vnitrostátními postupy prodloužení platnosti, jestliže záznam dosud nesplnil svůj účel a dotyčná osoba je nadále hledaná. Kromě toho je nezbytné sladit SIS s dobou uchovávání údajů u jiných nástrojů, jako je směrnice o navracení a Eurodac. V zájmu transparentnosti a jasnosti je třeba stanovit stejnou dobu uchovávání záznamů o osobách, s výjimkou záznamů vytvořených pro účely skrytých, vyšetřovacích nebo zvláštních kontrol. Prodloužení doby uchovávání není na újmu zájmům subjektů údajů, neboť záznam nemůže být uchováván déle, než je k jeho účelu nezbytné. Pravidla pro výmaz záznamů byla výslovně stanovena v článku 52. Článek 51 stanoví lhůtu pro přezkum záznamů a zahrnuje zejména omezenou dobu uchovávání záznamů o věcech. Vzhledem k neexistenci operativní potřeby zachovat delší dobu pro věci byla tato doba nyní omezena na pět let, aby bylo dosaženo souladu s dobou uchovávání údajů o osobách. Doba platnosti pro vydané a nevyplněné doklady nicméně zůstává 10 let, neboť doba platnosti dokumentů je 10 let.

Výmaz

Článek 52 vymezuje, za jakých okolností musí být záznamy vymazány, a tak zajišťuje větší harmonizaci vnitrostátních postupů v této oblasti. Článek 51 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[35] a směrnicí 2016/680[36]. Článek 63 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.

Sdílení údajů o ztracených, odcizených, neplatných a neoprávněně užívaných dokladech s Interpolem

Článek 63 plně zachovává znění článku 55 rozhodnutí Rady 2007/533/JHA, neboť lepší interoperabilita mezi oddílem dokladů SIS a databází odcizených a ztracených dokladů Interpolu bude předmětem sdělení expertní skupiny na vysoké úrovni a druhého souboru návrhů ohledně SIS v červnu 2017.

Statistika

Aby byl zachováván přehled o fungování opravných prostředků v praxi, stanoví článek 66 standardní statistický systém, který umožní vypracovávat roční zprávy o těchto údajích:

- počet žádostí subjektů údajů o přístup,

[35] 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).

[36] 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).

- 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 71 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. 71 odst. 5 musí agentura eu-LISA postoupit členským státům, Komisi, Europolu a Evropské agentuře pro pohraniční a pobřežní stráž statistické zprávy, které vypracuje, a Komise může tuto agenturu požádat o další statistické zprávy a zprávy o kvalitě údajů týkající se SIS a komunikace prostřednictvím center SIRENE.

Podle čl. 71 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, Eurojustu a Evropské agentury pro pohraniční a pobřežní stráž tak získají přístup k údajům vymezeným v čl. 71 odst. 3, což umožní zpracování požadovaných statistik.

2016/0409 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, o změně nařízení (EU) č. 515/2014 a o zrušení nařízení (ES) č. 1986/2006, rozhodnutí Rady 2007/533/SVV a rozhodnutí Komise 2010/261/EU

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na čl. 82 odst. 1 druhý pododstavec písm. d), čl. 85 odst. 1, čl. 87 odst. 2 písm. a) a čl. 88 odst. 2 písm. a) 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 a policejními, celními a dalšími donucovacími a justičními orgány v trestních věcech.

(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[37] (dále jen „Schengenská úmluva“). Vývoj SIS druhé generace (dále jen „SIS II“) byl svěřen Komisi na základě nařízení Rady (ES) č. 2424/2001[38] a rozhodnutí Rady 2001/886/SVV[39] a tento systém byl zřízen nařízením (ES) č. 1987/2006[40] a rozhodnutím Rady 2007/533/SVV[41]. SIS II nahradil SIS vytvořený na základě Schengenské úmluvy.

---

37 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).

38 Úř. věst. L 328, 13.12.2001, s. 4.

39 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).

40 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[42]. 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 kapitol 4 a 5 Smlouvy o fungování Evropské unie. Nařízení Evropského parlamentu a Rady (EU) 2018/… o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol[43] představuje nezbytný právní základ pro řízení SIS v souvislosti se záležitostmi spadajícími do oblasti působnosti hlavy V kapitoly 2 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[44]

---

41 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).

42 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.…).

43 Nařízení (EU) 2018/...

44 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 trestnou činnost, 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. Za účelem snazšího určování totožnosti osob a odhalování vícenásobných identit by proto měly kategorie údajů týkajících se osob obsahovat 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[45]. 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 otisků prstů a zobrazení obličeje. V případě jakýchkoli pochybností o totožnosti dané osoby by vyhledávání pomocí daktyloskopických údajů mělo být povinné. Zobrazení obličeje

[45] 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 měla být používána za účelem určení totožnosti pouze v rámci běžných hraničních kontrol prováděných v samoobslužných kioscích a elektronických branách.

(18) Zavedení služby automatizované identifikace otisků prstů v rámci SIS doplňuje stávající prümský mechanismus pro vzájemný přeshraniční on-line přístup do určených vnitrostátních databází DNA a automatizovaných systémů identifikace otisků prstů[46]. Prümský mechanismus umožňuje propojení vnitrostátních systémů identifikace otisků prstů, díky němuž může členský stát podat žádost s cílem zjistit, zda pachatel trestného činu, jehož otisky prstů byly nalezeny, je znám v jakémkoli jiném členském státě. Prümský mechanismus ověřuje, zda je vlastník otisků prstů znám v určitém momentě, takže pokud se pachatel stane v některém členském státě známým později, nemusí být nutně dopaden. Vyhledávání otisků prstů v SIS umožňuje aktivně vyhledávat pachatele. Proto by mělo být možné vkládat do SIS otisky prstů neznámého pachatele, a to za předpokladu, že vlastníka otisků prstů lze s vysokou pravděpodobností označit za pachatele závažného trestného činu nebo teroristického činu. Jde zejména o případy, kdy jsou otisky prstů nalezeny na zbrani nebo jakémkoli jiném předmětu použitém při spáchání daného trestného činu. Pouhý výskyt otisků prstů na místě činu by neměl být považován za znamení, že jde o s vysokou pravděpodobností o otisky prstů pachatele. Další podmínkou pro vytvoření takového záznamu je, že totožnost pachatele nemůže být určena prostřednictvím jiných vnitrostátních, evropských a mezinárodních databází. Pokud by se na základě tohoto vyhledávání otisků prstů zjistila možná shoda, měl by daný členský stát provést další kontrolu s jejich otisky prstů, případně se zapojením odborníků na otisky prstů, s cílem zjistit, zda je daná osoba vlastníkem otisků uložených v SIS, a měl by určit totožnost osoby. Příslušné postupy by měly být upraveny vnitrostátními právními předpisy. Identifikace vlastníka jako „neznámé hledané osoby“ v SIS může podstatně přispět k vyšetřování a může vést k zatčení za předpokladu, že jsou splněny všechny podmínky pro zatčení.

(19) Mělo by být umožněno porovnávání otisků prstů nalezených na místě činu s otisky prstů 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[47] a „teroristickým trestným činem“ je třeba rozumět trestné činy podle vnitrostátního práva uvedené v rámcovém rozhodnutí Rady 2002/475/SVV[48].

(20) Mělo by být možné přidat profil DNA v případech, kdy nejsou k dispozici žádné daktyloskopické údaje, a tyto profily by měly být dostupné pouze oprávněným uživatelům. Profily DNA by měly usnadnit určování totožnosti pohřešovaných osob, které potřebují ochranu, a zejména pohřešovaných dětí, a to mimo jiné tím, že bude možné k určení totožnosti použít profily DNA rodičů či sourozenců. Údaje o DNA by neměly obsahovat informaci o rasovém původu.

---

[46] Rozhodnutí Rady 2008/615/SVV ze dne 23. června 2008 o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti (Úř. věst. L 210, 6.8.2008, s. 1); rozhodnutí Rady 2008/616/SVV ze dne 23. června 2008 o provádění rozhodnutí 2008/615/SVV o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti (Úř. věst. L 210, 6.8.2008, s. 12).

[47] 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).

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

(21) SIS by měl obsahovat záznamy o osobách hledaných za účelem zatčení a předání a hledaných za účelem zatčení a vydání. Je vhodné, aby byla kromě záznamů umožněna i výměna doplňujících informací nezbytných pro postupy předávání a vydávání. V SIS by se měly zpracovávat zejména údaje uvedené v článku 8 rámcového rozhodnutí Rady 2002/584/SVV ze dne 13. června 2002 o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy[49]. Z operativních důvodů je vhodné, aby členský stát, který záznam pořídil, s povolením soudních orgánů dočasně skryl stávající záznam za účelem zatčení v případě, že je osoba, na niž je vydán evropský zatýkací rozkaz, intenzivně a aktivně hledána a koncoví uživatelé, kteří nejsou zapojeni do konkrétní pátrací akce, by mohli ohrozit její úspěšný výsledek. Dočasná nedostupnost těchto záznamů by neměla přesáhnout 48 hodin.

(22) Mělo by být možné doplnit do SIS překlad dalších údajů vložených za účelem předání v rámci evropského zatýkacího rozkazu a za účelem vydání.

(23) SIS by měl obsahovat záznamy o pohřešovaných osobách k zajištění jejich ochrany nebo předcházení ohrožení veřejné bezpečnosti. Pořizování záznamů v SIS o dětech, kterým hrozí únos (t.j. s cílem zabránit budoucím škodám, ke kterým doposud nedošlo, například v případě dětí, u nichž je riziko únosu dítěte jedním z jeho rodičů), by mělo být omezeno, a proto je vhodné stanovit přísné a přiměřené záruky. V případech dětí by tyto záznamy a příslušné postupy měly sloužit nejvlastnějším zájmům dítěte s ohledem na článek 24 Listiny základních práv Evropské unie a na Úmluvu Organizace spojených národů o právech dítěte ze dne 20. listopadu 1989.

(24) Mělo by být zavedeno nové opatření pro případy podezření z terorismu nebo závažné trestné činnosti, které by umožňovalo zadržet a vyslechnout osobu podezřelou ze spáchání závažného trestného činu, nebo pokud existuje důvod domnívat se, že spáchá závažný trestný čin, s cílem poskytnout co nejpodrobnější informace členskému státu, který pořídil příslušný záznam. Toto nové opatření by nemělo vést ani k hledání dané osoby, ani k jejímu zatčení. Mělo by však poskytnout dostatek informací k rozhodnutí o dalších krocích. Za závažnou trestnou činnost by měly být považovány činy uvedené v rámcovém rozhodnutí Rady 2002/584/SVV.

(25) SIS by měl obsahovat nové kategorie věcí s vysokou hodnotou, jako je elektronické a technické vybavení, které lze identifikovat a vyhledávat pomocí jedinečného čísla.

(26) Členský stát by měl mít možnost opatřit záznam návěstím zvaným označení, v jehož důsledku opatření, které má být přijato na základě záznamu, nebude přijato na jeho území. Pokud se pořizují záznamy za účelem zatčení a předání, nesmí být žádné ustanovení tohoto nařízení vykládáno v tom smyslu, že se odchyluje od ustanovení uvedených v rámcovém rozhodnutí 2002/584/SVV nebo že brání jejich použití. Rozhodnutí o označení by se mělo zakládat pouze na důvodech zamítnutí uvedených ve zmíněném rámcovém rozhodnutí.

(27) Pokud byl záznam označen a pokud se zjistí místo pobytu osoby hledané za účelem zatčení a předání, mělo by být toto místo pobytu vždy sděleno vystavujícímu justičnímu orgánu, který může rozhodnout o předání evropského zatýkacího rozkazu příslušnému justičnímu orgánu v souladu s ustanoveními rámcového rozhodnutí 2002/584/SVV.

---

[49] 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).

(28) 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.

(29) Záznamy by v SIS měly být uchovávány nanejvýš po dobu nezbytnou pro splnění účelů, pro které byly pořízeny. Za účelem snížení administrativní zátěže pro různé orgány, které se zabývají zpracováváním údajů o jednotlivcích k různým účelům, je třeba sladit dobu uchovávání záznamů o osobách s dobou uchovávání záznamů pro účely navracení a neoprávněného pobytu. Členské státy navíc pravidelně prodlužují dobu platnosti záznamů o osobách, pokud požadované opatření nemohlo být realizováno v původně stanovené lhůtě. Proto by doba uchovávání záznamů o osobách měla činit nejvýše pět let. Obecnou zásadou by mělo být, že se záznamy o osobách ze SIS automaticky vymažou po uplynutí pěti let, s výjimkou záznamů pořízených pro účely skrytých, vyšetřovacích nebo zvláštních kontrol. Ty by měly být vymazány po jednom roce. Záznamy o věcech pořízené pro účely skrytých, vyšetřovacích nebo zvláštních kontrol by měly být ze SIS automaticky vymazány po uplynutí jednoho roku, neboť se vždy vztahují k osobám. Záznamy o věcech hledaných za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení by měly být ze SIS automaticky vymazány po uplynutí pěti let, neboť po uplynutí této doby je pravděpodobnost jejich nalezení velmi nízká a jejich ekonomická hodnota významně snížená. Záznamy o vydaných a nevyplněných dokladech totožnosti by měly být uchovávány po dobu 10 let, neboť platnost dokladů je 10 let od okamžiku vydání. 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.

(30) 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. Trestné činy podle článků 1, 2, 3 a 4 rámcového rozhodnutí Rady 2002/475/SVV o boji proti terorismu[50] představují velmi závažnou hrozbu pro veřejnou bezpečnost a integritu života jednotlivců i společnosti a je mimořádně obtížné těmto činům předcházet, odhalovat je a vyšetřovat je v prostoru bez vnitřních hranic, kde se mohou potenciální pachatelé volně pohybovat. Pokud se hledá osoba nebo věc v souvislosti s těmito trestnými činy, je nezbytné vytvořit odpovídající záznam v SIS o osobách hledaných za účelem soudního řízení, o osobách nebo věcech hledaných za účelem skrytých, vyšetřovacích nebo zvláštních kontrol, jakož i o věcech hledaných za účelem zabavení, protože žádný jiný způsob by nebyl pro tento účel stejně účinný.

(31) Je třeba zajistit jasnost ohledně výmazu záznamů. Záznam by měl být uchováván pouze po dobu nezbytnou pro dosažení účelu, pro nějž byl vložen. S ohledem na různé postupy členských států při definování okamžiku, kdy záznam splnil svůj účel, je vhodné u každé kategorie záznamů stanovit podrobná kritéria, aby se určilo, kdy by záznam měl být vymazán ze SIS.

(32) Neporušenost údajů SIS má prvořadý význam. Proto by měly být stanoveny odpovídající záruky pro zpracování údajů SIS na centrální i na vnitrostátní úrovni s

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

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.

(33) Údaje zpracovávané v SIS za použití tohoto nařízení by neměly být poskytovány ani zpřístupňovány žádným třetím zemím nebo mezinárodním organizacím. Je však vhodné posílit spolupráci mezi Evropskou unií a Interpolem prostřednictvím podpory účinné výměny údajů o pasech. Pokud se Interpolu předávají osobní údaje ze SIS, tyto osobní údaje by měly podléhat odpovídající úrovni ochrany zaručené dohodou stanovící přísné záruky a podmínky.

(34) Je vhodné udělit přístup do SIS orgánům odpovědným za registraci vozidel, plavidel a letadel, aby mohly tyto orgány ověřit, zda se dopravní prostředek již nehledá v členských státech za účelem zabavení nebo kontroly. Přímý přístup by měl být poskytnut státním subjektům. Tento přístup by měl být omezen na záznamy o příslušných dopravních prostředcích a jejich registračních dokladech či značkách. Proto by do tohoto nařízení měla být zahrnuta ustanovení nařízení Evropského parlamentu a Rady (ES) č. 1986/2006[51], které by mělo být zrušeno.

(35) Na zpracování osobních údajů příslušnými vnitrostátními orgány za účelem prevence, vyšetřování a odhalování trestných činů nebo teroristických trestných činů či stíhání trestných činů a výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, by se měly vztahovat vnitrostátní předpisy provádějící směrnici (EU) 2016/680. Je-li to potřebné, měla by být ustanovení nařízení Evropského parlamentu a Rady (EU) 2016/679[52] a směrnice (ES) č. 2016/680 v tomto nařízení blíže upřesněna.

(36) Na zpracování osobních údajů vnitrostátními orgány podle tohoto nařízení by se mělo použít nařízení (EU) 2016/679, pokud se nepoužije směrnice (EU) 2016/680. 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[53].

(37) 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 (nařízení o Europolu)[54].

---

51 Nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 ze dne 20. prosince 2006 o přístupu subjektů odpovědných za vydávání osvědčení o registraci vozidel v členských státech k Schengenskému informačnímu systému druhé generace (SIS II) (Úř. věst. L 381, 28.12.2006, s. 1).

52 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).

53 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).

54 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).

(38) Na zpracování údajů SIS Eurojustem se vztahují ustanovení rozhodnutí 2002/187/SVV ze dne 28. února 2002[55] o zřízení Evropské jednotky pro justiční spolupráci (Eurojust) za účelem posílení boje proti závažné trestné činnosti, která se týkají ochrany údajů, včetně pravomocí společného kontrolního orgánu zřízeného podle uvedeného rozhodnutí sledovat činnosti Eurojustu a odpovědnosti za jakékoliv protiprávní zpracování osobních údajů ze strany Eurojustu. V případech, kdy vyhledávání provedená Eurojustem v SIS odhalí existenci záznamu pořízeného členským státem, nemůže Eurojust přijmout požadované opatření. Měl by proto uvědomit dotčený členský stát, aby tento členský stát mohl na případu dále pracovat.

(39) 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.

(40) 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.

(41) 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.

(42) 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.

(43) 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. Rozšíření práv přístupu Europolu k záznamům SIS o pohřešovaných osobách by mělo dále zlepšit schopnost Europolu poskytovat vnitrostátním donucovacím orgánům komplexní operační a analytické produkty týkající se obchodování s lidmi a pohlavního vykořisťování dětí, a to i on-line. To by přispělo k lepší prevenci těchto trestných činů, ochraně případných obětí a k vyšetřování pachatelů. Z nového přístupu Europolu k záznamům SIS o pohřešovaných osobách by mělo prospěch také Evropské centrum pro boj proti kyberkriminalitě při Europolu, a to včetně případů cestujících sexuálních delikventů a pohlavního zneužívání dětí na internetu, kde pachatelé často tvrdí, že mají nebo mohou získat přístup k dětem, které mohou být vedeny jako pohřešované. Navíc vzhledem k tomu, že hraje důležitou strategickou úlohu v boji proti zprostředkovávání nelegální migrace, mělo by získat přístup k záznamům o osobách, kterým byl odepřen vstup nebo pobyt na území členského státu buď z trestních důvodů, nebo kvůli

[55] Rozhodnutí Rady 2002/187/SVV ze dne 28. února 2002 o zřízení Evropské jednotky pro soudní spolupráci (Eurojust) za účelem posílení boje proti závažné trestné činnosti (Úř. věst. L 63, 6.3.2002, s. 1).

nedodržení podmínek vstupu a pobytu, i Evropské středisko pro boj proti převaděčství zřízené při Europolu.

(44) 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.

(45) 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.

(46) Nařízení Evropského parlamentu a Rady (EU) 2016/1624[56] stanoví pro účely tohoto nařízení, že hostitelský členský stát může zmocnit 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 kontroly, 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 podpůrného týmu pro řízení migrace je poskytnout technickou a operativní posilu žádajícím členským státům, zejména těm, které čelí nepřiměřeným migračním výzvám. Jednotky Evropské pohraniční a pobřežní stráže, týmy pracovníků, kteří se podílejí na úkolech spojených s navracením, a podpůrný tým pro řízení migrace potřebují pro plnění úkolů, které jim byly svěřeny, přístup do SIS přes technické rozhraní Evropské agentury pro pohraniční a pobřežní stráž propojené s centrálním 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.

(47) Podle návrhu nařízení Evropského parlamentu a Rady, kterým se zřizuje evropský systém pro cestovní informace a povolení (ETIAS)[57], předloženého Komisí, bude 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

[56] 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).

[57] COM (2016) 731 final.

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 rovněž měla mít přístup k údajům SIS v rozsahu nezbytném k plnění svého mandátu, a to pro všechny kategorie záznamů o osobách a záznamů týkajících nevyplněných a vydaných dokladů totožnosti.

(48) 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, specifikaci nových kategorií záznamů o věcech v rámci kategorie technického a elektronického vybavení, 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.

(49) 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[58]. Postup pro přijímání prováděcích opatření podle tohoto nařízení a nařízení (EU) 2018/xxx (o hraničních kontrolách) by měl být totožný.

(50) 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.

(51) 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.

(52) 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 zvláštní ochranu pro děti, které by se mohly stát obětí obchodování s lidmi nebo rodičovského únosu, a to při plném dodržování ochrany osobních údajů.

(53) V souladu s články 1 a 2 Protokolu č. 22 o postavení Dánska, připojeného ke Smlouvě o Evropské unii a 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.

---

[58] 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).

(54) Spojené království se účastní tohoto nařízení podle článku 5 Protokolu o schengenském *acquis* začleněném do rámce Evropské unie, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, a podle čl. 8 odst. 2 rozhodnutí Rady 2000/365/ES ze dne 29. května 2000 o žádosti Spojeného království Velké Británie a Severního Irska, aby se na ně vztahovala některá ustanovení schengenského *acquis*[59].

(55) Irsko se účastní tohoto nařízení v souladu s článkem 5 Protokolu o schengenském *acquis* začleněném do rámce Evropské unie, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, a s čl. 6 odst. 2 rozhodnutí Rady 2002/192/ES ze dne 28. února 2002 o žádosti Irska, aby se na ně vztahovala některá ustanovení schengenského *acquis*[60].

(56) 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*[61], která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí Rady 1999/437/ES[62] o některých opatřeních pro uplatňování dané dohody.

(57) 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[63] a rozhodnutí Rady 2004/860/ES[64].

(58) Pokud jde o Lichtenštejnsko, rozvíjí toto nařízení 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*[65], která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí 1999/437/ES ve

---

59 Úř. věst. L 131, 1.6.2000, s. 43.

60 Úř. věst. L 64, 7.3.2002, s. 20.

61 Úř. věst. L 176, 10.7.1999, s. 36.

62 Úř. věst. L 176, 10.7.1999, s. 31.

63 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).

64 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).

65 Úř. věst. L 160, 18.6.2011, s. 21.

spojení s článkem 3 rozhodnutí Rady 2011/349/EU[66] a článkem 3 rozhodnutí Rady 2011/350/EU[67].

(59) 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 2010/365/EU o uplatňování ustanovení schengenského *acquis* týkajících se Schengenského informačního systému v Bulharské republice a Rumunsku[68].

(60) 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.

(61) Toto nařízení by se mělo vztahovat na Irsko ve lhůtách určených v souladu s postupy stanovenými v příslušných nástrojích týkajících se použití schengenského *acquis* na tento stát.

(62) 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[69]. 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.

(63) Rozhodnutí Rady 2007/533/SVV a rozhodnutí Komise 2010/261/EU[70] by proto měly být zrušeny.

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

---

66 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).

67 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).

68 Úř. věst. L 166, 1.7.2010, s. 17.

69 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).

70 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).

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 4 a kapitoly 5 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 osobách a věcech a pro výměnu doplňujících informací a dalších údajů za účelem policejní a justiční spolupráce v trestních věcech.

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 a článku 40, vložených do SIS umožňující příslušným orgánům identifikovat osobu nebo věc 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) „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjektu údajů“);

e) „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;

f) „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;

g) „pozitivním nálezem“ v SIS:

   1) uživatel provede 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) je požadováno další opatření.

h) „označením“ pozastavení platnosti záznamu na vnitrostátní úrovni, které lze připojit k záznamům za účelem zatčení, záznamům o pohřešovaných osobách a záznamům pro účely skrytých, vyšetřovacích nebo zvláštních kontrol, pokud má členský stát za to, že účinek záznamu není slučitelný s jeho vnitrostátními právními předpisy, jeho mezinárodními závazky nebo základními vnitrostátními zájmy. Je-li záznam označen, požadované opatření, které má být přijato na základě záznamu, se nebude realizovat na území tohoto členského státu;

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

j) „vykonávajícím členským státem“ členský stát, který po pozitivním nálezu přijímá nebo přijal požadovaná opatření;

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

l) „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;

m) „závažnou trestnou činností“ trestné činy uvedené v čl. 2 odst. 1 a 2 rámcového rozhodnutí 2002/584/SVV ze dne 13. června 2002[71];

n) „teroristickými trestnými činy“ trestné činy podle vnitrostátního práva uvedené v článcích 1 až 4 rámcového rozhodnutí 2002/475/SVV ze dne 13. června 2002[72].

[71] 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).

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 uvedenými v 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. Dílčí vnitrostátní kopie musí obsahovat alespoň údaje uvedené v čl. 20 odst. 2 týkající se věcí a údaje uvedené v čl. 20 odst. 3 písm. a) až v) tohoto nařízení týkající se záznamů o osobách. 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[73] (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.

---

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

[73] 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. 53 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 61 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. 72 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 přijímají prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 72 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 článku 66 (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 43.

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. Evidence obsahuje zejména historii záznamu, datum a čas zpracování údajů, údaje použité pro provedení vyhledávání; odkaz na předávané údaje a název příslušného orgánu i jméno osoby odpovědné za zpracování údajů.

3. Pokud je vyhledávání provedeno s pomocí daktyloskopických údajů nebo zobrazení obličeje v souladu s článkem 40, 41 a 42, obsahují protokoly zejména druh údajů

použitých pro provedení vyhledávání, odkaz na druh předávaných údajů a název příslušného orgánu i 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.

7. Provedou-li členské státy automatizované skenovací vyhledávání registračních značek motorových vozidel, s použitím systémů automatického rozpoznávání registračních značek, musí uchovat protokol o tomto vyhledávání v souladu s vnitrostátními právními předpisy. Obsah tohoto protokolu se stanoví prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 72 odst. 2. V případě pozitivního výsledku v porovnání s údaji uloženými v SIS nebo ve vnitrostátních nebo technických kopiích údajů SIS se provede úplné vyhledávání v SIS za účelem ověření, že je výsledek skutečně pozitivní. Na toto úplné vyhledávání se uplatní ustanovení odstavců 1 až 6 tohoto článku.

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

Zaměstnanci orgánů s právem přístupu do SIS předtím, než 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 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 prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 72 odst. 2.

6. Provozní řízení centrálního SIS sestává ze všech úkolů nezbytných pro zachování funkčnosti centrálního SIS 24 hodiny denně sedm dní v týdnu, 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 64 (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 40, 41 a 42, 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

KATEGORIE ÚDAJŮ A OZNAČOVÁNÍ ZÁZNAMŮ

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 článcích 26, 32, 34, 36 a 38.

2. Kategorie údajů jsou následující:

   a) informace o osobách, u kterých byl pořízen záznam;

   b) informace o věcech uvedené v článcích 32, 36 a 38.

3. 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(i);

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(y) podle článku 53 na další záznamy pořízené v SIS;

p) druh trestného činu, pro nějž byl záznam pořízen;

q) registrační číslo osoby ve vnitrostátním rejstříku

r) kategorizace typu případu pohřešované osoby (pouze pro záznamy podle článku 32);

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) příslušné profily DNA podle čl. 22 odst. 1 písm. b) tohoto nařízení;

y) daktyloskopické údaje;

z) barevná kopie dokladu totožnosti.

4. Technická pravidla pro vkládání, aktualizaci, výmaz a vyhledávání údajů uvedených v odstavcích 2 a 3 se stanoví a vypracují prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 72 odst. 2.

5. Technická pravidla pro vyhledávání údajů uvedených v odstavci 3 se stanoví a vypracují přezkumným postupem uvedeným v čl. 72 odst. 2. Tato technická pravidla jsou podobná pro vyhledávání v CS-SIS, v národních kopiích a technických kopiích, jak je uvedeno v čl. 53 odst. 2, a vycházejí ze společných norem stanovených a

vypracovaných prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 72 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. Pokud je osoba nebo věc hledána členským státem v souvislosti s trestným činem, který spadá do oblasti působnosti článků 1 až 4 rámcového rozhodnutí Rady 2002/475/SVV o boji proti terorismu, musí členský stát za všech okolností vytvořit odpovídající záznam podle příslušného článku 34, 36 nebo 38.

Článek 22
Zvláštní pravidla pro vkládání fotografií, zobrazení obličeje, daktyloskopických údajů a profilů DNA

1. Vkládání údajů uvedených v čl. 20 odst. 3 písm. w), x) a y) se provádí podle těchto ustanovení:

a) Fotografie, zobrazení obličeje, daktyloskopické údaje a profily DNA se vloží pouze po provedení zvláštní kontroly kvality s cílem zjistit, zda jsou splněny minimální normy kvality údajů.

b) Profil DNA může být přidán pouze k záznamům podle čl. 32 odst. 2 písm. a) a c), a to pouze pokud fotografie, zobrazení obličeje ani daktyloskopické údaje vhodné pro určení totožnosti nejsou k dispozici. Profily DNA osob, které jsou přímými předky, potomky či sourozenci subjektu záznamu, lze přidat do záznamu, pouze pokud k tomu tyto dotčené osoby dají výslovný souhlas. Rasový původ osoby nesmí být do profilu DNA zahrnut.

2. Pro uchovávání údajů uvedených v odstavci 1 písm. a) tohoto článku a v článku 40 se stanoví normy kvality. Specifikace těchto norem se stanoví prostřednictvím prováděcích opatření a aktualizují přezkumným postupem uvedeným v čl. 72 odst. 2.

Článek 23
Požadavek na vložení záznamu

1. Záznam o osobě nesmí být vložen bez údajů uvedených v čl. 20 odst. 3 písm. a), g), k), m), n), jakož i případně (p), s výjimkou situací uvedených v článku 40.

2. Dále se vloží všechny další údaje uvedené v čl. 20 odst. 3, jsou-li k dispozici.

Článek 24
Obecná ustanovení týkající se označování záznamů

1. Pokud má členský stát za to, že provedení záznamu pořízeného v souladu s články 26, 32 a 36 není slučitelné s jeho vnitrostátními právními předpisy, jeho mezinárodními závazky nebo základními vnitrostátními zájmy, může následně požadovat označení záznamu v tom smyslu, že opatření, které má být přijato na základě záznamu, nebude přijato na jeho území. Označení provede centrála SIRENE členského státu, který záznam vložil.

2. Aby členské státy mohly požadovat označení záznamu pořízeného v souladu s článkem 26, všem členským státům se automaticky prostřednictvím výměny doplňujících informací oznámí všechny nové záznamy této kategorie.

3. Pokud v mimořádně naléhavých a závažných případech požaduje členský stát, který pořídil záznam, přijetí opatření, vykonávající členský stát přezkoumá, zda může povolit zrušení označení záznamu, které bylo přidáno na jeho pokyn. Může-li vykonávající stát toto označení zrušit, učiní nezbytné kroky k zajištění možnosti okamžitého vykonání opatření, jež má být přijato.

Článek 25
Označování záznamů za účelem zatčení a předání

1. V případech, na které se vztahuje rámcové rozhodnutí 2002/584/SVV, se označení zamezující zatčení přiřadí k záznamu za účelem zatčení a předání, pouze pokud justiční orgán příslušný podle vnitrostátního práva k výkonu evropského zatýkacího rozkazu odmítl tento rozkaz vykonat na základě důvodu pro odmítnutí výkonu a pokud bylo označení záznamu požadováno.

2. Dle rozhodnutí justičního orgánu příslušného podle vnitrostátního práva, buď na základě obecného pokynu, nebo pro konkrétní případ, je však možné požadovat označení záznamu za účelem zatčení a předání i tehdy, pokud je zřejmé, že výkon evropského zatýkacího rozkazu bude muset být odmítnut.

KAPITOLA VI

ZÁZNAMY O OSOBÁCH HLEDANÝCH ZA ÚČELEM ZATČENÍ A PŘEDÁNÍ NEBO VYDÁNÍ

Článek 26
Cíle a podmínky pořizování záznamů

1. Údaje o osobách hledaných za účelem zatčení a předání na základě evropského zatýkacího rozkazu nebo hledaných za účelem zatčení a vydání se vkládají na žádost justičního orgánu členského státu pořizujícího záznam.

2. Údaje o osobách hledaných za účelem zatčení a předání se vkládají na základě zatýkacích rozkazů vydaných v souladu s dohodami uzavřenými mezi Unií a třetími státy na základě článku 37 Smlouvy o Evropské unii za účelem předání osob na základě zatýkacího rozkazu, které stanoví předávání tohoto zatýkacího rozkazu prostřednictvím SIS.

3. Jakýkoliv odkaz v tomto nařízení na ustanovení rámcového rozhodnutí 2002/584/SVV se považuje rovněž za odkaz na odpovídající ustanovení dohod uzavřených mezi Evropskou unií a třetími státy na základě článku 37 Smlouvy o Evropské unii za účelem předávání osob na základě zatýkacího rozkazu, která stanoví předávání tohoto zatýkacího rozkazu prostřednictvím Schengenského informačního systému.

4. Členský stát, který pořídil záznam, může v případě probíhající pátrací operace a na základě schválení příslušným soudním orgánem členského státu, který záznam pořídil, dočasně znemožnit vyhledávání existujícího záznamu za účelem zatčení pořízeného podle článku 26 tohoto nařízení tak, aby ho koncoví uživatelé nemohli

vyhledat a byl dostupný pouze centrálám SIRENE. Tato funkce se použije pouze na dobu nepřesahující 48 hodin. Pokud je to nutné z operativního hlediska, může však být tato lhůta opakovaně prodloužena o dalších 48 hodin. Členské státy uchovávají statistiky o počtu záznamů, u nichž byla tato funkce použita.

Článek 27

Další údaje o osobách hledaných za účelem zatčení a předání

1. V případě osoby hledané za účelem zatčení a předání na základě evropského zatýkacího rozkazu vloží pořizující členský stát do SIS kopii originálu evropského zatýkacího rozkazu.
2. Pořizující členský stát může vložit kopii překladu evropského zatýkacího rozkazu do jednoho nebo několika dalších úředních jazyků orgánů Evropské unie.

Článek 28

Doplňující informace o osobách hledaných za účelem zatčení a předání

Členský stát, který vložil do SIS záznam za účelem zatčení a předání, sdělí prostřednictvím výměny doplňujících informací ostatním členským státům údaje uvedené v čl. 8 odst. 1 rámcového rozhodnutí 2002/584/SVV.

Článek 29

Doplňující informace o osobách hledaných za účelem zatčení a vydání

1. Členský stát, který vložil do SIS záznam za účelem vydání, sdělí prostřednictvím výměny doplňujících informací ostatním členským státům tyto údaje:
   a) orgán, který vydal žádost o zatčení;
   b) zda je k dispozici zatýkací rozkaz nebo akt se stejným právním účinkem nebo pravomocný rozsudek;
   c) podstatu a právní kvalifikaci trestného činu;
   d) popis okolností, za kterých byl trestný čin spáchán, včetně doby, místa činu a stupně účasti dotyčné osoby na něm;
   e) je-li to možné, následky trestného činu;
   f) nebo jakékoliv další informace, které jsou užitečné nebo nezbytné pro výkon záznamu.
2. Údaje uvedené v odstavci 1 se nesdělí, pokud byly již poskytnuty údaje uvedené v článcích 27 nebo 28 a pokud jsou považovány za dostačující pro výkon záznamu dotčeným členským státem.

Článek 30

Úprava záznamů o osobách hledaných za účelem zatčení a předání nebo vydání

Není-li možné zatčení provést buď z důvodu zamítavého rozhodnutí dožádaného členského státu v souladu s postupy týkajícími se označování uvedenými v článcích 24 nebo 25 nebo z toho důvodu, že v případě záznamu za účelem zatčení a vydání nebylo vyšetřování ukončeno, musí dožádaný členský stát považovat záznam za záznam pro účely sdělení místa pobytu dotyčné osoby.

Článek 31

Výkon opatření na základě záznamu o osobě hledané za účelem zatčení a předání nebo vydání

1. V případech, na které se vztahuje rámcové rozhodnutí 2002/584/SVV, je záznam vložený do SIS podle článku 26 ve spojení s dalšími údaji podle článku 27 evropským zatýkacím rozkazem vystaveným v souladu s rámcovým rozhodnutím 2002/584/SVV a má stejný účinek.

2. V případech, na které se rámcové rozhodnutí 2002/584/SVV nevztahuje, má záznam vložený do SIS podle článku 26 a 29 stejnou platnost jako žádost o předběžnou vazbu podle článku 16 Evropské úmluvy o vydávání ze dne 13. prosince 1957 nebo článku 15 smlouvy zemí Beneluxu o vydávání a vzájemné pomoci ve věcech trestních ze dne 27. června 1962.

KAPITOLA VII

ZÁZNAMY O POHŘEŠOVANÝCH OSOBÁCH

Článek 32

Cíle a podmínky pořizování záznamů

1. Údaje o pohřešovaných osobách nebo jiných osobách, které musí být umístěny pod dočasnou ochranu nebo jejichž místo pobytu je třeba zjistit, se vloží do SIS na žádost příslušného orgánu členského státu pořizujícího záznam.

2. Je možné vkládat tyto kategorie pohřešovaných osob:

   a) pohřešované osoby, které musí být umístěny pod ochranu

      i) v zájmu své vlastní ochrany,

      ii) za účelem předcházení nebezpečí hrozícího těmto osobám;

   b) pohřešované osoby, které nemusí být umístěny pod ochranu;

   c) děti, kterým hrozí únos podle odstavce 4.

3. Odst. 2 písm. a) se použije zejména na děti a na osoby, které musí být internovány na základě rozhodnutí příslušného orgánu.

4. Záznam o dítěti podle odst. 2 písm. c) se pořizuje na žádost soudního orgánu členského státu, který je příslušný ve věcech rodičovské zodpovědnosti v souladu s nařízením Rady č. 2201/2003[74], je-li konkrétní a zjevné riziko, že by dítě mohlo být nezákonně a v blízké budoucnosti odebráno z členského státu, ve kterém se tento soudní orgán nachází. V členských státech, které jsou smluvními stranami Haagské úmluvy ze dne 19. října 1996 o pravomoci orgánů, použitelném právu, uznávání, výkonu a spolupráci ve věcech rodičovské zodpovědnosti a opatření k ochraně dětí a které nejsou vázány nařízením Rady č. 2201/2003, platí ustanovení Haagské úmluvy.

5. Členské státy zajistí, aby údaje vložené do SIS uváděly, do které z kategorií zmíněných v odstavci 2 pohřešovaná osoba patří. Členské státy rovněž zajistí, aby údaje vložené do SIS uváděly, o který typ případů pohřešovaných nebo zranitelných

[74] Nařízení Rady (ES) č. 2201/2003 ze dne 27. listopadu 2003 o příslušnosti a uznávání a výkonu rozhodnutí ve věcech manželských a ve věcech rodičovské zodpovědnosti a o zrušení nařízení (ES) č. 1347/2000 (Úř. věst. L 338, 23.12.2003, s. 1).

osob se jedná. Pravidla týkající se kategorizace typů případů a vkládání uvedených údajů se stanoví a vypracují prostřednictvím prováděcích opatření v souladu s přezkumným postupem uvedeným v čl. 72 odst. 2.

6. Čtyři měsíce před datem, kdy dítě, které je subjektem záznamu podle tohoto článku, dosáhne plnoletosti, CS-SIS automaticky informuje členský stát, který pořídil záznam, že důvod pro žádost a opatření, jež má být přijato, musí být aktualizovány nebo musí být záznam vymazán.

7. Pokud existuje důvodné podezření, že s osobou, která je subjektem záznamu podle odstavce 2, jsou spojena vozidla, plavidla nebo letadla, lze pořídit záznamy o těchto vozidlech, plavidlech a letadlech za účelem nalezení dané osoby. V těchto případech se záznam o pohřešované osobě propojí se záznamem o věci v souladu s článkem 60. Technická pravidla pro vkládání, aktualizaci, výmaz a vyhledávání údajů uvedených v tomto odstavci se stanoví a vypracují prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 72 odst. 2.

Článek 33
Výkon opatření na základě záznamu

1. Je-li nalezena osoba uvedená v článku 32, příslušné orgány sdělí s výhradou odstavce 2 členskému státu pořizujícímu záznam její místo pobytu. V případě pohřešovaných dětí nebo dětí, které musí být umístěny pod dočasnou ochranu, vykonávající členský stát okamžitě konzultuje členský stát, který záznam pořídil, aby se neprodleně dohodly na opatřeních, která mají být přijata za účelem ochrany nejvlastnějšího zájmu dítěte. V případech uvedených v čl. 32 odst. 2 písm. a) a c) mohou příslušné orgány umístit osobu pod ochranu a zabránit jí tak v tom, aby pokračovala v cestě, pokud to dovolují vnitrostátní právní předpisy.

2. Sdělení údajů o pohřešované osobě, jež byla nalezena a která je plnoletá, jiné než sdělení mezi příslušnými orgány, vyžaduje souhlas této osoby. Příslušné orgány však mohou sdělit osobě, jež oznámila pohřešování osoby, skutečnost, že záznam byl z důvodu nalezení pohřešované osoby vymazán.

KAPITOLA VIII

ZÁZNAMY O OSOBÁCH ZA ÚČELEM ZAJIŠTĚNÍ JEJICH SPOLUPRÁCE V SOUDNÍM ŘÍZENÍ

Článek 34
Cíle a podmínky pořizování záznamů

1. Pro účely sdělení místa pobytu nebo bydliště osob vloží členské státy na žádost příslušného orgánu do SIS údaje o:

   a) svědcích;

   b) osobách předvolaných nebo hledaných za účelem předvolání justičními orgány v rámci trestního řízení, aby vypovídaly o skutečnostech, pro které jsou stíhány;

   c) osobách, kterým musí být doručen trestní rozsudek nebo jiné dokumenty v rámci trestního řízení, aby vypovídaly o skutečnostech, pro které jsou stíhány;

d) osobách, kterým musí být doručena obsílka k nástupu trestu odnětí svobody.

2. Pokud existuje důvodné podezření, že s osobou, která je subjektem záznamu podle odstavce 1, jsou spojena vozidla, plavidla nebo letadla, lze pořídit záznamy o těchto vozidlech, plavidlech a letadlech za účelem nalezení dané osoby. V takových případech se záznam o dané osobě propojí se záznamem o věci v souladu s článkem 60. Technická pravidla pro vkládání, aktualizaci, výmaz a vyhledávání údajů uvedených v tomto odstavci se stanoví a vypracují prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 72 odst. 2.

Článek 35
Provádění opatření na základě záznamu

Požadované informace jsou žádajícímu členskému státu sdělovány prostřednictvím výměny doplňujících informací.

KAPITOLA IX

ZÁZNAMY O OSOBÁCH A VĚCECH POŘÍZENÉ PRO ÚČELY SKRYTÝCH, VYŠETŘOVACÍCH NEBO ZVLÁŠTNÍCH KONTROL

Článek 36
Cíle a podmínky pořizování záznamů

1. Údaje o osobách nebo vozidlech, plavidlech, letadlech a kontejnerech se vkládají pro účely skrytých, vyšetřovacích nebo zvláštních kontrol v souladu s čl. 37 odst. 4 podle právních předpisů členského státu pořizujícího záznam.

2. Tento záznam může být pořízen pro účely trestního stíhání, výkon rozsudku v trestním řízení a předcházení ohrožení veřejné bezpečnosti, pokud:

   a) existuje důvodné podezření, že osoba zamýšlí spáchat nebo páchá závažnou trestnou činnost, zejména trestné činy uvedené v čl. 2 odst. 2 rámcového rozhodnutí 2002/584/SVV, nebo

   b) informace uvedené v čl. 37 odst. 1 jsou nezbytné pro výkon rozsudku v trestním řízení týkajícího se osoby odsouzené za závažnou trestnou činnost, zejména trestné činy uvedené v čl. 2 odst. 2 rámcového rozhodnutí 2002/584/JHA; nebo

   c) z celkového posouzení osoby, zejména na základě dosud spáchaných trestných činů, lze předpokládat, že se i v budoucnosti může dopustit závažné trestné činnosti, zejména trestných činů uvedených v čl. 2 odst. 2 rámcového rozhodnutí 2002/584/SVV.

3. Kromě toho může být záznam v souladu s vnitrostátními právními předpisy pořízen na žádost orgánů odpovědných za státní bezpečnost, pokud existuje konkrétní důvod předpokládat, že informace uvedené v čl. 37 odst. 1 jsou nezbytné pro předcházení závažnému ohrožení ze strany dotyčné osoby nebo jiným závažným ohrožením vnitřní nebo vnější státní bezpečnosti. Členský stát pořizující záznam podle tohoto odstavce o tom informuje ostatní členské státy. Každý členský stát určí, kterým orgánům se tyto informace předávají.

4. Pokud existuje důvodné podezření, že jsou se závažnými trestnými činy uvedenými v odstavci 2 nebo závažnými hrozbami uvedenými v odstavci 3 spojena vozidla, plavidla, letadla a kontejnery, mohou být o těchto vozidlech, plavidlech, letadlech a kontejnerech pořízeny záznamy.

5. Pokud existuje důvodné podezření, že jsou se závažnými trestnými činy uvedenými v odstavci 2 nebo závažnými hrozbami uvedenými v odstavci 3 spojeny nevyplněné úřední doklady nebo vydané doklady totožnosti, mohou být o těchto dokladech pořízeny záznamy, a to bez ohledu na totožnost případného původního držitele dokladu. Technická pravidla pro vkládání, aktualizaci, výmaz a vyhledávání údajů uvedených v tomto odstavci se stanoví a vypracují prostřednictvím prováděcích opatření přezkumným postupem uvedeným v čl. 72 odst. 2.

Článek 37
Provádění opatření na základě záznamu

1. Pro účely skrytých, vyšetřovacích nebo zvláštních kontrol mohou být při provádění hraničních, policejních a celních kontrol nebo jiných činností v oblasti vymáhání práva v členském státě shromažďovány a předávány orgánu, který pořídil záznam, všechny nebo některé z následujících informací:

   a) skutečnost, že osoba, o které byl pořízen záznam, nebo vozidlo, plavidlo, letadlo, kontejner, nevyplněný úřední doklad či vydaný doklad totožnosti, o nichž byl pořízen záznam, byly nalezeny;

   b) místo, čas a důvod kontroly;

   c) trasa a cíl cesty;

   d) osoby, které doprovázejí dotyčnou osobu nebo cestující ve vozidle, na plavidle nebo v letadle nebo osoby doprovázející držitele nevyplněného úředního dokladu či vydaného dokladu totožnosti, o kterých lze důvodně předpokládat, že jsou s dotyčnou osobou spojeny;

   e) zjištěnou totožnost a osobní popis osoby používající nevyplněný úřední doklad či vydaný doklad totožnosti, které jsou subjektem záznamu;

   f) použité vozidlo, plavidlo, letadlo nebo kontejner;

   g) převážené předměty, včetně cestovních dokladů;

   h) okolnosti, za jakých byly osoba nebo vozidlo, plavidlo, letadlo, kontejner nebo nevyplněné úřední doklady či vydané doklady totožnosti nalezeny.

2. Informace uvedené v odstavci 1 se sdělí prostřednictvím výměny doplňujících informací.

3. V závislosti na provozních podmínkách a v souladu s vnitrostátním právem zahrnuje skrytá kontrola systematickou kontrolu osoby či věci s cílem získat co nejvíce informací popsaných v odstavci 1, aniž by byla pokud možno ohrožena utajená povaha kontroly.

4. V závislosti na provozních podmínkách a v souladu s vnitrostátním právem zahrnuje vyšetřovací kontrola důkladnější kontrolu a výslech osoby. Pokud vyšetřovací kontroly nejsou podle právních předpisů členského státu povoleny, nahrazují se v tomto členském státě skrytými kontrolami.

5. Během zvláštních kontrol může být v souladu s vnitrostátními právními předpisy pro účely uvedené v článku 36 provedena prohlídka osob, vozidel, plavidel, letadel, kontejnerů a převážených věcí. Prohlídky se vykonávají v souladu s vnitrostátními právními předpisy. Pokud zvláštní kontroly nejsou podle právních předpisů členského státu povoleny, nahrazují se v tomto členském státě vyšetřovacími kontrolami.

KAPITOLA X

ZÁZNAMY O VĚCECH HLEDANÝCH ZA ÚČELEM ZABAVENÍ NEBO ZA ÚČELEM ZAJIŠTĚNÍ DŮKAZŮ V TRESTNÍM ŘÍZENÍ

Článek 38
Cíle a podmínky pořizování záznamů

1. Do SIS se vkládají údaje o věcech hledaných za účelem zabavení v rámci vymáhání práva nebo za účelem zajištění důkazů v trestním řízení.

2. Vkládají se tyto kategorie snadno identifikovatelných věcí:

   a) motorová vozidla vymezená vnitrostátními právními předpisy, bez ohledu na systém pohonu;

   b) přívěsy o pohotovostní hmotnosti přesahující 750 kg;

   c) obytné přívěsy;

   d) průmyslová zařízení;

   e) plavidla;

   f) lodní motory;

   g) kontejnery;

   h) letadla;

   i) palné zbraně;

   j) odcizené, neoprávněně užívané nebo pohřešované nevyplněné úřední doklady;

   k) odcizené, neoprávněně užívané, pohřešované nebo neplatné doklady totožnosti, jako jsou pasy, občanské průkazy, řidičské průkazy, povolení k pobytu a cestovní doklady, jež byly vydány, nebo doklady, které vypadají jako uvedené doklady, ale jsou padělané;

   l) odcizené, neoprávněně užívané, pohřešované nebo neplatné osvědčení o registraci vozidel a registrační značky vozidel, nebo osvědčení či značky, které vypadají jako uvedená osvědčení a značky, ale jsou padělané;

   m) bankovky (evidované) a padělané bankovky;

   n) technické vybavení, IT vybavení a jiné snadno identifikovatelné cenné věci;

   o) identifikovatelné součásti motorových vozidel;

   p) identifikovatelné součásti průmyslového zařízení.

3. Definice nových podkategorií věcí podle odst. 2 písm. n) a 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. 72 odst. 2.

Článek 39
Provádění opatření na základě záznamu

1. Pokud se při vyhledávání zjistí záznam o věci, která byla nalezena, zabaví orgán, který zjistil shodu dvou položek údajů, dotčenou věc a spojí se s orgánem, který pořídil záznam, s cílem dohodnout vhodná opatření. Za tímto účelem mohou být v souladu s tímto nařízením sdělovány i osobní údaje.
2. Informace uvedené v odstavci 1 se sdělí prostřednictvím výměny doplňujících informací.
3. Požadované opatření, jež má přijmout členský stát, který věc nalezl, musí být v souladu s jeho vnitrostátními právními předpisy.

KAPITOLA XI

ZÁZNAMY O NEZNÁMÝCH HLEDANÝCH OSOBÁCH ZA ÚČELEM URČENÍ TOTOŽNOSTI V SOULADU S VNITROSTÁTNÍMI PRÁVNÍMI PŘEDPISY ČI VYHLEDÁVÁNÍ POMOCÍ BIOMETRICKÝCH ÚDAJŮ

Článek 40
Záznamy o neznámých hledaných osobách za účelem zadržení podle vnitrostátních právních předpisů

Do SIS lze vkládat daktyloskopické údaje, které se netýkají osob, které jsou předmětem záznamů. Tyto daktyloskopické údaje mohou představovat úplné či neúplné soubory otisků prstů nebo otisků dlaní zajištěných na místě vyšetřovaného činu, závažného trestného činu či teroristického trestného činu, u nichž lze s vysokou mírou pravděpodobnosti stanovit, že patří pachateli daného trestného činu. Daktyloskopické údaje v této kategorii se uloží jako „neznámá podezřelá či hledaná osoba“ za předpokladu, že příslušné orgány nemohou určit totožnost osoby s využitím žádné jiné vnitrostátní, evropské nebo mezinárodní databáze.

Článek 41
Provádění opatření na základě záznamu

V případě pozitivního nálezu nebo potenciální shody s údaji uloženými podle článku 40 se určí totožnost osoby v souladu s vnitrostátními právními předpisy a ověří se, zda daktyloskopické údaje uložené v SIS patří dané osobě. Členské státy komunikují prostřednictvím výměny doplňujících informací s cílem napomoci včasnému vyšetření případu.

Článek 42
Zvláštní pravidla pro ověřování nebo vyhledávání fotografií, zobrazení obličeje, daktyloskopických údajů a profilů DNA

1. Fotografie, zobrazení obličeje, daktyloskopické údaje a profily DNA 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 vyhledají 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 26, čl. 34 odst. 1 písm. b) a d) a článku 36 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 daného trestného činu.

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 XII

PRÁVO PŘÍSTUPU K ZÁZNAMŮM A JEJICH UCHOVÁVÁNÍ

Článek 43
Orgány mající právo přístupu k záznamům

1. Přístup k údajům vloženým do SIS a právo v těchto údajích vyhledávat přímo nebo v kopii údajů CS-SIS je vyhrazeno orgánům odpovědným za:

   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.

2. Právo na přístup k údajům vloženým do SIS a právo v těchto údajích přímo vyhledávat mohou však při plnění svých úkolů stanovených vnitrostátním právem vykonávat i vnitrostátní justiční orgány, včetně těch, které odpovídají za zahájení trestního stíhání a za vyšetřování před podáním obžaloby, jakož i jejich koordinační orgány.

3. Právo na přístup k údajům vloženým do SIS a v těchto údajích přímo vyhledávat mohou vykonávat orgány příslušné k plnění úkolů uvedených v odst. 1 písm. c) při plnění těchto úkolů. Přístup těchto orgánů k uvedeným údajům se řídí právem každého členského státu.

4. Orgány uvedené v tomto článku se zahrnou do seznamu uvedeného v čl. 53 odst. 8.

Článek 44

Orgány příslušné pro registraci vozidel

1. Subjekty v členských státech odpovědné za vydávání osvědčení o registraci vozidel uvedených ve směrnici Rady 1999/37/ES[75] mají přístup k následujícím údajům vloženým do SIS podle čl. 38 odst. 2 písm. a), b), c) a l) tohoto nařízení pouze za účelem kontroly, zda vozidla přihlašovaná k registraci nepatří mezi vozidla odcizená, neoprávněně užívaná nebo pohřešovaná nebo hledaná za účelem zajištění důkazů v trestním řízení:

   a) údaje o motorových vozidlech vymezených vnitrostátním právem, bez ohledu na systém pohonu;

   b) údaje o přívěsech o pohotovostní hmotnosti přesahující 750 kg a obytných přívěsech;

   c) údaje o odcizených, neoprávněně užívaných, pohřešovaných nebo neplatných osvědčeních o registraci vozidel a registračních značkách.

   Přístup subjektů odpovědných za vydávání osvědčení o registraci vozidel k těmto údajům se řídí vnitrostátním právem daného členského státu.

2. Subjekty uvedené v odstavci 1, které jsou státními subjekty, mají právo přímého přístupu k údajům vloženým do SIS.

3. Subjekty uvedené v odstavci 1, které nejsou státními subjekty, mají právo přístupu k údajům vloženým do SIS pouze prostřednictvím orgánu uvedeného v článku 43 tohoto nařízení. Tento orgán má právo přímého přístupu k uvedeným údajům a právo na jejich předání dotčenému subjektu. Dotčený členský stát zajistí, aby daný subjekt i jeho zaměstnanci byli povinni dodržovat veškerá omezení související s přípustným používáním údajů, které jim předal příslušný orgán.

4. Článek 39 tohoto nařízení se nepoužije pro přístup uskutečněný v souladu s tímto článkem. Sdělování informací zjištěných z přístupu do SIS a vedoucích k podezření, že byl spáchán trestný čin, policejním či justičním orgánům ze strany subjektů uvedených v odstavci 1 se řídí vnitrostátním právem.

Článek 45

Orgány příslušné pro registraci plavidel a letadel

1. Subjekty v členských státech odpovědné za vydávání osvědčení o registraci nebo zajišťování řízení provozu u plavidel, včetně lodních motorů, a letadel mají přístup k následujícím údajům vloženým do SIS v souladu s čl. 38 odst. 2 tohoto nařízení pouze pro účely ověření, zda plavidla, včetně lodních motorů, letadla nebo kontejnery přihlašované k registraci, nebo předmět řízení provozu, nejsou odcizeny, neoprávněně užívány nebo pohřešovány nebo hledány za účelem zajištění důkazů v trestním řízení:

   a) údaje o plavidlech;

   b) údaje o lodních motorech;

   c) údaje o letadlech.

[75] Směrnice Rady 1999/37 ze dne 29. dubna 1999 o registračních dokladech vozidel (Úř. věst. L 138, 1.6.1999, s. 57).

S výhradou odstavce 2 se přístup těchto subjektů členského státu k uvedeným údajům řídí právem v daném členském státě. Přístup k údajům uvedeným v písmenech a) až c) výše je omezen na konkrétní pravomoc dotčených subjektů.

2. Subjekty uvedené v odstavci 1, které jsou státními subjekty, mají právo přímého přístupu k údajům vloženým do SIS.

3. Subjekty uvedené v odstavci 1, které nejsou státními subjekty, mají právo přístupu k údajům vloženým do SIS pouze prostřednictvím orgánu uvedeného v článku 43 tohoto nařízení. Tento orgán má právo přímého přístupu k údajům a právo na předání uvedených údajů dotčenému subjektu. Dotčený členský stát zajistí, aby subjekt i jeho zaměstnanci byli povinni dodržovat veškerá omezení související s přípustným používáním údajů, které jim předal příslušný orgán.

4. Článek 39 tohoto nařízení se nepoužije pro přístup uskutečněný v souladu s tímto článkem. Sdělování informací zjištěných z přístupu do SIS a vedoucích k podezření, že byl spáchán trestný čin, policejním či justičním orgánům ze strany subjektů uvedených v odstavci 1 se řídí vnitrostátním právem.

Článek 46
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.

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. Veškeré 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 protokol 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 47
Přístup Eurojustu k údajům SIS

1. Národní členové Eurojustu a jejich asistenti mají v rámci svého mandátu právo na přístup k údajům vloženým do SIS a právo v těchto údajích vyhledávat v rámci svého mandátu v souladu s články 26, 32, 34, 38 a 40.

2. Pokud vyhledávání provedené národním členem Eurojustu odhalí existenci záznamu v SIS, informuje o tom členský stát, který záznam pořídil.

3. Žádné ustanovení tohoto článku se nedotýká ustanovení rozhodnutí 2002/187/SVV týkajících se ochrany údajů a odpovědnosti za neoprávněné nebo nesprávné zpracování takových údajů národními členy Eurojustu nebo jejich asistenty, ani pravomocí společného kontrolního orgánu zřízeného podle uvedeného rozhodnutí.

4. Každý vstup a vyhledávání provedené národním členem Eurojustu nebo jeho asistentem se zaprotokoluje v souladu s článkem 12 a každé jejich použití údajů, k nimž získali přístup, se zaprotokoluje.

5. Žádné části SIS se nepropojí s jakýmkoli počítačovým systémem pro sběr a zpracování údajů provozovaným Eurojustem ani se do takového počítačového systému nepřenesou údaje v SIS obsažené, k nimž mají národní členové nebo jejich asistenti přístup. Žádná část SIS se nestáhne. Protokolování přístupu a vyhledávání není považováno za protiprávní stahování nebo kopírování údajů SIS.

6. Přístup k údajům vloženým do SIS je omezen na národní členy a jejich asistenty a nelze jej rozšířit na zaměstnance Eurojustu.

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

Článek 48

Přístup jednotek Evropské pohraniční a pobřežní stráže, týmů pracovníků, kteří se podílejí na úkolech spojených s navracením, a členů podpůrného týmu 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. 49 odst. 1.

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 podpůrného týmu pro řízení migrace se zaprotokoluje v souladu s článkem 12 a každé jejich použití údajů, k nimž získali přístup, se zaprotokoluje.

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 podpůrného týmu 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 49

Přístup Evropské agentury pro pohraniční a pobřežní stráž k údajům SIS

1. Pro účely čl. 48 odst. 1 a 2 tohoto článku Evropská agentura pro pohraniční a pobřežní stráž vytvoří a spravuje technické rozhraní, které umožňuje přímé propojení s centrálním SIS.

2. 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 v těchto údajích vyhledávat, a to v souladu s články 26, 32, 34, 36 a čl. 38 odst. 2 písm. j) a k).

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

4. 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.

5. Každý vstup a každé vyhledávání provedené Evropskou agenturou pro pohraniční a pobřežní stráž se zaprotokoluje v souladu s článkem 12 a každé její použití údajů, k nimž byl získán přístup, se zaeviduje.

6. 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.

7. Za účelem zajištění důvěrnosti a bezpečnosti Evropská agentura pro pohraniční a pobřežní stráž přijme a bude uplatňovat opatření stanovená v článcích 10 a 11.

Článek 50
Rozsah přístupu

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

Článek 51
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. Záznamy pořízené pro účely článku 36 tohoto nařízení se uchovávají po dobu nanejvýš jednoho roku.

3. Záznamy o nevyplněných úředních dokladech a vydaných dokladech totožnosti vložené v souladu s článkem 38 se uchovávají po dobu nanejvýš deseti let. Kratší doby uchovávání pro kategorie záznamů o věcech mohou být stanoveny prováděcími opatřeními přijatými v souladu s přezkumným postupem podle čl. 72 odst. 2.

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

5. 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.

6. Členský stát, jenž záznam pořídil, může v době pro přezkum na základě souhrnného individuálního posouzení, které zaprotokoluje, 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.

7. 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 6. O plánovaném výmazu údajů ze systému uvědomí CS-SIS členské státy automaticky čtyři měsíce předem.

8. Členské státy uchovávají statistiky o počtu záznamů, u nichž byla doba uchovávání prodloužena v souladu s odstavcem 6.

KAPITOLA XIII

VÝMAZ ZÁZNAMŮ

Článek 52
Výmaz záznamů

1. Záznamy za účelem zatčení a předání nebo vydání podle článku 26 se vymažou, jakmile je osoba předána nebo vydána příslušným orgánům členského státu, který záznam pořídil. Mohou být rovněž vymazány, pokud justiční rozhodnutí, na němž byl záznam založen, zrušil příslušný justiční orgán podle vnitrostátního práva.

2. Záznamy o pohřešovaných osobách se vymažou v souladu s těmito pravidly:

   a) U pohřešovaných dětí podle článku 32 se záznam vymaže:

      – po vyřešení případu, například když bylo dítě navráceno do vlasti nebo příslušné orgány vykonávajícího členského státu přijaly rozhodnutí o péči o dítě,

      – po uplynutí platnosti záznamu podle článku 51,

      – poté, co příslušný orgán členského státu, který pořídil záznam, rozhodl o jeho vymazání, nebo

      – po nalezení dítěte.

   b) U pohřešovaných dospělých osob podle článku 32, pokud se nevyžadují ochranná opatření, se záznam vymaže:

      – po vykonání opatření, jež má být přijato (vykonávající členský stát potvrdí místo pobytu osoby),

      – po uplynutí platnosti záznamu podle článku 51 nebo

      – poté, co příslušný orgán členského státu, který pořídil záznam, rozhodl o jeho vymazání.

c) U pohřešovaných dospělých osob podle článku 32, pokud se vyžadují ochranná opatření, se záznam vymaže:

– po vykonání opatření, jež má být přijato (osoba umístěna pod ochranu),

– po uplynutí platnosti záznamu podle článku 51 nebo

– poté, co příslušný orgán členského státu, který pořídil záznam, rozhodl o jeho vymazání.

V závislosti na vnitrostátním právu může být u osoby, jež byla internována na základě rozhodnutí příslušného orgánu, záznam uchován, dokud není tato osoba navrácena do vlasti.

3. Záznamy o osobách hledaných za účelem předvolání justičními orgány se vymažou v souladu s těmito pravidly:

U záznamů o osobách hledaných za účelem předvolání justičními orgány podle článku 34 se záznam vymaže:

a) poté, co je příslušnému orgánu členského státu, který pořídil záznam, sděleno místo pobytu hledané osoby. Pokud na základě zaslaných informací nelze učinit další kroky, informuje centrála SIRENE členského státu, který pořídil záznam, za účelem vyřešení problému centrálu SIRENE vykonávajícího členského státu;

b) po uplynutí platnosti záznamu podle článku 51 nebo

c) poté, co příslušný orgán členského státu, který pořídil záznam, rozhodl o jeho vymazání.

Jestliže byl v členském státě učiněn pozitivní nález, členskému státu, který pořídil záznam, byla zaslána adresa a následný pozitivní nález v tomto členském státě odhalí stejnou adresu, zaprotokoluje se pozitivní nález ve vykonávajícím členském státě, ale členskému státu, který pořídil záznam, se znovu nezasílá ani adresa, ani doplňující informace. V takových případech vykonávající členský stát informuje členský stát, který pořídil záznam, o opakovaných pozitivních nálezech a ten zváží, zda je třeba záznam ponechat.

4. Záznamy o skrytých, vyšetřovacích a zvláštních kontrolách se vymažou v souladu s těmito pravidly:

U záznamů o skrytých, vyšetřovacích a zvláštních kontrolách podle článku 36 se záznam vymaže:

a) po uplynutí platnosti záznamu podle článku 51;

b) poté, co příslušný orgán členského státu, který pořídil záznam, rozhodl o jeho vymazání.

5. Záznamy o věcech hledaných za účelem zabavení nebo za účelem zajištění důkazů se vymažou v souladu s těmito pravidly:

U záznamů o věcech hledaných za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení podle článku 38 se záznam vymaže:

(a) po zabavení věci nebo rovnocenném opatření, jakmile si centrály SIRENE následně vymění potřebné doplňující informace, nebo je o věci zahájeno další soudní nebo správní řízení;

(b) po uplynutí platnosti záznamu nebo

(c) poté, co příslušný orgán členského státu, který pořídil záznam, rozhodl o jeho vymazání.

6. Záznamy o neznámých hledaných osobách podle článku 40 se vymažou v souladu s těmito pravidly:

7. a) po identifikaci dané osoby nebo

8. b) po uplynutí platnosti záznamu.

KAPITOLA XIV

OBECNÁ PRAVIDLA PRO ZPRACOVÁNÍ ÚDAJŮ

Článek 53
Zpracování údajů v SIS

1. Členské státy mohou zpracovávat údaje uvedené v článku 20 pouze pro účely stanovené pro každou kategorii záznam uvedenou v článcích 26, 32, 34, 36, 38 a 40.

2. Kopie údajů se mohou pořizovat pouze pro technické účely, pokud jsou potřebné k přímému vyhledávání orgány uvedenými v článku 43. 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.

4. 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.

5. Přístup k takovým údajům se povoluje pouze v mezích pravomoci vnitrostátních orgánů uvedených v článku 43 a pouze pracovníkům vybaveným náležitým oprávněním.

6. Pokud jde o záznamy podle článků 26, 32, 34, 36, 38 a 40 tohoto nařízení, jakékoli zpracování informací v nich uvedených pro jiné účely než účely, pro které byly vloženy do SIS, 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 závažnému trestnému činu. Za tím účelem musí být předem získáno povolení členského státu, jenž záznam pořídil.

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 54
Údaje SIS a vnitrostátní soubory

1. Ustanovením čl. 53 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. 53 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 55
Informování v případě nepoužití záznamu

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

Článek 56
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 59.

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 57

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 vnitrostátnímu orgánu dozoru. 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 58

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. 56 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 59

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) fotografie a 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. 72 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 60
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. 72 odst. 2.

Článek 61
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 62
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.

Článek 63
Výměna údajů o odcizených, neoprávněně užívaných, ztracených nebo neplatných cestovních pasech s Interpolem

1. Odchylně od článku 62 si lze s členy Interpolu vyměňovat údaje o čísle cestovního pasu, zemi vystavení a druhu odcizených, neoprávněně užívaných, ztracených nebo neplatných cestovních pasů vložených do SIS prostřednictvím propojení SIS a databáze Interpolu o odcizených nebo pohřešovaných cestovních dokladech, s výhradou uzavření dohody mezi Interpolem a Evropskou unií. Dohodou se stanoví, že předávání údajů vložených členským státem podléhá souhlasu uvedeného členského státu.

2. Dohodou uvedenou v odstavci 1 se stanoví, že přístup ke sdíleným údajům mají pouze členové Interpolu ze zemí, které zajišťují náležitou úroveň ochrany osobních údajů. Před uzavřením této dohody si Rada vyžádá stanovisko Komise k přiměřenosti úrovně ochrany osobních údajů a dodržování lidských práv a svobod, pokud jde o automatické zpracovávání osobních údajů Interpolem a zeměmi, které mají zástupce u Interpolu.

3. V souladu s příslušnými ustanoveními tohoto nařízení týkajícími se odcizených, neoprávněně užívaných, pohřešovaných nebo neplatných cestovních pasů vložených do SIS může dohoda uvedená v odstavci 1 rovněž umožnit členským státům prostřednictvím SIS přístup k údajům z databáze Interpolu o odcizených nebo pohřešovaných cestovních dokladech.

KAPITOLA XV

OCHRANA ÚDAJŮ

Článek 64
Platné právní předpisy

1. Na zpracování osobních údajů agenturou podle tohoto nařízení se vztahuje nařízení (ES) č. 45/2001.

2. Na zpracování osobních údajů se použije 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 65
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. Každý má právo na opravu věcně nepřesných údajů nebo výmaz protiprávně uchovávaných údajů, které se jej týkají.

6. 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.

7. 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 66
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 70, 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 vypracují vnitrostátní orgány 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 69.

Článek 67
Dohled nad N.SIS

1. Každý členský stát zajistí, aby 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, 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 68
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 69
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.

CHAPTER XVI

ODPOVĚDNOST

Článek 70
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.

CHAPTER XVII

ZÁVĚREČNÁ USTANOVENÍ

Článek 71
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 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. Vypracované statistiky nesmí obsahovat osobní údaje. Roční statistická zpráva se zveřejní. Agentura rovněž poskytuje roční statistiky o využívání funkce, kterou se dočasně znemožňuje vyhledávání záznamu pořízeného podle článku 26 tohoto nařízení, a to celkem a pro každý členský stát jednotlivě, včetně jakéhokoli prodloužení 48hodinové doby znemožnění vyhledávání.

4. Členské státy, jakož i Europol, Eurojust a Evropská agentura pro pohraniční a pobřežní stráž poskytnou agentuře a Komisi informace nezbytné pro vypracování zpráv uvedených v odstavcích 3, 7 a 8. Tyto informace zahrnují oddělené statistiky o počtu vyhledávání provedených subjekty v členských státech odpovědnými za vydávání osvědčení o registraci vozidel nebo jménem těchto subjektů, o počtu

vyhledávání provedených subjekty v členských státech odpovědnými za vydávání osvědčení o registraci nebo za zajištění řízení provozu u plavidel, včetně lodních motorů, a dále letadel a kontejnerů, nebo jménem těchto subjektů. Statistiky musí rovněž uvádět počet pozitivních nálezů podle kategorie záznamů.

5. Agentura postoupí členským státům, Komisi, Europolu, Eurojustu 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, 4 a 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 určení totožnosti osob a dovolí Komisi a agenturám uvedeným v odstavci 5 získat konkrétní zprávy a statistiky. Agentura udělí členským státům, Komisi, Europolu, Eurojustu 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 přijmou prostřednictvím prováděcích opatření přijatých přezkumným postupem uvedeným v čl. 72 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 infrastruktuře, 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 72
Postup projednávání ve výborech

1. Komisi je nápomocen výbor ve smyslu nařízení (EU) č. 182/2011.

2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

Článek 73
Změny nařízení (EU) 515/2014

Nařízení (EU) č. 515/2014[76] se mění takto:

[76] 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).

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 v nařízení (Úř. věst. ....).“

Článek 74
Zrušení

Dnem použitelnosti tohoto nařízení se zrušují tyto právní akty:

nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 ze dne 20. prosince 2006 o přístupu subjektů odpovědných za vydávání osvědčení o registraci vozidel v členských státech k Schengenskému informačnímu systému druhé generace (SIS II),

rozhodnutí Rady 2007/533/SVV ze dne 12. června 2007 o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II),

rozhodnutí Komise 2010/261/EU ze dne 4. května 2010 o bezpečnostním plánu pro centrální SIS II a komunikační infrastrukturu[77].

Článek 75
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 poté, 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.

[77] 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).

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 policejní spolupráce a justiční spolupráce v trestních věcech, o změně nařízení (EU) č. 515/2014 a o zrušení nařízení (ES) č. 1986/2006, rozhodnutí Rady 2007/533/SVV a rozhodnutí Komise 2010/261/EU.

1.2 Příslušné oblasti politik podle členění ABM/ABB[78]

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[79]

☑ 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 – „Narušování organizované trestné činnosti“

Cíl – „Silná reakce EU na terorismus a předcházení radikalizaci“

Nutnost přezkoumat právní základ SIS za účelem řešení nových výzev v oblasti bezpečnosti a migrace zdůraznila Komise již při mnoha příležitostech. Například v „Evropském programu pro bezpečnost“[80] Komise oznámila, že má v úmyslu v letech 2015 a 2016 zhodnotit SIS a posoudit, zda je kvůli novým operačním potřebám třeba provést změny právních předpisů. Kromě toho bylo v programu pro bezpečnost zdůrazněno, že SIS je ústředním prvkem policejní výměny informací a měl by být posílen. Později Komise ve svém sdělení „Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost“[81] uvedla, že další funkce systému budou zváženy na základě celkové hodnotící zprávy za účelem předložení návrhů na revizi právního základu SIS. Dne 20. dubna 2016 pak Komise ve svém sdělení „Naplňování Evropského programu pro bezpečnost v zájmu boje proti terorismu a položení základů účinné a skutečné bezpečnostní unie“[82] navrhla řadu změn SIS, aby se zvýšila jeho přidaná hodnota pro účely prosazování práva.

Celkové hodnocení provedené Komisí potvrdilo operativní úspěšnost SIS. I přes četné úspěchy SIS byla v hodnocení obsažena i řada doporučení, jejichž cílem bylo zlepšit technickou a provozní účinnost a efektivnost systému.

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

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

80 COM(2015) 185 final.

81 COM(2016) 205 final.

82 COM(2016) 230 final.

Na základě doporučení v celkové hodnotící zprávě a plně v souladu s cíli Komise vymezenými ve výše zmíněných sděleních a strategickém plánu GŘ pro migraci a vnitřní věci 2016–2020[83] má tento návrh za cíl:

- uskutečnit záměr Komise zvýšit přidanou hodnotu SIS pro účely prosazování práva v reakci na nové hrozby,
- provést doporučení o technických a procesních změnách, která vyplynula z komplexního hodnocení SIS,
- splnit požadavky koncových uživatelů SIS ohledně technických zlepšení,
- zohlednit prozatímní zjištění expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu, pokud jde o kvalitu údajů.

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. 2.1 – silná reakce EU na terorismus a předcházení radikalizaci,

Specifický cíl č. 2.2 – narušování závažné a organizované přeshraniční trestné činnosti.

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.

Hlavním cílem navrhovaných právních a technických změn v SIS je učinit tento systém z provozního hlediska účinnějším. 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 spolupráce při prosazování práva.

Nový návrh zavádí opatření, jež řeší provozní a technické potřeby koncových uživatelů. Zejména jsou to nová datová pole ve stávajících záznamech, která poskytnou policistům všechny informace nezbytné k účinnému plnění úkolů. Návrh také výslovně zdůrazňuje význam nepřetržité dostupnosti SIS, protože jeho výpadky mohou podstatně ohrozit práci pracovníků donucovacích orgánů. Kromě toho tento návrh stanoví technické změny, díky nimž bude systém účinnější a jednodušší.

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.

Návrh zavádí nové biometrické identifikátory – otisky dlaní, zobrazení obličeje a profily DNA ve specifických a omezených případech. Tato skutečnost ve spojení se zamýšlenými změnami článků 32 a 33 (záznamy o pohřešovaných osobách), které umožní vkládání preventivních záznamů a kategorizaci případů pohřešovaných osob, za prvé významně posílí ochranu nezletilých osob bez doprovodu a za druhé umožní určení jejich totožnosti na základě jejich profilu DNA nebo profilu DNA jejich rodičů a/nebo sourozenců (se souhlasem).

Orgány členských států budou rovněž schopny pořizovat záznamy týkající se neznámých osob hledaných v souvislosti s trestným činem pouze na základě latentních otisků prstů či dlaní nebo otisků prstů či dlaní z místa činu. Ve stávajícím právním a technickém rámci to není možné, a tudíž to představuje významnou změnu.

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 zavedením nových prvků vedle stávajících kategorií záznamů, 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

Jakmile je systém funkční:

Po uvedení systému do provozu agentura eu-LISA zajistí zavedení postupů pro sledování, jak funguje Schengenský informační systém 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 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. Kromě toho bude agentura rovněž poskytovat roční statistiky o využívání funkce, kterou se dočasně znemožňuje vyhledávání záznamu pořízeného podle článku 26 tohoto nařízení, a to celkem a pro každý členský stát jednotlivě, včetně jakéhokoli prodloužení 48hodinové doby použití této funkce.

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 bude předávat hodnotící zprávy Evropskému parlamentu a Radě.

Specifický cíl č. 1 – narušování organizované trestné činnosti

Ukazatel – využívání unijních mechanismů výměny informací. To lze měřit na základě zvýšení počtu pozitivních nálezů v SIS. Ukazateli jsou statistické zprávy vydané agenturou eu-LISA a členskými státy. Tyto ukazatele umožní Komisi posoudit, jak se nové funkce systému využívají.

Specifický cíl č. 2 – silná reakce EU na terorismus a předcházení radikalizaci.

Ukazatel – zvýšení počtu záznamů a pozitivních nálezů, zejména v souvislosti s čl. 36 odst. 3 návrhu u záznamů o osobách a věcech pořízených pro účely skrytých kontrol, vyšetřovacích kontrol nebo zvláštních kontrol.

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. Důkladněji harmonizovat vnitrostátní postupy pro využívání SIS.

3. Rozšířit seznam institucionálních uživatelů s přístupem k údajům SIS poskytnutím úplného přístupu do tohoto systému Europolu a nové Evropské pohraniční a pobřežní stráži.

4. Zavést nové prvky do záznamů SIS a nové funkce, aby byla rozšířena oblast působnosti systému, aby se tento systém mohl vypořádat s nynějším bezpečnostním prostředím, aby se posílila spolupráce mezi donucovacími a bezpečnostními orgány členských států a snížila administrativní zátěž.

5. Vyřešit komplexní využívání všech prvků SIS (end-to-end), které by nejen pokrývalo centrální a vnitrostátní systémy, ale také zajistilo, že koncoví uživatelé obdrží veškeré údaje potřebné k plnění svých úkolů.

6. Posílit kontinuitu provozu a zajistit nepřerušený provoz SIS na centrální a vnitrostátní úrovni.

7. Zesílit boj proti mezinárodní trestné činnosti, terorismu a kyberkriminalitě jakožto vzájemně souvisejícím oblastem s výrazným přeshraničním rozměrem.

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. 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 dosáhl počet vstupů příslušných orgánů členských států do SIS téměř 2,9 miliardy, což jasně prokazuje zásadní podíl tohoto systému na spolupráci při prosazování práva v schengenském prostoru. Decentralizovaná vnitrostátní řešení by takovouto vysokou úroveň výměny informací mezi členskými státy nezajistila a na úrovni členských států 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 členskými státy EU. Europol a nová Evropská agentura pro 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

1. Fáze vývoje by měla být zahájena až po přesném definování provozních potřeb a požadavků koncových uživatelů. 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) průběžné konzultace s příslušnými zúčastněnými stranami, mimo jiné se zástupci ve 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 se velmi transparentně a komplexně projednávají na zvláštních setkáních a pracovních seminářích. 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 dvou studií, jejichž výsledky byly při vypracovávání tohoto návrhu zohledněny:

– Technický posudek SIS – v tomto posudku byly vymezeny klíčové otázky pro fungování SIS a budoucí potřeby, které by měly být zváženy. Také v něm 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 – 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.

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.

Tento návrh je dále úzce provázán s dalšími politikami Unie a doplňuje je, konkrétně jde o tyto politiky:

a) vnitřní bezpečnost, jak je zdůrazněno v Evropském programu pro bezpečnost[85], s cílem předcházet, odhalovat, vyšetřovat a stíhat závažné a teroristické trestné činy tím, že se umožní donucovacím orgánům zpracovávat osobní údaje osob, u nichž existuje podezření, že se podílejí na teroristických činech nebo závažných trestných činech;

b) ochrana údajů, neboť 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) Evropská pohraniční a pobřežní stráž[86], pokud jde za prvé o možnost, aby pracovníci agentury prováděli analýzy rizik, a za druhé o jejich přístup do SIS pro účely navrhovaného systému ETIAS. Účelem návrhu je také poskytnout technické rozhraní pro přístup do SIS jednotkám Evropské pohraniční a pobřežní stráže,

84 COM(2016) 205 final.

85 COM(2015) 185 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).

týmům pracovníků, kteří se podílejí na úkolech spojených s navracením, a členům podpůrného týmu 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;

b) Europol, neboť tento návrh uděluje Europolu v rámci jeho mandátu další práva na přístup a vyhledávání v údajích vložených do SIS;

c) Prümské rozhodnutí[87], neboť nová ustanovení tohoto návrhu umožňující určení totožnosti osob na základě otisků prstů (jakož i zobrazení obličeje a profilů DNA) doplňují stávající prümská ustanovení o vzájemném přeshraničním on-line přístupu k určeným vnitrostátním databázím DNA a automatizovaným systémům pro identifikaci otisků prstů.

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

a) správa vnějších hranic. Návrh doplňuje zamýšlenou novou zásadu pro Schengenský hraniční kodex spočívající v provádění systematických kontrol všech cestujících, včetně státních příslušníků EU, na základě příslušných databází při vstupu do schengenského prostoru a výstupu z něj, která se zavádí jako reakce na fenomén zahraničních teroristických bojovníků;

b) systém vstupu/výstupu[88] (EES), neboť cílem tohoto návrhu je zohlednit navrhované použití kombinace otisků prstů a zobrazení obličeje jako biometrických identifikátorů pro provoz EES.

c) systém ETIAS, neboť návrh zohledňuje navrhovaný systém ETIAS, jehož účelem je důkladné posuzování státních příslušníků třetích zemí, kteří mají v úmyslu cestovat do EU, z bezpečnostního hlediska, včetně jejich ověření v SIS.

[87] Rozhodnutí Rady 2008/615/SVV ze dne 23. června 2008 o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti (Úř. věst. L 210, 6.8.2008, s. 1); rozhodnutí Rady 2008/616/SVV ze dne 23. června 2008 o provádění rozhodnutí 2008/615/SVV o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti (Úř. věst. L 210, 6.8.2008, s. 12).

[88] 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

- Přípravné období 2017

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

– poté plné fungování.

1.7 Předpokládaný způsob řízení[89]

☑**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 (SIS) v oblasti hraničních kontrol) by proto měly být považovány nikoli za dvě oddělené částky, ale za jedinou. Rozpočtové důsledky změn vyžadovaných

[89] 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.

pro provedení obou návrhů jsou proto uvedeny v jediném legislativním finančním výkazu.

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 obsahuje ustanovení (čl. 71 odst. 7 a 8) 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, a 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 nařízení v souvislosti s centrálním systémem;

d) vyhodnocení zabezpečení centrálního systému;

e) zhodnocení dopadů budoucího fungování systému.

Dále má agentura eu-LISA 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.

2.2 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 eu-LISA 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 eu-LISA.

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[90]	zemí ESVO[91]	kandidátských zemí[92]	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

[90] RP = rozlišené prostředky / NRP = nerozlišené prostředky.

[91] ESVO: Evropské sdružení volného obchodu.

[92] 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 na OKRUH <….>	Závazky	=4+6								
	Platby	=5+6								

víceletého finančního rámce										

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“

		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								

v milionech EUR (zaokrouhleno na tři desetinná místa)

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

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **N**[93]	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								

3.2.3.1 Odhadovaný dopad na operační prostředky GŘ HOME

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

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

– ☑ 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[94]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 1[95] 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

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

[95] Popsaný v bodě 1.4.2 „Specifické cíle…“

3.2.3.2 Odhadovaný dopad na operační prostředky eu-LISA

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

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

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

Uveďte cíle a výstupy ⇩			Rok **2018**		Rok **2019**		Rok **2020**		Vložit počet let podle trvání finančního dopadu (viz bod 1.6)						**CELKEM**			
	VÝSTUPY																	
	Druh[96]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 1[97] Vývoj centrálního systému																		
– Externí			1	5,013														5,013
– Programové			1	4,050														4,050
– Technické			1	3,692														3,692
Mezisoučet za specifický cíl č. 1				12,755														12,755
SPECIFICKÝ CÍL Č. 2 Údržba centrálního systému																		
– Externí			1	0	1	0,365	1	0,365										0,730
Programové			1	0	1	0,810	1	0,810										1,620
Technické			1	0	1	0,738	1	0,738										1,476
Mezisoučet za specifický cíl č. 2						1,913		1,913										3,826

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

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

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

3.2.3.3 Odhadovaný dopad na lidské zdroje eu-LISA

Shrnutí

– ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

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

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **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)**[98]								
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** [99]	– 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	

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

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

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 související s modernizací funkcí SIS II 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[100]						
		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*.

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