EVROPSKÁ UNIE

EVROPSKÝ PARLAMENT **RADA**

Brusel 28. listopadu 2018
(OR. en)

2016/0409 (COD)
LEX 1849

PE-CONS 36/1/18
REV 1

SIRIS 71
ENFOPOL 337
COPEN 222
SCHENGEN 30
COMIX 335
CODEC 1126

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 A O ZRUŠENÍ ROZHODNUTÍ RADY 2007/533/SVV
A O ZRUŠENÍ NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY
(ES) č. 1986/ 2006 A ROZHODNUTÍ KOMISE 2010/261/EU

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

(EU) 2018/...

ze dne 28. listopadu 2018

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

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[1],

[1] Postoj Evropského parlamentu ze dne 24. října 2018 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne 19. listopadu 2018.

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 kompenzačních opatření přispívajících k udržení vysokého stupně bezpečnosti v prostoru svobody, bezpečnosti a práva Unie prostřednictvím podpory operativní spolupráce mezi příslušnými vnitrostátními orgány, zejména pohraniční stráží, policií, celními orgány, imigračními orgány a orgány odpovědnými za prevenci, odhalování, vyšetřování či stíhání trestných činů nebo výkon trestů.

(2) SIS byl původně 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[1] (dále jen „Úmluva k provedení Schengenské dohody“). Vývoj SIS druhé generace (dále jen „SIS II“) byl svěřen Komisi na základě nařízení Rady (ES) č. 2424/2001[2] a rozhodnutí Rady 2001/886/SVV[3]. Tento systém byl posléze zřízen nařízením Evropského parlamentu a Rady (ES) č. 1987/2006[4] a rozhodnutím Rady 2007/533/SVV[5]. SIS II nahradil SIS vytvořený na základě Úmluvy k provedení Schengenské dohody.

---

1 Úř. věst. L 239, 22.9.2000, s. 19.

2 Nařízení Rady (ES) č. 2424/2001 ze dne 6. prosince 2001 o vývoji Schengenského informačního systému druhé generace (SIS II)(Úř. věst. L 328, 13.12.2001, s. 4.).

3 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).

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

5 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).

(3) Po třech letech od uvedení SIS II do provozu provedla Komise vyhodnocení tohoto systému v souladu s nařízením (ES) č. 1987/2006 a s rozhodnutím 2007/533/SVV. Dne 21. prosince 2016 předložila Komise Evropskému parlamentu a Radě zprávu 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. Doporučení uvedená v těchto dokumentech by měla být v tomto nařízení vhodně zohledněna.

(4) Toto nařízení představuje právní základ pro SIS v souvislosti se záležitostmi spadajícími do oblasti působnosti části třetí hlavy V kapitol 4 a 5 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“). Nařízení Evropského parlamentu a Rady (EU) 2018/...[1+] představuje právní základ pro SIS v souvislosti se záležitostmi spadajícími do oblasti působnosti části třetí hlavy V kapitoly 2 Smlouvy o fungování EU.

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2018/... ze dne ... o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol, o změně Úmluvy k provedení Schengenské dohody a o změně a zrušení nařízení (ES) č. 1987/2006 (Úř. věst. L …).

[+] Pro Úř. věst.*:* vložte prosím v textu číslo nařízení obsaženého v dokumentu PE-CONS 35/18 a doplňte odpovídajícím způsobem poznámku pod čarou.

(5) Skutečnost, že právní základ pro SIS sestává ze samostatných právních předpisů, nemá dopad na zásadu, že SIS představuje jednotný informační systém, který by měl fungovat jako takový. Měl by zahrnovat jednotnou síť národních orgánů, označovaných jako centrály SIRENE, které zajišťují výměnu doplňujících informací. Proto by určitá ustanovení těchto předpisů měla být totožná.

(6) Je nezbytné konkrétně vymezit účely SIS, určité prvky jeho technické architektury a jeho financování, stanovit pravidla pro komplexní provoz a využívání všech prvků tohoto systému a vymezit příslušné povinnosti. Je nezbytné rovněž stanovit kategorie údajů vkládaných do systému, účely jejich vkládání a zpracování a kritéria pro jejich vkládání. Je třeba rovněž přijmout pravidla upravující výmaz záznamů, orgány oprávněné k přístupu k údajům, používání biometrických údajů a blíže stanovit další pravidla týkající se ochrany údajů a zpracování údajů.

(7) Záznamy v SIS obsahují pouze informace nezbytné k identifikaci osoby nebo věci a ohledně opatření, jež má být přijato. Členské státy by si proto měly v případě potřeby vyměňovat doplňující informace týkající se záznamů.

(8) SIS zahrnuje centrální systém (dále jen „centrální SIS“) a vnitrostátní systémy. Vnitrostátní systémy mohou obsahovat úplnou nebo částečnou kopii databáze SIS, která může být sdílena dvěma či více členskými státy. Vzhledem k tomu, že SIS je nejdůležitějším nástrojem výměny informací v Evropě pro zajištění bezpečnosti a účinné správy hranic, je nezbytné zajistit jeho nepřetržitý provoz na centrální i na vnitrostátní úrovni. Dostupnost SIS by měla být předmětem pečlivého sledování na centrální úrovni i na úrovni členských států a všechny případy nedostupnosti pro koncové uživatele by měly být zaznamenány a nahlášeny zúčastněným stranám na vnitrostátní úrovni a na úrovni Unie. Všechny členské státy by měly zřídit národní záložní systém. Členské státy by rovněž měly zajistit nepřetržité propojení s centrálním SIS prostřednictvím zdvojených, fyzicky a zeměpisně oddělených bodů připojení. Centrální SIS a komunikační infrastruktura by měly být provozovány tak, aby bylo zajištěno jejich fungování 24 hodin denně sedm dní v týdnu. Agentura Evropské unie pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (dále jen „agentura eu-LISA“), zřízená nařízením Evropského parlamentu a Rady (EU) 2018/...[1+], by proto měla zavést technická řešení na posílení nepřetržité dostupnosti SIS, podléhající nezávislému posouzení dopadů a analýze nákladů a přínosů.

---

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

\+ Pro Úř. věst.: vložte prosím v textu číslo nařízení obsaženého v dokumentu PE-CONS 29/18 a v poznámce pod čarou jeho číslo, datum přijetí a odkaz na vyhlášení v Úředním věstníku.

(9) Je nutné vést aktualizovanou příručku obsahující podrobná pravidla pro výměnu doplňujících informací týkajících se opatření, která záznam vyžaduje (příručka SIRENE). Centrály SIRENE by měly zajistit rychlou a účinnou výměnu těchto informací.

(10) Aby byla zajištěna účinná výměna doplňujících informací, včetně 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 dožádání obdržených z jiných centrál SIRENE.

(11) Členské státy by měly zajistit, aby pracovníci jejich centrály SIRENE měli jazykové dovednosti a znalosti příslušných právních předpisů a procesních pravidel nezbytné pro plnění svých úkolů.

(12) Pro plné využití funkcí SIS by členské státy měly zajistit, aby byli koncoví uživatelé a pracovníci centrál SIRENE pravidelně proškolováni, mimo jiné v oblasti bezpečnosti, ochrany údajů a kvality údajů. Centrály SIRENE by se měly podílet na vývoji programů odborné přípravy. Centrály SIRENE by měly pokud možno také zorganizovat alespoň jednou ročně výměnu pracovníků s ostatními centrálami SIRENE. Členské státy se vyzývají, aby přijaly vhodná opatření k zamezení úbytku dovedností a odborné praxe v důsledku odchodů pracovníků.

(13) Provozní řízení centrálních složek SIS vykonává agentura eu-LISA. Aby agentura eu-LISA mohla vyčlenit nezbytné finanční a personální zdroje na pokrytí všech aspektů provozního řízení centrálního SIS a komunikační infrastruktury, mělo by toto nařízení podrobně vymezit její úkoly, zejména pokud jde o technické aspekty výměny doplňujících informací.

(14) Aniž je dotčena odpovědnost členských států za správnost údajů vkládaných do SIS a úloha centrál SIRENE jakožto koordinátorů kvality, měla by být agentura eu-LISA zodpovědná za zlepšování kvality údajů zavedením centrálního nástroje pro sledování kvality údajů a měla by Komisi a členským státům předkládat zprávy v pravidelných intervalech. Komise by měla podávat Evropskému parlamentu a Radě zprávy o problémech, které se vyskytly ohledně kvality údajů. Pro další zlepšení kvality údajů v SIS by agentura eu-LISA rovněž měla nabízet školení ohledně používání SIS pro vnitrostátní školící subjekty a pokud možno také pro centrály SIRENE a koncové uživatele.

(15) Aby bylo možno lépe sledovat využívání SIS a analyzovat vývoj, pokud jde o trestné činy, měla by být agentura eu-LISA schopna vytvořit kapacitu na nejvyšší úrovni pro statistické hlášení členským státům, Evropskému parlamentu, Radě, Komisi, Europolu, Eurojustu a Evropské agentuře pro pohraniční a pobřežní stráž, aniž by byla ohrožena neporušenost údajů. Mělo by být proto zřízeno centrální úložiště údajů. Statistiky uchovávané v úložišti nebo obdržené od úložiště by neměly obsahovat žádné osobní údaje. Členské státy by měly v rámci spolupráce mezi dozorovými úřady a Evropským inspektorem ochrany údajů podle tohoto nařízení poskytovat statistické údaje týkající se výkonu práva přístupu, oprav nesprávných údajů a výmazu protiprávně uchovávaných údajů.

(16) V SIS by měly být zavedeny nové kategorie údajů, aby koncoví uživatelé mohli na základě záznamu činit informovaná rozhodnutí bez ztráty času. Za účelem usnadnění identifikace a odhalování vícenásobných totožností by proto měl být v záznamu dále uveden odkaz na doklad totožnosti dotčené osoby, jeho číslo včetně kopie, pokud možno barevné, takového dokladu, jsou-li tyto informace k dispozici.

(17) Příslušné orgány by měly mít možnost ve zcela nezbytných případech vkládat do SIS konkrétní informace související s jakýmikoli zvláštními objektivními a nezměnitelnými tělesnými znaky dotčené osoby, jako jsou například tetování, znaménka nebo jizvy.

(18) Jsou-li k dispozici, měly by být při vytváření záznamu vkládány veškeré relevantní údaje dotčené osoby, zejména jméno, aby bylo minimalizováno riziko falešných pozitivních nálezů a nadbytečných operativních činností.

(19) SIS by neměl uchovávat žádné údaje použité k vyhledávání s výjimkou protokolů umožňujících ověřit, zda je vyhledávání v souladu se zákonem, za účelem sledování zákonnosti zpracovávání údajů, pro vlastní kontrolu, pro zajištění řádného fungování národních systémů, neporušenosti údajů a jejich zabezpečení.

(20) SIS by měl umožnit zpracování biometrických údajů s cílem napomoci spolehlivé identifikaci dotyčných osob. Žádné vložení a použití fotografií, zobrazení obličeje a daktyloskopických údajů do SIS by nemělo překročit rámec toho, co je nezbytné pro splnění sledovaných cílů, veškerá tato vložení a použití by měla být založena na právu Unie, brát ohled na základní práva, včetně nejlepšího zájmu dítěte, a být v souladu s právem Unie v oblasti ochrany údajů, včetně příslušných ustanovení o ochraně údajů stanovených v tomto nařízení. Ve stejném smyslu by měl SIS umožňovat rovněž zpracování údajů o osobách, jejichž totožnost byla zneužita, aby se předešlo nežádoucím důsledkům způsobeným chybnou identifikací, s výhradou vhodných záruk, a to se souhlasem dotyčné osoby pro každou kategorii údajů a zejména pro otisky dlaní, a za přísného omezení účelů, pro něž se tyto osobní údaje mohou zákonným způsobem zpracovávat.

(21) Členské státy by měly přijmout nezbytná technická opatření, aby pokaždé, když jsou koncoví uživatelé oprávněni provést vyhledávání ve vnitrostátní policejní nebo imigrační databázi, vyhledávali také souběžně v SIS, v souladu se zásadami stanovenými v článku 4 směrnice Evropského parlamentu a Rady (EU) 2016/680[1] a článku 5 nařízení Evropského parlamentu a Rady (EU) 2016/679[2]. 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.

(22) Toto nařízení by mělo stanovit podmínky pro používání daktyloskopických údajů, fotografií a zobrazení obličeje pro účely identifikace a ověření totožnosti. Rozpoznávání zobrazení obličejů a fotografie by se pro účely identifikace měly zpočátku používat pouze v rámci řádných hraničních přechodů. Komise by měla k takovému používání vypracovat zprávu, která potvrdí dostupnost, spolehlivost a připravenost této technologie.

---

[1] 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).

[2] 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).

(23) Zavedení služby automatizovaného porovnávání 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, jak je stanoveno v rozhodnutích Rady 2008/615/SVV[1] a 2008/616/SVV[2]. Vyhledávání daktyloskopických údajů v SIS umožňuje aktivně vyhledávat pachatele. Proto by mělo být možné vkládat do SIS daktyloskopické údaje neznámého pachatele, a to za předpokladu, že vlastníka daných údajů lze s velmi vysokou pravděpodobností označit za pachatele závažného trestného činu nebo teroristického činu. Jde zejména o případy, kdy jsou daktyloskopické údaje nalezeny na zbrani nebo jakékoli jiné věci použité při spáchání daného trestného činu. Z pouhého výskytu daktyloskopických údajů na místě činu by nemělo být vyvozováno, že jde s velmi vysokou pravděpodobností o daktyloskopické údaje pachatele. Další podmínkou pro vytvoření takového záznamu by mělo být, že podezřelou osobu nelze identifikovat na základě údajů z jiných relevantních vnitrostátních, unijních nebo mezinárodních databází. Pokud by se na základě tohoto vyhledávání daktyloskopických údajů zjistila možná shoda, měl by daný členský stát provést další kontrolu se zapojením znalců, s cílem zjistit, zda je podezřelá osoba vlastníkem otisků uložených v SIS, a měl by identifikovat osobu. Příslušné postupy by měly být upraveny vnitrostátním právem. Taková identifikace by mohla podstatně přispět k vyšetřování a mohla by vést k zatčení za předpokladu, že jsou splněny všechny podmínky pro zatčení.

---

1 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).

2 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).

(24) Mělo by být umožněno porovnávání úplných nebo neúplných souborů otisků prstů či otisků dlaní nalezených na místě činu s daktyloskopickými údaji uloženými v SIS, pokud lze s vysokou mírou pravděpodobnosti stanovit, že patří pachateli závažného trestného činu nebo teroristického trestného činu, a to za předpokladu, že se současně provádí vyhledávání i v příslušných vnitrostátních databázích otisků prstů. Zvláštní pozornost by měla být věnována zavedení norem kvality upravujících uchovávání biometrických údajů, včetně latentních daktyloskopických údajů.

(25) V případě, že není možné identifikovat určitou osobu jinými prostředky, mělo by být k pokusu ji identifikovat využito daktyloskopických údajů. Ve všech případech by mělo být přípustné identifikovat určitou osoby pomocí daktyloskopických údajů.

(26) V jasně vymezených případech, kdy nejsou dostupné daktyloskopické údaje, by mělo být možné do záznamu doplnit profil DNA. Tento profil DNA by měl být přístupný pouze oprávněným uživatelům. Profily DNA by měly usnadnit identifikaci pohřešovaných osob, které potřebují ochranu, a zejména pohřešovaných dětí, a to mimo jiné tím, že bude možné k identifikaci použít profily DNA jejich přímých předků, potomků či sourozenců. Údaje o DNA by měly obsahovat pouze minimum informací nezbytných k identifikaci pohřešované osoby.

(27) Profily DNA by se ze SIS měly získávat pouze v případě, že identifikace je nezbytná a přiměřená pro účely uvedené v tomto nařízení. Profily DNA by neměly být získávány a zpracovávány za jiným účelem, než pro který byly vloženy do SIS. Měla by se uplatnit pravidla pro ochranu údajů a pro bezpečnost stanovená v tomto nařízení. V případě potřeby by se při používání profilů DNA měly zavést dodatečné záruky za účelem předcházení rizikům týkajícím se falešných shod, útoků hackerů a neoprávněného sdílení se třetími stranami.

(28) SIS by měl obsahovat záznamy o osobách hledaných za účelem zatčení a předání a osobách hledaných za účelem zatčení a vydání. Je vhodné, aby byla kromě záznamů umožněna i výměna doplňujících informací prostřednictvím centrál SIRENE nezbytných pro postupy předávání a vydávání. V SIS by se měly zpracovávat zejména údaje uvedené v článku 8 rámcového rozhodnutí Rady 2002/584/SVV[1]. Z operativních důvodů je vhodné, aby vkládající členský stát s povolením justičních orgánů dočasně znemožnil vyhledávání existujícího záznamu 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 v zásadě neměla přesáhnout 48 hodin.

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

---

[1] 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).

(30) SIS by měl obsahovat záznamy o pohřešovaných nebo zranitelných osobách, kterým je třeba zabránit v cestování s cílem zajistit jejich ochranu nebo předejít ohrožení veřejné bezpečnosti nebo veřejného pořádku. V případech dětí by tyto záznamy a příslušné postupy měly sloužit nejlepšímu zájmu dítěte v souladu s článkem 24 Listiny základních práv Evropské unie a článkem 3 Úmluvy Organizace spojených národů o právech dítěte ze dne 20. listopadu 1989. Opatření a rozhodnutí, která příslušné orgány, včetně justičních orgánů, přijímají v návaznosti na záznam o dítěti, by měla být přijímána ve spolupráci s orgány pro ochranu dětí. V příhodných případech by měla být informována vnitrostátní tísňová linka pro případy pohřešovaných dětí.

(31) Na žádost příslušného orgánu by měly být vkládány údaje o pohřešovaných osobách, které musí být umístěny pod ochranu. Všechny děti, které jsou pohřešovány y přijímacích azylových střediscích v členských státech, by měly být v SIS předmětem záznamu o pohřešovaných osobách.

(32) Záznamy o dětech, kterým hrozí tzv. rodičovský únos, by měly být do SIS vkládány na žádost příslušných orgánů, včetně justičních orgánů příslušných ve věcech rodičovské zodpovědnosti podle vnitrostátního práva. Záznamy o dětech, kterým hrozí tzv. rodičovský únos, by měly být do SIS vkládány, pouze pokud je toto riziko konkrétní a zjevné a pouze ve vymezených situacích. Proto je nezbytné stanovit přesně vymezené a vhodné záruky. Při posuzování toho, zda existuje konkrétní a zjevné riziko, že by dítě mohlo být bezprostředně a protiprávně přemístěno z členského státu, by měl příslušný orgán zohlednit osobní poměry a prostředí, jimž je dítě vystaveno.

(33) Toto nařízení by mělo vytvořit nový druh záznamů pro některé kategorie zranitelných osob, kterým je třeba zabránit v cestování. Za zranitelné je třeba považovat osoby, kterým je třeba s ohledem na jejich věk, zdravotní postižení nebo rodinné poměry poskytnout ochranu.

(34) Záznamy o dětech, kterým je třeba zabránit v cestování v zájmu jejich vlastní ochrany, by měly být do SIS vkládány, hrozí-li konkrétní a zjevné riziko, že budou přemístěny z území členského státu nebo toto území opustí. Tyto záznamy by měly být vkládány v případě, že je s cestou spojeno riziko, že se děti stanou oběťmi obchodování s lidmi, riziko nuceného sňatku, mrzačení ženských pohlavních orgánů nebo jiných forem násilí na základě pohlaví, nebo riziko, že se stanou oběťmi nebo se zapojí do teroristických trestných činů, či riziko, že budou odvedeny a začleněny do ozbrojených skupin nebo přinuceny k aktivní účasti na páchání násilností.

(35) Záznamy o zranitelných dospělých osobách, kterým je třeba zabránit v cestování v zájmu jejich vlastní ochrany, by měly být vkládány v případě, že je s cestou spojeno riziko, že se stanou oběťmi obchodování s lidmi nebo násilí založeného na pohlaví.

(36) V zájmu zajištění přesně vymezených a vhodných záruk by záznamy o dětech a jiných zranitelných osobách, kterým je třeba zabránit v cestování, měly být, vyžaduje-li to vnitrostátní právo, vkládány do SIS na základě rozhodnutí justičního orgánu nebo rozhodnutí příslušného orgánu potvrzeného justičním orgánem.

(37) Mělo by být zavedeno nové opatření umožňující zastavení a podání vysvětlení určitou osobou, aby mohl vkládající členský stát získat co nejpodrobnější informace. Toto opatření by mělo být uplatněno v případě, kdy je určitá osoba na základě jasných indicií podezřelá, že má v úmyslu spáchat nebo spáchala některý z trestných činů uvedených v čl. 2 odst. 1 a 2 rámcového rozhodnutí 2002/584/ SVV, kdy jsou zapotřebí další informace pro účely výkonu trestu odnětí svobody či ochranného opatření spojeného se zbavením osobní svobody, které byly uloženy osobě odsouzené za některý z trestných činů uvedených v čl. 2 odst. 1 a 2 rámcového rozhodnutí 2002/584/SVV, nebo pro případy, kdy existují důvody se domnívat, že tato osoba některý z těchto trestných činů spáchá. Tímto opatřením by rovněž neměly být dotčeny stávající mechanismy vzájemné právní pomoci. Mělo by poskytnout dostatek informací k rozhodnutí o dalších krocích. Toto nové opatření by nemělo zahrnovat osobní prohlídku dané osoby, ani vést k jejímu zatčení. Měla by být zachována procesní práva podezřelých a obviněných osob podle unijního a vnitrostátního práva, včetně jejich práva na přístup k obhájci v souladu se směrnicí Evropského parlamentu a Rady 2013/48/EU[1].

(38) V případě záznamů o věcech hledaných za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení by tyto věci měly být zabaveny v souladu s vnitrostátním právem, které stanoví, zda a za jakých podmínek se určitá věc zabavuje, a to zejména v případě, že daná věc je v držení jejího právoplatného vlastníka.

[1] Směrnice Evropského parlamentu a Rady 2013/48/EU ze dne 22. října 2013 o právu na přístup k obhájci v trestním řízení a řízení týkajícím se evropského zatýkacího rozkazu a o právu na informování třetí strany a právu na komunikaci s třetími osobami a konzulárními úřady v případě zbavení osobní svobody (Úř. věst. L 294, 6.11.2013, s. 1).

(39) SIS by měl obsahovat nové kategorie věcí s vysokou hodnotou, jako jsou například IT zařízení, které lze identifikovat a vyhledávat pomocí jedinečného identifikačního čísla.

(40) Pokud jde o záznamy vkládané do o dokladech za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení, měl by být pojem „falešné“ vykládán tak, že zahrnuje doklady jak padělané, tak pozměněné.

(41) Členský stát by měl mít možnost opatřit záznam upozorněním zvaným označení, v jehož důsledku opatření, které má být na základě záznamu přijato, nebude přijato na jeho území. Pokud se vkládají záznamy za účelem zatčení a předání, nesmí být žádné ustanovení tohoto nařízení vykládáno tak, aby se odchylovalo od ustanovení uvedených v rámcovém rozhodnutí 2002/584/SVV nebo bránilo jejich použití. Rozhodnutí opatřit záznam označením proto, aby nebyl vykonán evropský zatýkací rozkaz, by se mělo zakládat pouze na důvodech pro zamítnutí uvedených ve zmíněném rámcovém rozhodnutí.

(42) 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 justičnímu orgánu, který vložil záznam a který může rozhodnout o předání evropského zatýkacího rozkazu příslušnému justičnímu orgánu v souladu s ustanoveními rámcového rozhodnutí 2002/584/SVV.

(43) Členským státům by mělo být umožněno zavést propojení mezi záznamy v SIS. Vytvoření propojení mezi dvěma nebo více záznamy by nemělo mít dopad na přijímaná opatření, na délku doby pro přezkum záznamů ani na práva přístupu k záznamům.

(44) Záznamy by v SIS neměly být uchovávány po dobu delší, než je nezbytné pro splnění konkrétních účelů, pro které byly vloženy. Lhůty pro přezkum jednotlivých kategorií záznamů by měly odpovídat jejich účelu. Záznamy o věcech, které jsou propojeny se záznamy o osobách, by měly být uchovávány pouze po dobu, kdy je uchováván záznam o osobě. Rozhodnutí o uchování záznamů o osobách by měla vycházet ze souhrnného individuálního posouzení. Členské státy by měly záznamy o osobách a věcech přezkoumávat během stanoveného období pro přezkum a měly by vést statistiku o počtu záznamů, u nichž byla doba uchovávání prodloužena.

(45) Na vložení záznamu do SIS a prodloužení doby jeho platnosti by se měl vztahovat požadavek přiměřenosti spočívající v posouzení, zda je daný případ dostatečně přiměřený, relevantní a závažný, aby odůvodňoval vložení záznamu do SIS V případě teroristických trestných činů by měl být daný případ považován za dostatečně přiměřený, relevantní a závažný pro to, aby odůvodňoval záznam do SIS. Ve výjimečných případech by měly mít členské státy možnost z důvodů veřejné nebo národní bezpečnosti od vložení záznamu do SIS upustit, pokud je pravděpodobné, že bude bránit úředním nebo právním šetřením, vyšetřování nebo postupům.

(46) Je třeba stanovit pravidla pro výmaz 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 stanovení 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.

(47) Neporušenost údajů SIS má prvořadý význam. Proto by měly být stanoveny odpovídající záruky pro zpracování údajů SIS na centrální i na vnitrostátní úrovni s cílem zajistit komplexní (end-to-end) zabezpečení údajů. Orgány, které se zabývají zpracováním údajů, by měly být vázány bezpečnostními požadavky uvedenými v tomto nařízení a měly by se řídit jednotným postupem hlášení incidentů. Jejich personál by měl být řádně proškolen a měl by být informován o případných trestných činech a sankcích v této souvislosti.

(48) Údaje zpracovávané v SIS a související doplňující informace vyměněné podle tohoto nařízení by neměly být poskytovány ani zpřístupňovány žádným třetím zemím nebo mezinárodním organizacím.

(49) Je vhodné poskytnout přístup do SIS subjektům odpovědným za registraci vozidel, plavidel a letadel, aby mohly ověřit, zda není určitý dopravní prostředek hledán v členských státech za účelem zabavení. Je rovněž vhodné poskytnout přístup do SIS subjektům odpovědným za registraci střelných zbraní, aby mohly ověřit, zda se určitá střelná zbraň již nehledá v členských státech za účelem zabavení nebo zda existuje záznam o osobě žádající o registraci této zbraně.

(50) Přímý přístup do SIS by měl být poskytnut pouze příslušným subjektům veřejné správy. Tento přístup by měl být omezen na záznamy o příslušných dopravních prostředcích a jejich registračních dokladech či značkách nebo o střelných zbraních a osobách žádajících o jejich registraci. Jakýkoli pozitivní nález v SIS by tyto orgány veřejné správy měly oznámit policejním orgánům, které by měly přijmout další opatření v souladu s konkrétním záznamem v SIS a oznámit vkládajícímu členskému státu daný pozitivní nález prostřednictvím centrály SIRENE.

(51) Aniž jsou dotčena konkrétnější pravidla stanovená v tomto nařízení, měly by se na zpracování, včetně shromažďování a sdělování osobních údajů příslušnými vnitrostátními orgány podle tohoto nařízení pro účely prevence, odhalování, vyšetřování či stíhání teroristických trestných činů či jiných závažných trestných činů nebo výkonu trestů vztahovat vnitrostátní právní a správní předpisy přijaté podle směrnice (EU) 2016/680. Na přístup k údajům vloženým do SIS a na právo v těchto údajích vyhledávat ze strany příslušných vnitrostátních orgánů odpovědných za prevenci, odhalování, vyšetřování či stíhání teroristických trestných činů či jiných závažných trestných činů nebo výkonu trestů se vztahují veškerá příslušná ustanovení tohoto nařízení a ustanovení směrnice (EU) 2016/680, jak je provedena ve vnitrostátním právu; zejména se na ně vztahuje monitorování ze strany dozorových úřadů podle směrnice (EU) 2016/680.

(52) Aniž jsou dotčena konkrétnější pravidla stanovená v tomto nařízení týkající se zpracování osobních údajů, mělo by se na zpracování osobních údajů členskými státy podle tohoto nařízení vztahovat nařízení (EU) 2016/679, s výjimkou případů, kdy toto zpracování provádějí příslušné vnitrostátní orgány pro účely prevence, vyšetřování, odhalování nebo stíhání teroristických trestných činů či jiných závažných trestných činů.

(53) Nařízení Evropského parlamentu a Rady (EU) 2018/...[1+] by se mělo vztahovat na zpracování osobních údajů orgány a institucemi Unie při plnění jejich úkolů podle tohoto nařízení.

(54) Na zpracování osobních údajů Europolem podle tohoto nařízení by se mělo vztahovat nařízení Evropského parlamentu a Rady (EU) 2016/794[2].

(55) V případech, kdy vyhledávání provedená národními členy Eurojustu a jejich asistenty v SIS odhalí existenci záznamu vloženého členským státem, Eurojust nemůže přijmout požadované opatření. Měl by proto uvědomit dotčený členský stát, aby tento členský stát mohl na případu dále pracovat.

---

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

\+ Úř. věst.: vložte prosím v textu číslo nařízení obsaženého v dokumentu PE-CONS 31/18 a v poznámce pod čarou uveďte číslo, datum a odkaz na vyhlášení uvedeného nařízení v Úředním věstníku.

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

(56) Při používání SIS by měly příslušné orgány zajistit, aby byla respektována lidská důstojnost a integrita osoby, jejíž údaje jsou zpracovávány. Zpracovávání osobních údajů pro účely tohoto nařízení nemá vést k diskriminaci osob na základě pohlaví, rasového či etnického původu, náboženského vyznání nebo přesvědčení, zdravotního postižení, věku nebo sexuální orientace.

(57) 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 stanoveného nařízením Rady (EHS, Euratom, ESUO) č. 259/68[1] (dále jen „služební řád“).

(58) Členské státy i agentura eu-LISA by měly mít bezpečnostní plány s cílem usnadnit plnění bezpečnostních povinností a měly by vzájemně spolupracovat s cílem společně řešit bezpečnostní otázky.

[1] Úř. věst. L 56, 4.6.1968, s. 1.

(59) Nezávislé vnitrostátní dozorové úřady uvedené v nařízení (EU) 2016/679 a ve směrnici (EU) 2016/680 (dále jen „dozorové úřady“) by měly sledovat zákonnost zpracování osobních údajů členskými státy podle tohoto nařízení, včetně výměny doplňujících informací. Dozorovým úřadům by měly být na plnění tohoto úkolu přiděleny dostatečné zdroje. Je třeba stanovit práva přístupu subjektů údajů k jejich údajům uchovávaným v SIS a práva na jejich opravu a výmaz, jakož i následnou právní ochranu poskytovanou vnitrostátními soudy a vzájemné uznávání soudních rozhodnutí. Rovněž je vhodné požadovat od členských států roční statistiky.

(60) Dozorové úřady by v rámci svého členského státu měly zajistit, aby alespoň jednou za čtyři roky byl v souladu s mezinárodními auditorskými standardy proveden audit činnosti zpracování údajů v jejich vnitrostátních systémech. Audit by měly provádět dozorové úřady, nebo by si jej dozorové úřady měly přímo vyžádat od nezávislého auditora pro ochranu údajů. Nezávislý auditor by měl i nadále podléhat kontrole a pravomoci příslušného dozorového úřadu či dozorových úřadů, které by proto měly samy dávat instrukce auditorovi a uvést jasně vymezený účel, rozsah a metodiku auditu, jakož i poskytnout vedení a dohled nad auditem a jeho konečnými výsledky.

(61) Evropský inspektor ochrany údajů by měl sledovat činnosti orgánů a institucí Unie související se zpracováváním osobních údajů podle tohoto nařízení. Evropský inspektor ochrany údajů a dozorové úřady by měli při sledování systému SIS vzájemně spolupracovat.

(62) Evropskému inspektorovi ochrany údajů by měly být přiděleny dostatečné zdroje k plnění úkolů, které jsou mu svěřeny tímto nařízením, včetně pomoci odborníků na biometrické údaje.

(63) Nařízení (EU) 2016/794 stanoví, že Europol má podporovat a posilovat činnost příslušných vnitrostátních orgánů, jakož i jejich vzájemnou spolupráci při boji proti terorismu a závažné trestné činnosti, a poskytovat analýzy a posouzení hrozeb. Rozšíření práv přístupu Europolu k záznamům o pohřešovaných osobách by mělo dále zlepšit schopnost Europolu poskytovat vnitrostátním orgánům pro vymáhání práva komplexní operativní 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 přístupu Europolu k záznamům 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, kdy pachatelé často tvrdí, že mají nebo mohou získat přístup k dětem, které mohou být vedeny jako pohřešované.

(64) Za účelem odstranění nedostatků ve sdílení informací týkajících se terorismu, zejména o zahraničních teroristických bojovnících, jejichž sledování pohybu je zásadní, se členské státy vyzývají, aby sdílely s Europolem informace o aktivitách souvisejících s terorismem. Toto sdílení informací by mělo probíhat prostřednictvím výměny doplňujících informací o příslušných záznamech s Europolem. Europol by měl za tímto účelem zřídit propojení s komunikační infrastrukturou.

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

(66) Nařízení Evropského parlamentu a Rady (EU) 2016/1624[1] stanoví pro účely uvedeného nařízení, že hostitelský členský stát zmocní příslušníky jednotek ve smyslu čl. 2 bodu 8 uvedeného nařízení a vyslané Evropskou agenturou pro pohraniční a pobřežní stráž k tomu, aby mohli nahlížet do unijních databází, je-li to nezbytné pro plnění operačních cílů uvedených v operačním plánu pro hraniční kontrolu, ostrahu hranic a navracení. Další relevantní agentury Unie, zejména Evropský podpůrný úřad pro otázky azylu a Europol, mohou také v rámci podpůrných týmů pro řízení migrace vysílat odborníky, kteří nejsou pracovníky těchto agentur Unie. Cílem vyslání jednotek a týmů ve smyslu čl. 2 bodů 8 a 9 uvedeného nařízení je poskytnout technickou a operativní posilu žádajícím členským státům, zejména těm, které čelí nepřiměřeným migračním výzvám. Plnění úkolů přidělených jednotkám a týmům ve smyslu čl. 2 bodů 8 a 9 uvedeného nařízení vyžaduje přístup do SIS prostřednictvím technického rozhraní Evropské agentury pro pohraniční a pobřežní stráž napojeného na centrální SIS. V případech, kdy vyhledávání v SIS provedená jednotkou nebo týmem ve smyslu čl. 2 bodů 8 a 9 nařízení (EU) 2016/1624 nebo týmy pracovníků odhalí existenci záznamu vloženého členským státem, nemůže příslušník jednotky nebo týmu ani pracovník přijmout požadované opatření, pokud to nepovolí hostitelský členský stát. Měl by být proto informován hostitelský členský stát, aby mohl podniknout další kroky. Hostitelský členský stát by měl o pozitivním nálezu uvědomit vkládající členský stát prostřednictvím výměny doplňujících informací.

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

(67) Z důvodu jejich technické podstaty, podrobného charakteru a potřeby časté aktualizace nelze některé aspekty SIS upravit tímto nařízením vyčerpávajícím způsobem. Mezi tyto aspekty patří například technická pravidla pro vkládání údajů, aktualizace, výmaz a vyhledávání údajů, pravidla pro kvalitu údajů, pravidla týkající se biometrických údajů, pravidla týkající se slučitelnosti a pořadí podle priority záznamů, pravidla pro propojení mezi záznamy a pravidla pro výměnu doplňujících informací. Prováděcí pravomoci, pokud jde o tyto aspekty, by proto měly být svěřeny Komisi. Technická pravidla pro vyhledávání v záznamech by měla zohlednit hladké fungování vnitrostátních aplikací.

(68) 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 Evropského parlamentu a Rady (EU) č. 182/2011[1]. Postup pro přijímání prováděcích aktů podle tohoto nařízení a nařízení (EU) 2018/...[+] by měl být totožný.

(69) Za účelem zajištění transparentnosti by měla agentura eu-LISA dva roky po zahájení provozu SIS podle tohoto nařízení vypracovat zprávu o technickém fungování centrálního SIS a komunikační infrastruktuře, včetně jejího zabezpečení, a o dvoustranné a vícestranné výměně doplňujících informací. Každé čtyři roky by měla Komise vydat celkové vyhodnocení.

---

[1] 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).

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 35/18.

(70) Za účelem zajištění hladkého fungování SIS by na Komisi měla být přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování EU, pokud jde o nové podkategorie věcí hledaných na základě záznamů o věcech hledaných za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení a určení okolností, za nichž lze fotografie a zobrazení obličeje používat k identifikaci osob jinak než v rámci řádných hraničních přechodů. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů[1]. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup na zasedání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

(71) Jelikož cílů tohoto nařízení, totiž vytvoření a právní úpravy unijního informačního systému a výměny souvisejících doplňujících informací, nemůže být dosaženo uspokojivě členskými státy, ale spíše jich může být vzhledem k jejich podstatě lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity, stanovenou v článku 5 Smlouvy o Evropské unii (dále jen „Smlouvy o EU“). V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení těchto cílů.

[1] Úř. věst. L 123, 12.5.2016, s. 1.

(72) Toto nařízení dodržuje základní práva a ctí zásady uznané zejména v Listině základních práv Evropské unie. Toto nařízení především v plném rozsahu dodržuje právo na ochranu osobních údajů v souladu s článkem 8 Listiny základních práv Evropské unie a jeho cílem by mělo být zajistit bezpečné prostředí pro všechny osoby žijící na území Unie a zvláštní ochranu pro děti, které by se mohly stát obětí obchodování s lidmi nebo únosu. V případech týkajících se dětí by měl být především zohledněn nejlepší zájem dítěte.

(73) V souladu s články 1 a 2 Protokolu č. 22 o postavení Dánska, připojeného ke Smlouvě o EU a ke Smlouvě o fungování EU, 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.

(74) Spojené království se účastní tohoto nařízení v souladu s čl. 5 odst. 1 Protokolu č. 19 o schengenském *acquis* začleněném do rámce Evropské unie, připojeného ke Smlouvě o EU a ke Smlouvě o fungování EU, a v souladu s čl. 8 odst. 2 rozhodnutí Rady 2000/365/ES[1].

[1] 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* (Úř. věst. L 131, 1.6.2000, s. 43).

(75) Irsko se účastní tohoto nařízení v souladu s čl. 5 odst. 1 Protokolu č. 19, připojeného ke Smlouvě o EU a ke Smlouvě o fungování EU, a v souladu s čl. 6 odst. 2 rozhodnutí Rady 2002/192/ES[1].

(76) 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*[2], která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí Rady 1999/437/ES[3].

---

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

2 Úř. věst. L 176, 10.7.1999, s. 36.

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

(77) Pokud jde o Švýcarsko, rozvíjí toto nařízení ta ustanovení schengenského *acquis* ve smyslu Dohody mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis*[1], která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí 1999/437/ES ve spojení s článkem 3 rozhodnutí Rady 2008/149/SVV[2].

[1] Úř. věst. L 53, 27.2.2008, s. 52.

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

(78) 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*[1], která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí 1999/437/ES ve spojení s článkem 3 rozhodnutí Rady 2011/349/EU[2].

[1] Úř. věst. L 160, 18.6.2011, s. 21.

[2] 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).

(79) 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 ve spojení s rozhodnutími Rady 2010/365/EU[1] a (EU) 2018/934[2].

(80) Pokud jde o Chorvatsko, představuje toto nařízení akt navazující na schengenské *acquis* nebo s ním jinak související ve smyslu čl. 4 odst. 2 aktu o přistoupení z roku 2011 a je třeba jej vykládat ve spojení s rozhodnutím Rady 2017/733.[3]

(81) Pokud jde o Kypr, 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.

(82) 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.

---

1 Rozhodnutí Rady 2010/365/EU 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).

2 Rozhodnutí Rady (EU) 2018/934 ze dne 25. června 2018 o uvedení v účinnost některých ustanovení schengenského *acquis* týkajících se Schengenského informačního systému v Bulharské republice a Rumunsku (Úř. věst. L 165, 2.7.2018, s. 37).

3 Rozhodnutí Rady (EU) 2017/733 ze dne 25. dubna 2017 o uplatňování ustanovení schengenského *acquis* týkajících se Schengenského informačního systému v Chorvatské republice (Úř. věst. L 108, 26.4.2017, s. 31).

(83) Tímto nařízením se do SIS zavádí řada zlepšení, která zvýší jeho účinnost, posílí ochranu údajů a rozšíří práva přístupu do SIS. Některá z těchto zlepšení nevyžadují složité technické změny, zatímco u jiných je zapotřebí provést technické změny různého rozsahu. S cílem zpřístupnit zlepšení systému co nejrychleji koncovým uživatelům se tímto nařízením zavádějí v několika fázích změny v rozhodnutí 2007/533/SVV. Některá zlepšení systému by měla být použitelná okamžitě po vstupu tohoto nařízení v platnost, zatímco jiná budou použitelná za jeden nebo dva roky od jeho vstupu v platnost. Toto nařízení by mělo být použitelné v plném rozsahu do tří let od svého vstupu v platnost. Postupné provádění tohoto nařízení by mělo být pečlivě sledováno, aby se zamezilo prodlevám v jeho uplatňování.

(84) Nařízení Evropského parlamentu a Rady (ES) č. 1986/2006[1], rozhodnutí 2007/533/SVV a rozhodnutí Komise 2010/261/EU[2] by měly být zrušeny s účinkem ode dne plné použitelnosti tohoto nařízení.

(85) V souladu s čl. 28 odst. 2 nařízení Evropského parlamentu a Rady (ES) č. 45/2001[3] byl konzultován evropský inspektor ochrany údajů, který dne 3. května 2017 vydal stanovisko,

PŘIJALY TOTO NAŘÍZENÍ:

---

1 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).

2 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).

3 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).

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 zajistit uplatňování ustanovení části třetí hlavy V kapitoly 4 a kapitoly 5 Smlouvy o fungování EU, pokud jde o pohyb osob na jejich územích, s využitím informací předávaných prostřednictvím tohoto systému.

Článek 2

Předmět

1. Toto nařízení stanoví 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. Tímto nařízením se rovněž zavádí ustanovení o technické architektuře SIS, o povinnostech členských států a Agentury Evropské unie pro provozní řízení rozsáhlých informačních systémů v rámci prostoru svobody, bezpečnosti a práva (dále jen „agentura eu-LISA“), o obecném zpracování údajů, o právech dotčených osob a o příslušné odpovědnosti.

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

1) „záznamem“ soubor údajů vložených do SIS umožňující příslušným orgánům identifikovat osobu nebo věc za účelem přijetí konkrétního opatření;

2) „doplňujícími informacemi“ informace, které nejsou součástí údajů v záznamech uložených v SIS, ale souvisejí se záznamy v SIS, a které se vyměňují prostřednictvím center SIRENE:

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

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

   c) pokud nelze požadované opatření přijmout;

   d) pokud se jedná o kvalitu údajů SIS;

   e) pokud se jedná o slučitelnost a prioritu záznamů;

   f) pokud se jedná o práva přístupu;

3) „dalšími údaji“ údaje uložené v SIS a související se záznamy v SIS, které jsou okamžitě k dispozici příslušným orgánům, pokud je osoba, jejíž údaje jsou vloženy do SIS, nalezena na základě vyhledávání v SIS;

4) „osobními údaji“ osobní údaje ve smyslu čl. 4 bodu 1 nařízení (EU) 2016/679;

5) „zpracováním osobních údajů“ jakákoli operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, zaprotokolování, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

6) „shodou“ skutečnost, že nastaly tyto okolnosti:

   a) koncový uživatel provedl vyhledávání v SIS;

   b) při tomto vyhledávání se zjistilo, že jiný členský stát vložil do SIS záznam;

   c) údaje v záznamu v SIS se shodují s údaji použitými pro vyhledávání;

7) „pozitivním nálezem“ jakákoli shoda, která splňuje tato kritéria:

   a) byla potvrzena:

      i) koncovým uživatelem nebo

      ii) příslušným orgánem v souladu s vnitrostátními postupy, pokud daná shoda byla založena na srovnání biometrických údajů;

      a

   b) jsou požadována další opatření;

8) „označením záznamu“ pozastavení platnosti záznamu na vnitrostátní úrovni, které lze připojit k záznamům za účelem zatčení, záznamům o pohřešovaných a zranitelných osobách a záznamům pro účely skrytých, dotazovacích nebo zvláštních kontrol;

9) „vkládajícím členským státem“ členský stát, který vložil záznam do SIS;

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

11) „koncovým uživatelem“ pověření pracovníci příslušného orgánu přímo vyhledávající v CS-SIS, N.SIS nebo v jejich technické kopii;

12) „biometrickými údaji“ osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků fyzické osoby, které umožňují nebo potvrzují její jedinečnou identifikaci, jako jsou fotografie, zobrazení obličeje, daktyloskopické údaje a profil DNA;

13) „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 identifikace osoby;

14) „zobrazením obličeje“ digitální zobrazení obličeje v dostatečném obrazovém rozlišení a kvalitě určené k použití při automatizovaném porovnávání biometrických prvků;

15) „profilem DNA“ písmenný nebo číselný kód, který představuje soubor identifikačních znaků nekódující části analyzovaného vzorku lidské DNA, totiž konkrétní molekulární struktury na různých místech DNA (loci);

16) „teroristickými trestnými činy“ trestné činy podle vnitrostátního práva uvedené v článcích 3 až 14 směrnice Evropského parlamentu a Rady (EU) 2017/541[1] nebo trestné činy rovnocenné jednomu z těchto trestných činů v případě členských států, které uvedenou směrnicí nejsou vázány;

17) „hrozbou pro veřejné zdraví“ hrozba pro veřejné zdraví ve smyslu čl. 2 bodu 21 v nařízení Evropského parlamentu a Rady (EU) 2016/399[2].

Článek 4

Technická architektura a provozování SIS

1. SIS sestává z:

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

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

ii) 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, včetně alespoň jednoho vnitrostátního nebo sdíleného záložního N.SIS; a

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

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

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

N.SIS uvedený v písmenu b) může obsahovat soubor údajů (dále jen „vnitrostátní kopie“) obsahující úplnou nebo částečnou kopii databáze SIS. Dva nebo více členských států může v jednom ze svých N.SIS zřídit sdílenou kopii, která může být těmito členskými státy využívána společně. Tato sdílená kopie se považuje za vnitrostátní kopii každého ze zúčastněných členských států

Sdílený záložní N.SIS uvedený v písmenu b) může být společně využíván dvěma nebo více členskými státy. V takovém případě je považován za záložní N.SIS každého ze zúčastněných členských států. N.SIS a jeho záloha mohou být používány současně, aby byla zajištěna nepřetržitá dostupnost systému pro koncové uživatele

Členské státy, které hodlají zřídit sdílenou kopii nebo sdílený záložní N.SIS, které budou využívány společně, se písemně dohodnou na svých povinnostech. Členské státy o této dohodě uvědomí Komisi.

Komunikační infrastruktura podporuje nepřetržitou dostupnost SIS a přispívá k jejímu zajištění. Zahrnuje redundantní a oddělené cesty pro propojení mezi CS-SIS a záložním CS-SIS a rovněž redundantní a oddělené cesty pro propojení mezi jednotlivými národními přístupovými body do SIS a CS-SIS a záložním CS-SIS.

2. Členské státy vkládají, aktualizují, mažou a vyhledávají údaje SIS prostřednictvím svých vlastních N.SIS. Členské státy, které používají částečnou nebo úplnou vnitrostátní kopii nebo částečnou či úplnou sdílenou kopii, je zpřístupní pro účely provádění automatizovaného vyhledávání na území těchto členských států. Částečná vnitrostátní nebo sdílená kopie obsahuje alespoň údaje uvedené v čl. 20 odst. 3 písm. a) až v). Vyhledávání v souborech údajů N.SIS jiných členských států není možné, s výjimkou sdílených kopií.

3. CS-SIS vykonává funkce technického dohledu a správy, přičemž je jištěn záložním CS-SIS, který je schopen zajistit všechny funkce hlavního CS-SIS v případě jeho selhání. CS-SIS a záložní CS-SIS jsou umístěny ve dvou technických místech agentury eu- LISA.

4. Agentura eu- LISA provádí technická řešení k posílení nepřetržité dostupnosti SIS, buď prostřednictvím současného provozu CS-SIS a záložního CS-SIS, pokud je záložní CS-SIS i nadále schopen zajistit provoz SIS v případě selhání CS-SIS, nebo prostřednictvím zdvojení systému nebo jeho složek. Bez ohledu na procesní požadavky stanovené v článku 10 nařízení (EU) 2018/...[+] vypracuje agentura eu-LISA do ... [jeden rok ode dne vstupu tohoto nařízení v platnost] studii o možnostech technických řešení uvádějící nezávislé posouzení dopadů a analýzu nákladů a přínosů.

5. Pokud je to za výjimečných okolností nezbytné, může agentura eu-LISA dočasně vytvořit další kopii databáze SIS.

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 29/18.

6. Technická podpůrná funkce CS-SIS poskytuje služby nezbytné pro vložení a zpracování údajů SIS, včetně vyhledávání v databázi SIS. Členským státům, jež používají vnitrostátní nebo sdílenou kopii, CS-SIS poskytuje:

   a) on-line aktualizaci vnitrostátních kopií;

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

   c) počáteční nastavení a opětovné zavedení vnitrostátních kopií;

7. CS-SIS poskytuje nepřetržitou dostupnost.

Článek 5

Náklady

1. Náklady na provoz, údržbu a další rozvoj centrálního SIS a komunikační infrastruktury se hradí ze souhrnného rozpočtu Unie. Tyto náklady zahrnují práci vykonávanou v souvislosti s CS-SIS za účelem zajišťování poskytování služeb uvedených v čl. 4 odst. 6.

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

KAPITOLA II
POVINNOSTI ČLENSKÝCH STÁTŮ

Článek 6

Vnitrostátní systémy

Každý členský stát je odpovědný za zřízení, provoz, údržbu a dále rozvoj svého N.SIS a jeho připojení k NI-SIS.

Každý členský stát je odpovědný za zajištění nepřetržité dostupnosti údajů SIS pro koncové uživatele.

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

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 zajištění dodržování tohoto nařízení. Je odpovědný za zajištění toho, že veškeré funkce SIS jsou odpovídajícím způsobem zpřístupněny koncovým uživatelům.

2. Každý členský stát určí národní orgán, který je plně funkční 24 hodin denně sedm dní v týdnu a který zajistí výměnu a dostupnost veškerých doplňujících informací (dále jen „centrála SIRENE“), v souladu s příručkou SIRENE. Každá centrála SIRENE slouží jako jediné kontaktní místo v každém členském státě pro výměnu doplňujících informací týkajících se záznamů a usnadnění přijímání požadovaných opatření tehdy, jestliže byly do SIS vloženy záznamy o osobách nebo věcech a tyto osoby nebo věci jsou nalezeny na základě pozitivního nálezu.

Každá centrála SIRENE musí mít v souladu s vnitrostátním právem snadný přímý nebo nepřímý přístup ke všem příslušným vnitrostátním informacím, včetně vnitrostátních databází a všech informací o záznamech daného členského státu, jakož i k odborné podpoře, aby mohla rychle a ve lhůtách stanovených v článku 8 reagovat na žádosti o doplňující informace.

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

3. Každý členský stát sdělí agentuře eu-LISA údaje o svém úřadu N.SIS a o své centrále SIRENE. Agentura eu-LISA zveřejní seznam úřadů N.SIS a centrál SIRENE spolu se seznamem uvedeným v čl. 56 odst. 7.

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 lidské zdroje pro zajištění nepřetržité dostupnosti a včasné a účinné výměny doplňujících informací. V případě, že komunikační infrastruktura není dostupná, členské státy k výměně doplňujících informací použijí jiné náležitě zabezpečené technické prostředky. Seznam náležitě zabezpečených technických prostředků je stanoven v příručce SIRENE.

2. Doplňující informace se použijí pouze pro účely, pro které byly předány v souladu s článkem 64, ledaže by byl získán předchozí souhlas vkládajícího členského státu pro jiný způsob užití.

3. Centrály SIRENE plní své úkoly rychle a efektivně, zejména co nejrychleji odpovídají na žádost o doplňující informace, nejpozději však do 12 hodin od jejího obdržení. V případech záznamů týkajících se teroristických trestných činů, záznamů o osobách hledaných za účelem zatčení a předání nebo vydání a záznamů o dětech podle čl. 32 odst. 1 písm. c) jednají centrály SIRENE okamžitě.

   Žádosti o doplňující informace s nejvyšší prioritou se ve formulářích SIRENE označí výrazem „URGENT“ a uvede se důvod naléhavosti.

4. Komise přijme prováděcí akty, jimiž stanoví podrobná pravidla pro úkoly centrál SIRENE podle tohoto nařízení a pro výměnu doplňujících informací ve formě příručky nazvané „příručka SIRENE“. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

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 centrálním SIS.

2. Používá-li členský stát vnitrostátní kopii, zajistí prostřednictvím služeb, které poskytuje CS-SIS, a prostřednictvím automatizované aktualizace uvedené v čl. 4 odst. 6, aby údaje uložené ve vnitrostátní kopii byly totožné a shodné s databází SIS a aby vyhledávání v jeho vnitrostátní kopii poskytovalo rovnocenný výsledek jako vyhledávání v databázi SIS.

3. Koncoví uživatelé budou dostávat údaje nezbytné pro plnění jejich úkolů, zejména, a je-li to potřebné, veškeré dostupné údaje umožňující identifikovat subjekt údajů a přijmout požadované opatření.

4. Členské státy a agentura eu-LISA provádějí pravidelné zkoušky k ověření technického souladu vnitrostátních kopií podle odstavce 2. Výsledky těchto zkoušek se zohlední jako součást mechanismu stanoveného nařízením Rady (EU) č. 1053/2013[1].

5. Komise přijme prováděcí akty, jimiž stanoví a dále rozvíjí společné standardy, protokoly a technické postupy uvedené v odstavci 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

Článek 10

Zabezpečení– 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) fyzicky chránil údaje mimo jiné vypracováním plánů pro mimořádné situace k ochraně kritické infrastruktury;

   b) zabránil neoprávněným osobám v přístupu k zařízením na zpracování údajů využívaným pro zpracování osobních údajů („kontrola přístupu k zařízení“);

[1] 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).

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

d) zabránil neoprávněnému vkládání údajů a neoprávněnému prohlížení, pozměňování či mazání uložených osobních údajů („kontrola uložení“);

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

f) zabránil neoprávněnému zpracování údajů v SIS a jakémukoli neoprávněnému pozměňování nebo mazání údajů zpracovávaných v SIS („kontrola vstupu údajů“);

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

h) zajistil, aby všechny orgány s právem přístupu do SIS nebo k zařízením pro zpracování údajů vytvořily profily popisující funkce a povinnosti osob, jež jsou oprávněny k údajům přistupovat a údaje vkládat, aktualizovat, vymazávat a vyhledávat, a aby tyto profily neprodleně na základě žádosti zpřístupnily dozorovým úřadům uvedeným v čl. 69 odst. 1 („profily pracovníků“);

i) zajistil, aby bylo možné ověřit a zjistit, kterým subjektům se mohou osobní údaje předávat za použití zařízení pro přenos údajů („kontrola přenosu“);

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

k) zabránil neoprávněnému čtení, kopírování, pozměňování nebo mazání osobních údajů při jejich předávání nebo při přepravě nosičů údajů, zejména prostřednictvím vhodných technik šifrování („kontrola přepravy“);

l) sledoval účinnost bezpečnostních opatření uvedených v tomto odstavci a přijal nezbytná organizační opatření související s interní kontrolou pro zajištění souladu s tímto nařízením („interní kontrola“);

m) zajistil, aby v případě přerušení provozu bylo možné obnovit běžný provoz nainstalovaných systémů („obnova“); a

n) zajistil, aby SIS prováděl své funkce správně, aby závady byly hlášeny („spolehlivost“) a aby osobní údaje uložené v SIS nebylo možné poškodit nesprávných fungováním systému („neporušenost“).

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 center SIRENE.

3. Členské státy přijmou opatření rovnocenná opatřením uvedeným v odstavci 1 tohoto článku, pokud jde o zabezpečení v souvislosti se zpracováním údajů SIS orgány uvedenými v článku 44.

4. Opatření uvedená v odstavcích 1, 2 a 3 mohou být součástí obecného bezpečnostního přístupu a plánu na vnitrostátní úrovni zahrnujícího více informačních systémů. V takovém případě musí být v tomto plánu jasně identifikovatelné požadavky podle tohoto článku a jejich použitelnost na SIS a musí jím být zajištěny.

Článek 11

Důvěrnost – členské státy

1. Každý členský stát použije v souladu se svým vnitrostátním právem svá pravidla týkající se 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 zaměstnání, nebo poté, co dotyčné subjekty ukončí svou činnost.

2. Pokud členský stát při provádění jakéhokoliv úkolu souvisejícího se systémem SIS spolupracuje s externími dodavateli, pečlivě kontroluje činnosti dodavatele, aby bylo zajištěno dodržování všech ustanovení tohoto nařízení, zejména pokud jde o bezpečnost, důvěrnost a ochranu údajů.

3. Provozní řízení N.SIS nebo jakýchkoliv technických kopií nesmí být svěřeno soukromým společnostem nebo soukromým organizacím.

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 v souladu se zákonem, či nikoli, za účelem sledování zákonnosti zpracování údajů, pro vlastní kontrolu, pro zajištění řádného fungování N.SIS a rovněž neporušenosti údajů a jejich zabezpečení. Tento požadavek se nepoužije na automatizované postupy uvedené v čl. 4 odst. 6 písm. a), b) a c).

2. Protokoly obsahují zejména historii záznamu, datum a čas zpracování údajů, údaje použité pro provedení vyhledávání, odkaz na zpracovávané údaje a individuální a jedinečné identifikátory uživatele příslušného orgánu i osoby, které zpracovávají údaje.

3. Odchylně od odstavce 2 tohoto článku v případě, že je vyhledávání provedeno pomocí daktyloskopických údajů nebo zobrazení obličeje v souladu s článkem 43, obsahují protokoly namísto vlastních údajů druh údajů použitých pro provedení vyhledávání.

4. Protokoly lze použít pouze k účelu uvedenému v odstavci 1 a vymažou se po uplynutí tří let od jejich vytvoření. Protokoly obsahující historii záznamů se vymažou po uplynutí tří let od výmazu těchto záznamů.

5. Protokoly lze uchovat déle, než je uvedeno v odstavci 4, jsou-li potřebné pro postupy kontroly, které již byly zahájeny.

6. Příslušné vnitrostátní orgány pověřené kontrolou toho, zda je vyhledávání v souladu se zákonem, či nikoli, sledováním zákonnosti zpracování údajů, vlastní kontrolou a zajištěním řádného fungování N.SIS, neporušenosti údajů a jejich zabezpečení mají v rozsahu svých pravomocí a na svou žádost k těmto protokolům přístup, aby mohly plnit své úkoly.

7. Provádí-li členské státy v souladu s vnitrostátním právem automatizované vyhledávání registračních značek motorových vozidel na základě kamerových záznamů, s použitím systémů automatického rozpoznávání registračních značek, musí uchovat protokol o tomto vyhledávání v souladu s vnitrostátním právem. V případě potřeby lze provést úplné vyhledávání v SIS za účelem ověření, zda byl učiněn pozitivní nález. Na všechna úplná vyhledávání se použijí odstavce 1 až 6.

8. Komise přijme prováděcí akty, kterými stanoví obsah protokolu uvedeného v odstavci 7 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

Článek 13

Vlastní kontrola

Členské státy zajistí, aby každý orgán s oprávněním k přístupu k údajům SIS přijal opatření nezbytná k zajištění dodržování tohoto nařízení a spolupracoval, je-li to nutné, s dozorovým úřadem.

Článek 14

Odborná příprava pracovníků

1. Pracovníci orgánů s právem přístupu do SIS předtím, než obdrží povolení zpracovávat údaje uložené v SIS, a pravidelně poté, co jim byl přístup do SIS poskytnut, absolvují odpovídající odbornou přípravu týkající se zabezpečení údajů, základních práv včetně ochrany údajů, pravidel a postupů pro zpracování údajů uvedených v příručce SIRENE. Pracovníci jsou informováni o relevantních ustanoveních týkajících se trestných činů a sankcích, včetně těch, které jsou stanoveny podle článku 73.

2. Členské státy zavedou vnitrostátní vzdělávací program pro systém SIS, jehož součástí budou školení pro koncové uživatele i pro pracovníky centrál SIRENE.

   Tento vzdělávací program může být součástí obecného programu odborné přípravy na vnitrostátní úrovni zahrnujícího odbornou přípravu v dalších relevantních oblastech.

3. Alespoň jednou ročně se pořádají společné kurzy odborné přípravy na úrovni Unie s cílem posílit spolupráci mezi centrálami SIRENE.

KAPITOLA III
POVINNOSTI AGENTURY eu-LISA

Článek 15

Provozní řízení

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

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

   a) dohled;

   b) zabezpečení;

   c) koordinaci vztahů mezi členskými státy a poskytovatelem;

   d) úkoly související s plněním rozpočtu;

   e) pořizování a obnovu; a

   f) smluvní záležitosti.

3. Agentura eu-LISA odpovídá také za následující úkoly spojené s centrálami SIRENE a komunikací mezi centrálami SIRENE:

a) koordinaci, řízení a podporu činností v rámci testování;

b) údržbu a aktualizaci technických specifikací pro výměnu doplňujících informací mezi centrálami SIRENE a pro komunikační infrastrukturu; a

c) řízení vlivu technických změn, pokud mají dopad na SIS i na výměnu doplňujících informací mezi centrálami SIRENE.

4. Agentura eu-LISA vytvoří a spravuje mechanismus a postupy pro provádění kontrol kvality údajů v CS-SIS. V tomto ohledu pravidelně předkládá zprávy členským státům.

Agentura eu-LISA pravidelně předkládá Komisi zprávu o zjištěných problémech a o tom, kterých členských států se týkají.

Komise předkládá Evropskému parlamentu a Radě pravidelnou zprávu o problémech, které se vyskytly ohledně kvality údajů.

5. Agentura eu-LISA rovněž provádí úkoly související s poskytováním odborné přípravy o technickém používání SIS a o opatřeních ke zlepšení kvality údajů v SIS.

6. Provozní řízení centrálního SIS sestává ze všech úkolů nezbytných pro zachování nepřetržité funkčnosti centrálního SIS 24 hodin denně sedm dní v týdnu v souladu s tímto nařízením, zejména z údržby a technického rozvoje nezbytných pro plynulý chod systému. Mezi tyto úkoly patří také koordinace, řízení a podpora činností testování centrálního SIS a N.SIS, které zajišťují, aby centrální SIS a N.SIS fungovaly podle požadavků na technický a funkční soulad stanovených v článku 9.

7. Komise přijme prováděcí akty za účelem stanovení technických požadavků na komunikační infrastruktury. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

Článek 16

Zabezpečení – agentura eu-LISA

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

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

   b) zabránil neoprávněným osobám v přístupu k zařízením na zpracování údajů využívaným pro zpracování osobních údajů („kontrola přístupu k zařízení“);

c) zabránil neoprávněnému čtení, kopírování, pozměňování či odstraňování nosičů údajů („kontrola nosičů údajů“);

d) zabránil neoprávněnému vkládání údajů a neoprávněnému prohlížení, pozměňování či mazání uložených osobních údajů („kontrola uložení“);

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

f) zabránil neoprávněnému zpracování údajů v systému SIS a jakémukoli neoprávněnému pozměňování nebo mazání údajů zpracovávaných v systému SIS („kontrola vstupu údajů“);

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

h) vytvořil profily popisující funkce a povinnosti osob, jež jsou oprávněny k údajům nebo k zařízením pro zpracování údajů přistupovat, a tyto profily na žádost neprodleně zpřístupnil evropskému inspektorovi ochrany údajů („profily pracovníků“);

i) zajistil, aby bylo možné ověřit a zjistit, kterým subjektům se mohou osobní údaje předávat za použití zařízení pro přenos údajů („kontrola přenosu“);

j) zajistil, aby bylo možné zpětně ověřit a zjistit, které osobní údaje byly vloženy do automatizovaných systémů pro zpracování údajů, a kdy a kdo je vložil („kontrola vkládání“);

k) zabránil neoprávněnému čtení, kopírování, pozměňování nebo mazání osobních údajů při jejich předávání nebo při přepravě nosičů údajů, zejména prostřednictvím vhodných technik šifrování („kontrola přepravy“);

l) sledoval účinnost bezpečnostních opatření uvedených v tomto odstavci a přijal nezbytná organizační opatření související s interní kontrolou pro zajištění souladu s tímto nařízením („interní kontrola“);

m) zajistil, aby v případě přerušení provozu bylo možné obnovit běžný provoz nainstalovaných systémů („obnova“);

n) zajistil, aby SIS prováděl své funkce správně, aby závady byly hlášeny („spolehlivost“) a aby osobní údaje uložené v SIS nebylo možné poškodit nesprávným fungováním systému („neporušenost“); a

o) zajistil bezpečnost svých technických míst.

2. Agentura eu-LISA 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 eu-LISA

1. Aniž je dotčen článek 17 služebního řádu, použije agentura eu-LISA příslušná pravidla týkající se služebního tajemství nebo jiné srovnatelné povinnosti zachování důvěrnosti na všechny své pracovníky, kteří musí pracovat s údaji SIS, která jsou srovnatelná s pravidly stanovenými v článku 11 tohoto nařízení. Tato povinnost trvá i poté, co dotyčné osoby opustí svůj úřad nebo zaměstnání, nebo poté, co ukončí svou činnost.

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

3. Pokud agentura eu-LISA při provádění jakéhokoliv úkolu souvisejícího se systémem SIS spolupracuje s externími dodavateli, pečlivě kontroluje činnosti dodavatele, aby bylo zajištěno dodržování všech ustanovení tohoto nařízení, zejména pokud jde o bezpečnost, důvěrnost a ochranu údajů.

4. Provozní řízení CS-SIS nesmí být svěřeno soukromým společnostem nebo soukromým organizacím.

Článek 18

Vedení protokolů na centrální úrovni

1. Agentura eu-LISA 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 záznamu, datum a čas zpracování údajů, údaje použité pro provedení vyhledávání, odkaz na zpracovávané údaje a individuální a jedinečné identifikátory uživatele příslušného orgánu, který zpracovává údaje.

3. Odchylně od odstavce 2 tohoto článku v případě, že je vyhledávání provedeno pomocí daktyloskopických údajů nebo zobrazení obličeje v souladu s článkem 43, obsahují protokoly namísto vlastních údajů druh údajů použitých pro provedení vyhledávání.

4. Protokoly lze použít pouze k účelům uvedeným v odstavci 1 a vymažou se po uplynutí tří let od jejich vytvoření. Protokoly obsahující historii záznamů se vymažou po uplynutí tří let od výmazu záznamů.

5. Protokoly lze uchovat déle, než je uvedeno v odstavci 4, jsou-li potřebné pro postupy kontroly, které již započaly.

6. Agentura eu-LISA má v rozsahu svých pravomocí k těmto protokolům přístup za účelem vlastní kontroly a zajištění řádného fungování CS-SIS, neporušenosti údajů a jejich zabezpečení.

   Evropský inspektor ochrany údajů má v rozsahu svých pravomocí a na základě žádosti k těmto protokolům přístup, aby mohl plnit své úkoly.

KAPITOLA IV
INFORMOVÁNÍ VEŘEJNOSTI

Článek 19

Informační kampaně o SIS

Od okamžiku, použitelnosti tohoto nařízení uskuteční Komise ve spolupráci s dozorovými úřady a s evropským inspektorem ochrany údajů kampaň, jíž informuje veřejnost o účelech SIS, o údajích, které se v něm ukládají, o orgánech, které k němu mají přístup, a o právech subjektů údajů. Komise tyto kampaně pravidelně opakuje ve spolupráci s dozorovými úřady a evropským inspektorem ochrany údajů. Komise provozuje internetové stránky, které zpřístupňují veřejnosti všechny příslušné informace týkající se SIS. Členské státy, ve spolupráci se svými dozorovými úřady, navrhnou a provedou nezbytné politiky s cílem obecně informovat své občany a rezidenty o SIS.

KAPITOLA IV
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 poskytuje každý členský stát a které jsou potřebné pro účely uvedené v článcích 26, 32, 34, 36, 38 a 40.

2. Kategorie údajů jsou následující:

   a) informace o osobách, o kterých byl vložen záznam;

   b) informace o věcech uvedené v článcích 26, 32, 34, 36 a 38.

3. Jakýkoli záznam v SIS, který zahrnuje informace o osobách, musí obsahovat pouze tyto údaje:

   a) příjmení;

   b) jméno(a);

   c) rodné(á) příjmení;

d) dříve užívané(á) jméno(a) a alias;

e) jakékoli zvláštní objektivní a nezměnitelné tělesné znaky;

f) místo narození;

g) datum narození;

h) pohlaví;

i) veškeré státní příslušnosti dotčené osoby;

j) údaj o tom, zda dotčená osoba:

   i) je ozbrojena;

   ii) má sklon k násilí;

   iii) uprchla nebo hrozí její útěk;

   iv) existuje riziko, že spáchá sebevraždu;

   v) představuje hrozbu pro veřejné zdraví; nebo

   vi) je zapojena do činností uvedených v článcích 3 až 14 směrnice (EU) 2017/541;

k) důvod záznamu;

l) orgán, který vytvořil záznam;

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

n) opatření, jež má být přijato v případě pozitivního nálezu;

o) propojení podle článku 63 na další záznamy;

p) druh deliktu;

q) osobní identifikační číslo ve vnitrostátním rejstříku;

r) kategorizace typu případu v případě záznamů podle čl. 32 odst. 1;

s) druh dokladů totožnosti;

t) země vydání dokladů totožnosti;

u) číslo nebo čísla dokladů totožnosti;

v) datum vydání dokladů totožnosti;

w) fotografie a zobrazení obličeje;

x) příslušné profily DNA podle čl. 42 odst. 3;

y) daktyloskopické údaje;

z) kopie, pokud možno barevná, dokladu či dokladů totožnosti.

4. Komise přijme prováděcí akty, jimiž stanoví a dále rozvíjí technická pravidla nezbytná pro vkládání, aktualizaci, výmaz a vyhledávání údajů uvedených v odstavci 2 a 3 tohoto článku, jakož i společné normy uvedené v odstavci 5 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

5. Tato technická pravidla musí být podobná pro vyhledávání v CS-SIS, ve vnitrostátních nebo sdílených kopiích a v technických kopiích, jak je uvedeno v čl. 56 odst. 2, Musí se zakládat na společných standardech.

Článek 21

Proporcionalita

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

2. Pokud je osoba nebo věc hledána na základě záznamu, který souvisí s teroristickým trestným činem, je tento případ považován za dostatečně přiměřený, relevantní a závažný pro to, aby odůvodňoval vložení záznamu do SIS. Z důvodů veřejné nebo národní bezpečnosti mohou ve výjimečných případech členské státy od vložení záznamu upustit, pokud je pravděpodobné, že bude bránit úředním nebo právním šetřením, vyšetřováním nebo postupům.

Článek 22

Požadavek na vložení záznamu

1. Minimální soubor údajů nezbytných pro vložení záznamu do SIS představují údaje uvedené v čl. 20 odst. 3 písm. a), g), k), a n), s výjimkou situací podle článku 40. Ostatní údaje uvedené ve zmíněném odstavci se rovněž musí vložit do SIS, pokud jsou dostupné.

2. Údaje uvedené v čl. 20 odst. 3 písm. e) tohoto nařízení se vloží, pouze pokud je to nezbytně nutné pro účely identifikace dotčené osoby. Pokud jsou tyto údaje vloženy, zajistí členské státy, že je dodržován článek 10 směrnice (EU) 2016/680.

Článek 23

Slučitelnost záznamů

1. Před vložením záznamu členský stát ověří, zda dotčená osoba nebo věc již nejsou předmětem záznamu v SIS. Za účelem ověření, zda dotčená osoba již není předmětem záznamu, se rovněž provede ověření s použitím daktyloskopických údajů, pokud jsou tyto údaje dostupné.

2. Členský stát může o dané osobě nebo věci vložit do SIS pouze jediný záznam. Je-li to nezbytné, mohou nové záznamy o téže osobě nebo věci vkládat v souladu s odstavcem 3 jiné členské státy.

3. Pokud je určitá osoba nebo věc již předmětem záznamu v SIS, členský stát, který chce vložit nový záznam, ověří, zda dané záznamy jsou slučitelné. Jsou-li záznamy slučitelné, může členský stát vložit nový záznam. Jsou-li záznamy neslučitelné, proběhnou mezi centrálami SIRENE dotčených členských států konzultace prostřednictvím výměny doplňujících informací s cílem dosáhnout dohody. Pravidla týkající se slučitelnosti záznamů jsou stanovena v příručce SIRENE. Od pravidel slučitelnosti se po konzultaci mezi členskými státy lze odchýlit, pokud jsou ohroženy podstatné národní zájmy.

4. V případě pozitivních nálezů na základě vícenásobných záznamů o téže osobě nebo věci se vykonávající členský stát řídí pravidly pro prioritu záznamů stanovenými v příručce SIRENE.

V případě, že osoba je předmětem vícenásobných záznamů vložených různými členskými státy, se záznamy za účelem zatčení vložené podle článku 26 vykonají přednostně s výhradou článku 25.

Článek 24

Obecná ustanovení týkající se označování záznamů

1. Pokud má členský stát za to, že provedení záznamu vloženého v souladu s článkem 26, 32 nebo 36 není slučitelné s jeho vnitrostátním právem, jeho mezinárodními závazky nebo zásadními vnitrostátními zájmy, může požadovat označení záznamu v tom smyslu, že opatření, které má být přijato na základě záznamu, nebude přijato na jeho území. Označení záznamu provede centrála SIRENE vkládajícího členského státu.

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

3. Pokud v mimořádně naléhavých a závažných případech požaduje vkládající členský stát vykonání opatření, vykonávající členský stát přezkoumá, zda může povolit zrušení označení záznamu, které bylo doplněno na jeho pokyn. Může-li vykonávající členský stát toto označení záznamu zrušit, učiní nezbytné kroky k zajištění okamžitého provedení 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, požádá dotčený členský stát vkládající členský stát, aby k záznamu za účelem zatčení a předání následně doplnil označení záznamu zamezující zatčení, 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.

   Členský stát může rovněž požádat, aby bylo k záznamu doplněno označení záznamu v případě, že jeho příslušný justiční orgán subjekt záznamu během postupu zatčení a předání propustí.

2. Na základě pokynu justičního orgánu příslušného podle vnitrostátního práva, a to buď obecného, nebo pro konkrétní případ, může členský stát od vkládajícího členského státu požadovat, aby bylo k záznamu za účelem zatčení a předání doplněno označení záznamu 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 vkládání záznamů

1. Záznamy o osobách hledaných za účelem zatčení a předání na základě evropského zatýkacího rozkazu nebo záznamy o osobách hledaných za účelem zatčení a vydání se vkládají do SIS na žádost justičního orgánu vkládajícího členského státu.

2. Záznamy za účelem zatčení a předání se vkládají také na základě zatýkacích rozkazů vydaných v souladu s dohodami uzavřenými mezi Unií a třetími zeměmi na základě Smluv za účelem předání osob na základě zatýkacího rozkazu, které stanoví předávání tohoto zatýkacího rozkazu prostřednictvím SIS.

3. Má se za to, že jakýkoliv odkaz v tomto nařízení na ustanovení rámcového rozhodnutí 2002/584/SVV zahrnuje odpovídající ustanovení dohod uzavřených mezi Evropskou unií a třetími zeměmi na základě Smluv za účelem předávání osob na základě zatýkacího rozkazu, které stanoví předávání tohoto zatýkacího rozkazu prostřednictvím SIS.

4. V případě probíhající operace může vkládající členský stát dočasně znemožnit koncovým uživatelům v členských státech zapojených do operace vyhledávání existujícího záznamu za účelem zatčení vloženého podle tohoto článku. V takovém případě je záznam přístupný pouze centrálám SIRENE. Členské státy mohou znemožnit toto vyhledávání pouze tehdy, pokud:

   a) cíle operace nelze dosáhnout prostřednictvím jiných opatření;

   b) příslušný justiční orgán vkládajícího členského státu k tomu předtím udělil povolení; a

   c) všechny členské státy zapojené do operace byly informovány prostřednictvím výměny doplňujících informací.

   Funkce uvedená v prvním pododstavci může být použita pouze na dobu nepřesahující 48 hodin. Avšak pokud je to nutné z operativního hlediska, může být tato lhůta opakovaně prodloužena o dalších 48 hodin. Členské státy vedou statistiky o počtu záznamů, v souvislosti s nimiž byla tato funkce použita.

5. Pokud existují jasné indicie, že s osobou, která je předmětem záznamu podle odstavce 1 a 2 tohoto článku, jsou spojeny věci uvedené v čl. 38 odst. 2 písm. a), b), c), e), g), h), j) a k), lze vložit záznamy o těchto věcech za účelem nalezení dané osoby. V takových případech se záznam o dané osobě propojí se záznamem o věci v souladu s článkem 63.

6. Komise přijme prováděcí akty, jimiž stanoví a dále rozvíjí pravidla pro vkládání, aktualizaci, výmaz a vyhledávání údajů uvedených v odstavci 5 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

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 vkládající členský stát do SIS kopii originálu evropského zatýkacího rozkazu.

   Členský stát může vložit do záznamu za účelem zatčení a předání kopii více evropských zatýkacích rozkazů.

2. Vkládající členský stát může vložit kopii překladu evropského zatýkacího rozkazu do jednoho nebo několika dalších úředních jazyků orgánů Unie.

Článek 28

Doplňující informace o osobách hledaných za účelem zatčení a předání

Vkládající členský stát, který vložil 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. Vkládající členský stát, který vložil záznam za účelem vydání, sdělí prostřednictvím výměny doplňujících informací všem ostatním členským státům tyto údaje:

   a) orgán, který vydal žádost o zatčení;

   b) zda byl vydán 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 osoby, o níž byl záznam vložen, na něm;

   e) je-li to možné, následky trestného činu; a

   f) jakékoliv další informace, které jsou užitečné nebo nezbytné pro výkon záznamu.

2. Údaje uvedené v odstavci 1 tohoto článku se nesdělují, pokud byly již poskytnuty údaje uvedené v článku 27 nebo 28 a pokud jsou považovány za dostatečné pro výkon záznamu vykonávajícím členským státem.

Článek 30

Přeměna opatření týkajících se záznamů
za účelem zatčení a předání nebo vydání

Není-li možné zatčení provést buď z důvodu zamítavého rozhodnutí členského státu, jenž byl o provedení zatčení požádán v souladu s postupy týkajícími se označování záznamů uvedenými v článcích 24 nebo 25, nebo z toho důvodu, že v případě záznamu za účelem zatčení a vydání nebylo vyšetřování ukončeno, sdělí členský stát, jenž byl o provedení zatčení požádán, v reakci na záznam místo pobytu dotyčné osoby.

Článek 31

Výkon opatření na základě záznamu
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 spolu s dalšími údaji podle článku 27 považován za evropský zatýkací rozkaz vystavený v souladu s uvedeným rámcovým rozhodnutím a má stejný účinek.

2. V případech, na které se rámcové rozhodnutí 2002/584/SVV nevztahuje, má záznam vložený do SIS podle článků 26 a 29 stejný právní účinek 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 NEBO ZRANITELNÝCH OSOBÁCH, KTERÝM JE TŘEBA ZABRÁNIT V CESTOVÁNÍ

Článek 32

Cíle a podmínky vkládání záznamů

1. Do SIS se na žádost příslušného orgánu vkládajícího členského státu vkládají záznamy o těchto kategoriích osob:

   a) pohřešované osoby, které musí být umístěny pod ochranu:

      i) v zájmu jejich vlastní ochrany;

      ii) za účelem předcházení ohrožení veřejného pořádku nebo veřejné bezpečnosti;

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

   c) děti, kterým hrozí únos jedním z rodičů, rodinným příslušníkem nebo opatrovníkem a kterým je třeba zabránit v cestování;

d) děti, kterým je třeba zabránit v cestování, neboť jim hrozí konkrétní a zjevné riziko, že budou přemístěny z území členského státu nebo toto území opustí a

i) že se stanou oběťmi obchodování s lidmi, nuceného sňatku, mrzačení ženských pohlavních orgánů nebo jiných forem násilí na základě pohlaví,

ii) že se stanou oběťmi nebo se zapojí do teroristických trestných činů, nebo

iii) že budou odvedeny nebo začleněny do ozbrojených skupin nebo přinuceny k aktivní účasti na páchání násilností;

e) zletilé zranitelné osoby, kterým je třeba zabránit v cestování v zájmu jejich vlastní ochrany, neboť jim hrozí konkrétní a zjevné riziko, že budou přemístěny z území členského státu nebo toto území opustí a že se stanou oběťmi obchodování s lidmi nebo násilí na základě pohlaví.

2. Ustanovení odst. 1 písm. a) se použije zejména na děti a na osoby, které musí být umístěny do ústavní péče na základě rozhodnutí příslušného orgánu.

3. Záznam o dítěti podle odst. 1 písm. c) se vkládá na základě rozhodnutí příslušných orgánů, včetně justičních orgánů členských států, které jsou příslušné ve věcech rodičovské zodpovědnosti, hrozí-li konkrétní a zjevné riziko, že by dítě mohlo být protiprávně a bezprostředně přemístěno z členského státu, ve kterém se tyto příslušné orgány nacházejí.

4. Záznam o osobách podle odst. 1 písm. d) a e) se vkládá na základě rozhodnutí příslušných orgánů, včetně justičních orgánů.

5. Vkládající členský stát pravidelně přezkoumává nutnost uchovávat v souladu s čl. 53 odst. 4záznamy podle odst. 1 písm. c), d) a e) tohoto článku.

6. Vkládající členský stát zajistí:

a) aby údaje, které vložil do SIS, uváděly, do které z kategorií zmíněných v odstavci 1 osoba dotčená záznamem patří;

b) aby údaje, které vložil do SIS, uváděly, o který typ případu se jedná vždy, kdy je toto známo; a

c) aby v souvislosti se záznamy vloženými podle odst. 1 písm. c), d) a e) byly veškeré relevantní informace v okamžiku vytváření záznamu zpřístupněny v jeho centrále SIRENE.

7. Čtyři měsíce přede dnem, kdy dítě, které je subjektem záznamu podle tohoto článku, dosáhne plnoletosti v souladu s vnitrostátním právem vkládajícího členského státu, CS-SIS automaticky informuje vkládající členský stát, že důvod pro záznam a opatření, jež má být přijato, musí být aktualizovány, nebo že musí být záznam vymazán.

8. Pokud existují jasné indicie, že s osobou, která je předmětem záznamu podle odstavce 1 tohoto článku, jsou spojeny věci uvedené v čl. 38 odst. 2 písm. a), b), c), e), g), h) a k), lze vložit záznamy o těchto věcech za účelem nalezení dané osoby. V takových případech se záznam o dané osobě propojí se záznamem o věci v souladu s článkem 63.

9. Komise přijme prováděcí akty, jimiž stanoví a dále rozvíjí pravidla pro kategorizaci typů případů a vkládání údajů uvedených v odstavci 6. Typy případů týkajících se pohřešovaných dětí zahrnují mimo jiné děti, které utekly z domova, děti bez doprovodu v kontextu migrace a děti, jimž hrozí riziko rodičovského únosu.

Komise rovněž přijme prováděcí akty, jimiž stanoví a dále rozvíjí technická pravidla pro vkládání, aktualizaci, výmaz a vyhledávání údajů uvedených v odstavci 8.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

Článek 33

Výkon opatření na základě záznamu

1. Je-li nalezena osoba uvedená v článku 32, příslušné orgány vykonávajícího členského státu sdělí při splnění požadavků uvedených v odstavci 4 vkládajícímu členskému státu místo jejího pobytu.

2. V případě osob, které musí být umístěny pod ochranu podle čl. 32 odst. 1 písm. a), c), d) a e), vykonávající členský stát prostřednictvím výměny doplňujících informací okamžitě zprostředkuje konzultace mezi svými vlastními příslušnými orgány a příslušnými orgány vkládajícího členského státu, aby se tyto neprodleně dohodly na opatřeních, která mají být přijata. Příslušné orgány ve vykonávajícím členském státě mohou, v souladu s vnitrostátním právem, umístit dotyčné osoby pod ochranu a zabránit jim tak v tom, aby pokračovaly v cestě.

3. V případě dětí je jakékoliv rozhodnutí o opatřeních, která mají být přijata, nebo rozhodnutí o umístění dítěte pod ochranu podle odstavce 2 přijímáno s ohledem na nejlepší zájem dítěte. Tato rozhodnutí jsou přijímána okamžitě, avšak nejpozději 12 hodin poté, co je dítě nalezeno, v případě potřeby za konzultace s příslušnými orgány pro ochranu dětí.

4. Sdělení údajů o pohřešované osobě, jež byla nalezena a která je zletilá, 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 HLEDANÝCH ZA ÚČELEM ZAJIŠTĚNÍ JEJICH SPOLUPRÁCE V SOUDNÍM ŘÍZENÍ

Článek 34

Cíle a podmínky vkládání záznamů

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

   a) svědcích;

b) osobách předvolaných nebo hledaných za účelem předvolání justičními orgány v rámci trestního řízení, aby se zodpovídaly z činů, pro které jsou stíhány;

c) osobách, kterým má být doručen trestní rozsudek nebo jiné dokumenty v rámci trestního řízení, aby se zodpovídaly z činů, pro které jsou stíhány;

d) osobách, kterým má být doručena výzva za účelem výkonu trestu včetně trestu odnětí svobody.

2. Pokud existují jasné indicie, že s osobou, která je předmětem záznamu podle odstavce 1 tohoto článku, jsou spojeny věci uvedené v čl. 38 odst. 2 písm. a), b), c), e), g), h) a k), lze vložit záznamy o těchto věcech za účelem nalezení dané osoby. V takových případech se záznam o dané osobě propojí se záznamem o věci v souladu s článkem 63.

3. Komise přijme prováděcí akty, jimiž stanoví a dále rozvíjí technická pravidla pro vkládání, aktualizaci, výmaz a vyhledávání údajů uvedených v odstavci 2 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

Článek 35

Výkon opatření na základě záznamu

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

KAPITOLA IX
ZÁZNAMY O OSOBÁCH A VĚCECH PRO ÚČELY SKRYTÝCH, DOTAZOVACÍCH NEBO ZVLÁŠTNÍCH KONTROL

Článek 36

Cíle a podmínky vkládání záznamů

1. Záznamy o osobách o věcech uvedených v čl. 38 odst. 2 písm. a), b), c), e), g), h), j), k) a l) a o bezhotovostních platebních prostředcích se vkládají pro účely skrytých, dotazovacích nebo zvláštních kontrol v souladu s čl. 37 odst. 3, 4 a 5 podle vnitrostátního práva vkládajícího členského státu.

2. Při vkládání záznamů pro účely skrytých, dotazovacích nebo zvláštních kontrol a pokud informace požadované vkládajícím členským státem jsou nad rámec informací stanovených v čl. 37 odst. 1 písm. a) až h), doplní vkládající členský stát do záznamu veškeré informace, které jsou nad tento rámec požadovány. Pokud se tyto informace týkají zvláštních kategorií osobních údajů podle článku 10 směrnice (EU) 2016/680, lze je požadovat pouze v případě, že je to nezbytně nutné pro konkrétní účel záznamu a že se týkají trestného činu, o němž byl vložen záznam.

3. Záznam o osobách pro účely skrytých, dotazovacích nebo zvláštních kontrol může být vložen pro účely prevence, odhalování, vyšetřování nebo stíhání trestné činnosti, výkonu rozsudku v trestním řízení a předcházení ohrožení veřejné bezpečnosti v některém z těchto případů:

   a) existují jasné indicie, že osoba má v úmyslu spáchat nebo páchá některý z trestných činů uvedených v čl. 2 odst. 1 a 2 rámcového rozhodnutí 2002/584/SVV;

   b) informace uvedené v čl. 37 odst. 1 jsou nezbytné pro účely výkonu trestu odnětí svobody či ochranného opatření spojeného se zbavením osobní svobody, které byly uloženy osobě odsouzené za některý z trestných činů uvedených v čl. 2 odst. 1 a 2 rámcového rozhodnutí 2002/584/SVV;

   c) z celkového posouzení osoby, zejména na základě dosud spáchaných trestných činů, lze předpokládat, že tato osoba může i v budoucnu spáchat trestné činy uvedené v čl. 2 odst. 1 a 2 rámcového rozhodnutí 2002/584/SVV.

4. Kromě toho může být záznam o osobách pro účely skrytých, dotazovacích nebo zvláštních kontrol vložen v souladu s vnitrostátním právem na žádost orgánů odpovědných za národní bezpečnost, pokud existuje konkrétní indicie, 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 národní bezpečnosti. Členský stát, který vložil záznam podle tohoto odstavce, o tomto záznamu informuje ostatní členské státy. Každý členský stát určí, kterým orgánům se tyto informace dále předávají. Tyto informace se předávají prostřednictvím center SIRENE.

5. Pokud existují jasné indicie, že věci uvedené v čl. 38 odst. 2 písm. a), b), c), e), g), h), j), k), l) nebo bezhotovostní platební prostředky jsou spojeny se závažnými trestnými činy uvedenými v odstavci 3 tohoto článku nebo závažnými hrozbami uvedenými v odstavci 4 tohoto článku, lze o těchto věcech vložit záznamy a propojit je se záznamy vloženými podle odstavců 3 a 4 tohoto článku.

6. Komise přijme prováděcí akty, jimiž stanoví a dále rozvíjí technická pravidla nezbytná pro vkládání, aktualizaci, výmaz a vyhledávání údajů uvedených v odstavci 5 tohoto článku, jakož i dalších informací uvedených v odstavci 2 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

Článek 37

Výkon opatření na základě záznamu

1. Pro účely skrytých, dotazovacích nebo zvláštních kontrol vykonávající členský stát opatří a vkládajícímu členskému státu sdělí všechny nebo některé z těchto informací:

   a) skutečnost, že byla nalezena osoba, která je předmětem záznamu, nebo že byly nalezeny věci uvedené v čl. 38 odst. 2 písm. a), b), c), e), g), h), j), k), l) nebo bezhotovostní platební prostředky, které jsou předmětem záznamu;

   b) místo, čas a důvod kontroly;

   c) trasa a cíl cesty;

   d) osoby, které doprovázejí předmět záznamu, 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 předmětem záznamu spojeny;

   e) zjištěná totožnost a osobní popis osoby používající nevyplněný úřední doklad či vydaný doklad totožnosti, který je předmětem záznamu;

   f) použité věci uvedené v čl. 38 odst. 2 písm. a), b), c), e), g), h), j), k), l) nebo bezhotovostní platební prostředky;

g) převážené předměty, včetně cestovních dokladů;

h) okolnosti, za nichž byly daná osoba, věci uvedené v čl. 38 odst. 2 písm. a), b), c), e), g), h), j), k), l) nebo bezhotovostní platební prostředky nalezeny;

i) jakékoli další informace požadované vkládajícím členským státem v souladu s čl. 36 odst. 2.

Pokud se informace uvedené v prvním pododstavci písm. i) tohoto odstavce týkají zvláštních kategorií osobních údajů podle článku 10 směrnice (EU) 2016/680, zpracovávají se v souladu s podmínkami stanovenými v uvedeném článku a pouze v případě, že doplňují jiné osobní údaje zpracovávané pro stejný účel.

2. Informace uvedené v odstavci 1 sdělí vykonávající členský stát prostřednictvím výměny doplňujících informací.

3. Skrytá kontrola spočívá v nenápadném opatření co největšího množství informací uvedených v odstavci 1 v průběhu běžné činnosti prováděné příslušnými vnitrostátními orgány vykonávajícího členského státu. Opatření těchto informací nesmí ohrozit skrytou povahu kontrol a subjekt záznamu nesmí být na existenci záznamu žádným způsobem upozorněn.

4. Dotazovací kontrola spočívá v podání vysvětlení danou osobou, a to i na základě informací nebo konkrétních otázek doplněných do záznamu vkládajícím členským státem v souladu s čl. 36 odst. 2. Podání vysvětlení se provádí podle vnitrostátního práva vykonávajícího členského státu.

5. Během zvláštních kontrol může být pro účely uvedené v článku 36 provedena prohlídka osob, vozidel, plavidel, letadel, kontejnerů a převážených věcí. Prohlídky se vykonávají v souladu s vnitrostátním právem vykonávajícího členského státu.

6. Pokud zvláštní kontroly nejsou podle vnitrostátního práva vykonávajícího členského státu povoleny, nahrazují se v tomto členském státě dotazovacími kontrolami. Pokud dotazovací kontroly nejsou podle vnitrostátního práva vykonávajícího členského státu povoleny, nahrazují se v tomto členském státě skrytými kontrolami. V případech, na něž se vztahuje směrnice 2013/48/EU, členské státy zajistí, aby bylo za podmínek stanovených v uvedené směrnici dodrženo právo podezřelých a obviněných osob na přístup k obhájci.

7. Odstavcem 6 není dotčena povinnost členských států zpřístupnit koncovým uživatelům informace požadované podle čl. 36 odst. 2.

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

Článek 38

Cíle a podmínky vkládání záznamů

1. Členské státy do SIS vkládají záznamy o věcech hledaných za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení.

2. Vkládají se záznamy týkající se těchto kategorií snadno identifikovatelných věcí:

a) motorová vozidla bez ohledu na systém pohonu;

b) přívěsy o pohotovostní hmotnosti přesahující 750 kg;

c) obytné přívěsy;

d) stroje a zařízení;

e) plavidla;

f) lodní motory;

g) kontejnery;

h) letadla;

i) letecké motory;

j) střelné zbraně;

k) odcizené, neoprávněně užívané či ztracené nevyplněné úřední doklady nebo doklady, které vypadají jako uvedené doklady, ale jsou falešné;

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

m) odcizená, neoprávněně užívaná, pohřešovaná nebo neplatná osvědčení o registraci vozidel a registrační značky vozidel, nebo osvědčení či registrační značky, které vypadají jako uvedená osvědčení a registrační značky, ale jsou falešné;

n) bankovky (evidované bankovky) a falešné bankovky;

o) IT zařízení;

p) identifikovatelné součásti motorových vozidel;

q) identifikovatelné součásti strojů a zařízení;

r) jiné identifikovatelné cenné věci vymezené v souladu s odstavcem 3.

Pokud jde o doklady uvedené v písmenech k), l) a m), může vkládající členský stát upřesnit, zda jsou tyto doklady odcizené, neoprávněně užívané, ztracené, neplatné nebo falešné.

3. Komisi je svěřena pravomoc přijmout akt v přenesené pravomoci v souladu s článkem 75 za účelem změny tohoto nařízení, kterým vymezí nové podkategorie věcí podle odst. 2 písm. o), p), q) a r) tohoto článku.

4. Komise přijme prováděcí akty, jimiž stanoví a dále rozvíjí technická pravidla nezbytná pro vkládání, aktualizaci, výmaz a vyhledávání údajů uvedených v odstavci 2 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

Článek 39

Výkon opatření na základě záznamu

1. Pokud se při vyhledávání zjistí záznam o věci, která byla nalezena, zabaví příslušný orgán dotčenou věc v souladu s vnitrostátním právem a spojí se s orgánem vkládajícího členského státu, s cílem dohodnout se na opatřeních, který mají být přijata. 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. Vykonávající členský stát přijme požadovaná opatření v souladu s vnitrostátním právem.

KAPITOLA XI
ZÁZNAMY O NEZNÁMÝCH HLEDANÝCH OSOBÁCH ZA ÚČELEM IDENTIFIKACE PODLE VNITROSTÁTNÍHO PRÁVA

Článek 40

Záznamy o neznámých hledaných osobách za účelem identifikace podle vnitrostátního práva

Členské státy mohou do SIS vložit záznamy o neznámých hledaných osobách obsahující pouze daktyloskopické údaje. Tyto daktyloskopické údaje mohou představovat úplné či neúplné soubory otisků prstů nebo otisků dlaní zajištěných na místě vyšetřovaných teroristických trestných činů nebo jiných závažných trestných činů. Do SIS je lze vkládat pouze v případě, že je možné s velmi vysokou mírou pravděpodobnosti určit, že patří pachateli daného trestného činu.

V případě, že příslušný orgán vkládajícího členského státu nemůže identifikovat podezřelou osobu na základě údajů z jiné příslušné vnitrostátní, unijní nebo mezinárodní databáze, daktyloskopické údaje uvedené v prvním pododstavci lze vložit pouze do této kategorii záznamů pod označením „neznámá hledaná osoba“ pro účely identifikace této osoby.

Článek 41

Výkon opatření na základě záznamu

V případě pozitivního nálezu shodujícího se s údaji vloženými podle článku 40 se osoba identifikuje v souladu s vnitrostátním právem a provede se odborné ověření, zda daktyloskopické údaje uložené v SIS patří dané osobě. Vykonávající členské státy informace o totožnosti a místě pobytu dané osoby sdělí vkládajícímu členskému státu, prostřednictvím výměny doplňujících informací s cílem napomoci včasnému vyšetření případu.

KAPITOLA XII

ZVLÁŠTNÍ PRAVIDLA TÝKAJÍCÍ SE BIOMETRICKÝCH ÚDAJŮ

Článek 42

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

1. Do SIS se vloží pouze fotografie, zobrazení obličeje, daktyloskopické údaje uvedené v čl. 20 odst. 3 písm. w) a y), které splňují minimální normy kvality údajů a technické specifikace. Před vložením těchto údajů se provede kontrola kvality s cílem ověřit, že byly minimální normy kvality údajů a technické specifikace splněny.

2. Daktyloskopické údaje vkládané do SIS mohou sestávat z jednoho až deseti píchaných otisků prstů a z jednoho až deseti válených otisků prstů. Mohou rovněž zahrnovat až dva otisky dlaní.

3. Profil DNA může být doplněn do záznamů pouze v situacích podle čl. 32 odst. 1 písm. a), a to pouze po provedení kontroly kvality s cílem zjistit, zda byly splněny minimální normy kvality údajů a technické specifikace, a pouze pokud fotografie, zobrazení obličeje ani daktyloskopické údaje nejsou dostupné nebo nejsou vhodné pro identifikaci. Profily DNA osob, které jsou přímými předky, potomky či sourozenci osoby, která je předmětem záznamu, lze doplnit do záznamu, pouze pokud k tomu tyto osoby dají svůj výslovný souhlas. V případě, že je do záznamu doplněn profil DNA, musí tento profil obsahovat minimum informací nezbytně nutných k identifikaci pohřešované osoby.

4. Pro uchovávání biometrických údajů uvedených v odstavcích 1 a 3 tohoto článku se v souladu s odstavcem 5 tohoto článku stanoví minimální normy kvality údajů a technické specifikace. Tyto minimální normy kvality údajů a technické specifikace stanoví úroveň kvality požadované pro využívání údajů k ověření totožnosti osoby v souladu s čl. 43 odst. 1 a pro využívání údajů k identifikaci osoby v souladu s čl. 43 odst. 2 až 4.

5. Komise přijme prováděcí akty, jimiž stanoví minimální normy kvality údajů a technické specifikace uvedené v odstavcích 1 3 a 4 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

Článek 43

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

1. Pokud jsou fotografie, zobrazení obličeje, daktyloskopické údaje a profily DNA dostupné v záznamu v SIS, použijí se tyto fotografie, zobrazení obličeje, daktyloskopické údaje a profily DNA k potvrzení totožnosti osoby, která byla nalezena na základě alfanumerického vyhledávání v SIS.

2. Za účelem identifikace osoby lze v daktyloskopických údajích vyhledávat ve všech případech. Nelze-li však osobu identifikovat jinými prostředky, musí být za účelem identifikace osoby provedeno vyhledávání v daktyloskopických údajích. Za tímto účelem obsahuje centrální SIS systém automatizované identifikace otisků prstů (AFIS).

3. Daktyloskopické údaje v SIS v souvislosti se záznamy vloženými podle článků 26, 32, 36 a 40 lze vyhledávat též s použitím úplných či neúplných souborů otisků prstů či otisků dlaní zajištěných na místě spáchání vyšetřovaných závažných trestných činů nebo teroristických trestných činů, u nichž lze s vysokou mírou pravděpodobnosti stanovit, že patří pachateli daného trestného činu, a to za předpokladu, že jsou současně vyhledávány v příslušných vnitrostátních databázích otisků prstů.

4. Jakmile to bude z technického hlediska možné a bude-li zajištěna vysoká míra spolehlivosti identifikace, bude možné použít fotografie a zobrazení obličeje k identifikaci osoby na řádných hraničních přechodech.

Před zavedením této funkce v SIS předloží Komise zprávu o dostupnosti, připravenosti a spolehlivosti potřebné technologie. Tato zpráva bude konzultována s Evropským parlamentem.

Po zahájení používání této funkce na řádných hraničních přechodech se Komisi svěřuje pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 75 za účelem doplnění tohoto nařízení, pokud jde o určení dalších okolností, za nichž lze fotografie a zobrazení obličeje používat k identifikaci osob.

KAPITOLA XIII
PRÁVO PŘÍSTUPU K ZÁZNAMŮM A JEJICH PŘEZKUM

Článek 44

Příslušné vnitrostátní orgány mající právo přístupu k údajům v SIS

1. Příslušné vnitrostátní orgány mají přístup k údajům vloženým do SIS a právo v těchto údajích vyhledávat přímo nebo v kopii databáze SIS pro tyto účely:

   a) ochrana hranic v souladu s nařízením (EU) 2016/399;

   b) provádění policejních a celních kontrol v dotčeném členském státě, jakož i pro koordinaci těchto kontrol určenými orgány;

   c) prevence, odhalování, vyšetřování či stíhání teroristických trestných činů nebo jiných závažných trestných činů nebo výkonu trestů na území dotčeného členského států, pokud se na ně vztahuje směrnice (EU) 2016/680;

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, jakož i provádění kontrol státních příslušníků třetích zemí, kteří neoprávněně vstoupí na území členských států nebo na něm pobývají;

e) bezpečnostní kontroly státních příslušníků třetích zemí žádajících o mezinárodní ochranu, pokud orgány provádějící tyto kontroly nejsou „rozhodujícím orgánem“ ve smyslu čl. 2 písm. f) směrnice Evropského parlamentu a Rady 2013/32/EU[1], a případně poskytují poradenství v souladu s nařízením Rady (ES) č. 377/2004[2].

2. Právo přístupu k údajům v SIS a právo v těchto údajích přímo vyhledávat mohou v souladu s vnitrostátním právem vykonávat příslušné vnitrostátní orgány, které odpovídají za naturalizaci, pro účely přezkoumání žádosti o naturalizaci.

3. Právo přístupu k údajům vloženým do SIS a právo v těchto údajích přímo vyhledávat mohou při plnění svých úkolů vykonávat i vnitrostátní justiční orgány, včetně těch, které odpovídají za zahájení trestního stíhání a za vyšetřování před podáním obžaloby, jak je stanoveno ve vnitrostátním právu, jakož i jejich koordinační orgány.

---

[1] Směrnice Evropského parlamentu a Rady 2013/32/EU ze dne 26. června 2013 o společných řízeních pro přiznávání a odnímání statusu mezinárodní ochrany (Úř. věst. L 180, 29.6.2013, s. 60).

[2] Nařízení Rady (ES) č. 377/2004 ze dne 19. února 2004 o vytvoření sítě styčných úředníků pro přistěhovalectví (Úř. věst. L 64, 2. 3. 2004, s. 1).

4. Příslušné orgány uvedené v tomto článku se zahrnou na seznam uvedený v čl. 56 odst. 7.

Článek 45

Subjekty příslušné pro registraci vozidel

1. Subjekty v členských státech odpovědné za vydávání osvědčení o registraci vozidel uvedené ve směrnici Rady 1999/37/ES[1] mají přístup k údajům vloženým do SIS podle čl. 38 odst. 2 písm. a), b), c), m) a p) tohoto nařízení pouze pro účely ověření, zda vozidla a související osvědčení o registraci vozidel a registrační značky vozidel předložené k registraci nejsou odcizené, neoprávněně užívané či ztracené nebo se nejedná o doklady, které vypadají jako uvedené doklady, ale jsou falešné, nebo zda nejsou hledané za účelem zajištění důkazů v trestním řízení.

   Přístup subjektů uvedených v prvním pododstavci k těmto údajům se řídí vnitrostátním právem a omezuje se na pravomoci svěřené těmto subjektům.

2. Subjekty uvedené v odstavci 1, které jsou subjekty veřejné správy, mají právo přímého přístupu k údajům v SIS.

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

3. Subjekty uvedené v odstavci 1 tohoto článku, které nejsou subjekty veřejné správy, mají právo přístupu k údajům v SIS pouze prostřednictvím orgánu uvedeného v článku 44. 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 se nepoužije na přístup do SIS uskutečněný v souladu s tímto článkem. Sdělování informací zjištěných na základě přístupu do SIS policejním či justičním orgánům ze strany subjektů uvedených v odstavci 1 tohoto článku se řídí vnitrostátním právem.

Článek 46

Subjekty 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, včetně leteckých motorů, mají přístup k následujícím údajům vloženým do SIS v souladu s čl. 38 odst. 2 pouze pro účely ověření, zda plavidla, včetně lodních motorů, a letadla, včetně leteckých motorů, přihlašovaná k registraci nebo podléhající řízení provozu nejsou odcizená, neoprávněně užívaná nebo zda nejsou hledaná za účelem zajištění důkazů v trestním řízení:

   a) údaje o plavidlech;

   b) údaje o lodních motorech;

c) údaje o letadlech;

d) údaje o leteckých motorech.

Přístup subjektů uvedených v prvním pododstavci k těmto údajům se řídí vnitrostátním právem daného členského státu a omezuje se na pravomoci svěřené těmto subjektům.

2. Subjekty uvedené v odstavci 1, které jsou subjekty veřejné správy, mají právo přímého přístupu k údajům v SIS.

3. Subjekty uvedené v odstavci 1 tohoto článku, které nejsou subjekty veřejné správy, mají právo přístupu k údajům v SIS pouze prostřednictvím orgánu uvedeného v článku 44. Tento orgán má právo přímého přístupu k údajům a právo na jejich předání příslušnému 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 se nepoužije na přístup do SIS uskutečněný v souladu s tímto článkem. Sdělování informací zjištěných na základě přístupu do SIS policejním či justičním orgánům ze strany subjektů uvedených v odstavci 1 tohoto článku se řídí vnitrostátním právem.

Článek 47

Subjekty příslušné pro registraci střelných zbraní

1. Subjekty v členských státech odpovědné za vydávání osvědčení o registraci střelných zbraní mají přístup k údajům o osobách vloženým do SIS v souladu s články 26 a 36 a k údajům o střelných zbraních vloženým do SIS v souladu s čl. 38 odst. 2. Tento přístup se uskutečňuje pro účely ověření, zda osoba požadující registraci není hledaná za účelem zatčení a předání nebo vydání nebo pro účely skrytých, dotazovacích nebo zvláštních kontrol nebo zda střelné zbraně předložené k registraci nejsou hledané za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení.

2. Přístup subjektů uvedených v odstavci 1 k těmto údajům se řídí vnitrostátním právem a omezuje se na pravomoci svěřené těmto subjektům.

3. Subjekty uvedené v odstavci 1, které jsou subjekty veřejné správy, mají právo přímého přístupu k údajům v SIS.

4. Subjekty uvedené v odstavci 1, které nejsou subjekty veřejné správy, mají právo přístupu k údajům v SIS pouze prostřednictvím orgánu uvedeného v článku 44. Tento orgán má právo přímého přístupu k údajům a informuje dotčený subjekt, zda je možné střelnou zbraň registrovat. Dotčený členský stát zajistí, aby dotčený subjekt i jeho zaměstnanci byli povinni dodržovat veškerá omezení související s přípustným používáním údajů, které jim předal příslušný orgán.

5. Článek 39 se nepoužije na přístup do SIS uskutečněný v souladu s tímto článkem. Sdělování informací zjištěných na základě přístupu do SIS policejním či justičním orgánům ze strany subjektů uvedených v odstavci 1 tohoto článku se řídí vnitrostátním právem.

Článek 48

Přístup Europolu k údajům v SIS

1. Je-li to pro výkon jejích pravomocí nezbytné, má Agentura Evropské unie pro spolupráci v oblasti prosazování práva (Europol), zřízená nařízením (EU) 2016/794, právo přístupu k údajům v SIS a právo v těchto údajích vyhledávat. Europol může rovněž provádět výměnu doplňujících informací a požadovat další doplňující informace v souladu s ustanoveními příručky SIRENE.

2. Pokud vyhledávání provedené Europolem odhalí existenci záznamu v SIS, Europol o tom informuje vkládající členský stát formou výměny doplňujících informací prostřednictvím komunikační infrastruktury a v souladu s ustanoveními příručky SIRENE. Do doby, než bude Europol moci využívat funkcí pro výměnu doplňujících informací, informuje vkládající členské státy způsobem stanoveným v nařízení (EU) 2016/794.

3. Europol může zpracovávat doplňující informace, které mu byly poskytnuty členskými státy, pro účely jejich srovnání s vlastními databázemi a projekty operativní analýzy s cílem nalézt souvislosti nebo jiné důležité spojitosti a pro účely strategických, tematických nebo operativních analýz uvedených v čl. 18 odst. 2 písm. a), b) a c) nařízení (EU) 2016/794. Veškeré zpracování doplňujících informací Europolem pro účely uvedené v tomto článku se provádí v souladu s uvedeným nařízením.

4. Použití informací získaných na základě vyhledávání v SIS nebo zpracování doplňujících informací Europolem podléhá souhlasu vkládajícího 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 vkládajícího členského státu a při plném dodržování práva Unie v oblasti ochrany údajů.

5. Europol:

a) nepropojí, aniž jsou dotčena ustanovení odstavců 4 a 6, části SIS s žádným 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) vymaže, bez ohledu na čl. 31 odst. 1 nařízení (EU) 2016/794, doplňující informace obsahující osobní údaje nejpozději jeden rok od výmazu souvisejícího záznamu. Odchylně může Europol, pokud má ve svých databázích nebo projektech operativní analýzy informace o případu, jehož se doplňující informace týkají, za účelem plnění svých úkolů i nadále výjimečně uchovávat doplňující informace, je-li to nezbytné. Europol informuje vkládající členský stát a vykonávající členský stát o dalším uchovávání těchto doplňujících informací a toto uchovávání zdůvodní;

c) omezí přístup k údajům v SIS, včetně doplňujících informací, na konkrétně oprávněné pracovníky Europolu, pro něž je přístup k těmto údajům nezbytný k plnění jejich úkolů;

d) přijme a uplatňuje opatření pro zajištění bezpečnosti, důvěrnosti a vlastní kontroly v souladu s články 10, 11 a 13;

e) zajistí, aby jeho pracovníci oprávnění zpracovávat údaje v SIS absolvovali odpovídající odbornou přípravu a obdrželi informace v souladu s čl. 14 odst. 1; a

f) umožní, aniž je dotčeno nařízení (EU) 2016/794, evropskému inspektorovi ochrany údajů, aby sledoval a přezkoumával činnost Europolu při výkonu jeho práva přístupu k údajům v SIS a na vyhledávání v těchto údajích, jakož i při výměně a zpracování doplňujících informací.

6. Europol může pořizovat kopie údajů ze SIS pouze pro technické účely, pokud jsou potřebné k tomu, aby řádně zmocnění pracovníci Europolu mohli provádět přímé vyhledávání. Na tyto kopie se použije toto nařízení. Technická kopie se použije pouze pro účely uchovávání údajů SIS v průběhu vyhledávání údajů. Po dokončení vyhledávání se údaje vymažou. Tato použití nejsou považována za protiprávní stahování ani kopírování údajů SIS. Europol nesmí kopírovat údaje ze záznamů ani další údaje vložené členskými státy nebo získané z CS-SIS do jiných systémů Europolu.

7. Za účelem ověření zákonnosti zpracování údajů, pro vlastní kontrolu a pro zajištění řádného zabezpečení údajů a jejich neporušenosti vede Europol protokoly o každém přístupu do SIS a vyhledávání v tomto systému v souladu s ustanoveními článku 12. Tyto protokoly a dokumentace nejsou považovány za protiprávní stahování nebo kopírování jakékoli části SIS.

8. Členské státy sdělí Europolu prostřednictvím výměny doplňujících informací jakýkoli pozitivní nález záznamů týkajících se teroristických trestných činů. Členské státy nemusí ve výjimečných případech informovat Europol, pokud by to ohrozilo probíhající vyšetřování, bezpečnost fyzické osoby, nebo bylo v rozporu s podstatnými zájmy bezpečnosti vkládajícího členského státu.

9. Odstavec 8 se použije ode dne, kdy bude Europol schopen získávat doplňující informace podle odstavce 1.

Článek 49

Přístup Eurojustu k údajům SIS

1. Pouze národní členové Eurojustu a jejich asistenti mají v případech, kdy je to nezbytné pro plnění jejich úkolů, právo přístupu k údajům vloženým do SIS a právo v těchto údajích vyhledávat v rámci svých pravomocí 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 národní člen vkládající členský stát,. Informace získané na základě takového vyhledávání může Eurojust sdělit třetím státům a třetím subjektům pouze se souhlasem vkládajícího členského státu a při plném dodržování práva Unie v oblasti ochrany údajů.

3. Tímto článkem nejsou dotčena ustanovení nařízení Evropského parlamentu a Rady (EU) 2018/…[1+] a nařízení (EU) 2018/…[++] týkající se ochrany údajů a odpovědnosti národních členů Eurojustu a jejich asistentů za neoprávněné nebo nesprávné zpracování těchto údajů ani pravomoci evropského inspektora ochrany údajů podle uvedených nařízení.

4. Za účelem ověření zákonnosti zpracování údajů, pro vlastní kontrolu a pro zajištění řádného zabezpečení údajů a jejich neporušenosti povede Eurojust protokoly o každém přístupu do SIS a o vyhledávání v tomto systému provedeném národním členem Eurojustu nebo jeho asistentem v souladu s ustanoveními článkem 12.

5. Žádné části SIS se nepropojí s jakýmkoli systémem pro sběr a zpracování údajů provozovaným Eurojustem ani se do takového systému nepřenesou údaje ze SIS, k nimž mají tyto národní členové nebo jejich asistenti přístup. Žádná část SIS se nesmí stahovat ani kopírovat. Protokolování přístupu ani vyhledávání nejsou považovány za protiprávní stahování nebo kopírování údajů SIS.

6. Eurojust přijme a uplatňuje opatření za účelem zajištění bezpečnosti, důvěrnosti a vlastní kontroly v souladu s články 10, 11 a 13.

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2018/… ze dne ... o Agentuře Evropské unie pro justiční spolupráci v trestních věcech (Eurojust) a o nahrazení a zrušení rozhodnutí Rady 2002/187/SVV (Úř. věst. L ...).

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 37/18 a v poznámce pod čarou jeho číslo, datum přijetí a odkaz na vyhlášení v Úředním věstníku.

[++] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 31/18.

Článek 50

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

1. V souladu s čl. 40 odst. 8 nařízení (EU) 2016/1624 mají příslušníci jednotek a členové týmů ve smyslu čl. 2 bodů 8 a 9 uvedeného nařízení v rámci svých pravomocí a za předpokladu, že jsou oprávněni provádět kontroly v souladu s čl. 44 odst. 1 tohoto nařízení a že absolvovali odpovídající odbornou přípravu v souladu s čl. 14 odst. 1 tohoto nařízení, právo přístupu k údajům v SIS a právo v těchto údajích vyhledávat v rozsahu, v jakém je to nezbytné pro plnění jejich úkolů a v jakém to vyžaduje operační plán pro konkrétní operaci. Přístup k údajům v SIS nelze rozšířit na žádné jiné příslušníky jednotek a členy týmů.

2. Příslušníci jednotek a členové týmů uvedení v odstavci 1 vykonávají toto právo přístupu k údajům v SIS a právo v těchto údajích vyhledávat podle odstavce 1 prostřednictvím technického rozhraní. Technické rozhraní vytvoří a spravuje Evropská agentura pro pohraniční a pobřežní stráž a umožňuje jeho přímé propojení s centrálním SIS.

3. Pokud vyhledávání provedené příslušníky jednotek nebo členy týmů uvedenými v odstavci 1 tohoto článku odhalí existenci záznamu v SIS, musí být o tom informován vkládající 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 tohoto státu, kteří se podílejí na úkolech spojených s navracením. Hostitelský členský stát může příslušníky jednotek a členy týmů zmocnit k tomu, aby jednali jeho jménem.

4. Za účelem ověření zákonnosti zpracování údajů, pro vlastní kontrolu a pro zajištění řádného zabezpečení údajů a jejich neporušenosti vede Evropská agentura pro pohraniční a pobřežní stráž v souladu s ustanoveními článku 12 protokoly o každém přístupu do SIS a vyhledávání v tomto systému.

5. Evropská agentura pro pohraniční a pobřežní stráž přijme a uplatňuje opatření pro zajištění bezpečnosti, důvěrnosti a vlastní kontroly v souladu s články 10, 11 a 13 a zajistí, aby jednotky a týmy uvedené v odstavci 1 tohoto článku tato opatření uplatňovaly.

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

7. Aniž je dotčen odstavec 2, žádné části SIS se nepropojí s jakýmkoli systémem pro sběr a zpracování údajů provozovaným jednotkami či týmy uvedenými v odstavci 1 nebo Evropskou agenturou pro pohraniční a pobřežní stráž, ani se do takového systému nepřenesou údaje ze SIS, k nimž mají tyto jednotky a týmy přístup. Žádná část SIS se nesmí stahovat ani kopírovat. Protokolování přístupu ani vyhledávání nejsou považovány za protiprávní stahování nebo kopírování údajů SIS.

8. Evropská agentura pro pohraniční a pobřežní stráž umožní evropskému inspektorovi ochrany údajů sledovat a přezkoumávat činnosti jednotek a týmů uvedených v tomto článku při výkonu jejich práva přístupu a vyhledávání v údajích vložených v SIS. Tím nejsou dotčena další ustanovení nařízení (EU) 2018/...[+].

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 31/18.

Článek 51

Hodnocení využívání SIS Europolem, Eurojustem
a Evropskou agenturou pro pohraniční a pobřežní stráž

1. Komise provádí hodnocení provozu a využívání SIS Europolem, národními členy Eurojustu a jejich asistenty a jednotkami a týmy uvedenými v čl. 50 odst. 1 alespoň každých pět let.

2. Europol, Eurojust a Evropská agentura pro pohraniční a pobřežní stráž zajistí náležitá opatření v návaznosti na zjištění a doporučení vyplývající z tohoto hodnocení.

3. Zpráva o výsledcích hodnocení a navazujících opatřeních se zasílá Evropskému parlamentu a Radě.

Článek 52

Rozsah přístupu

Koncoví uživatelé, včetně Europolu, národních členů Eurojustu a jejich asistentů a příslušníků jednotek a členů týmů ve smyslu čl. 2 bodů 8 a 9 nařízení (EU) 2016/1624, mají přístup pouze k údajům, které jsou nezbytné pro plnění jejich úkolů.

Článek 53

Doba pro přezkum záznamů o osobách

1. Záznamy o osobách se uchovávají pouze po dobu nezbytnou pro splnění účelů, pro které byly vloženy.

2. Členský stát může záznam o osobě pro účely článku 26 a čl. 32 odst. 1 písm. a) a b) vložit na dobu pěti let. Vkládající členský stát během těchto pěti let přezkoumá nutnost jej uchovávat.

3. Členský stát může záznam o osobě pro účely článků 34 a 40 vložit na dobu tří let. Vkládající členský stát během těchto tří let přezkoumá nutnost jej uchovávat.

4. Členský stát může záznam o osobě pro účely čl. 32 odst. 1 písm. c), d) a e) a článku 36 vložit na dobu jednoho roku. Vkládající členský stát během tohoto jednoho roku přezkoumá nutnost jej uchovávat.

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

6. Vkládající členský stát může v době pro přezkum uvedené v odstavcích 2, 3 a 4 na základě souhrnného individuálního posouzení, které zaznamená, rozhodnout o delší době uchovávání záznamu o osobě, než je doba pro přezkum, je-li to nezbytné a přiměřené pro účely, pro něž byl záznam vložen. V tomto případě se použijí odstavec 2, 3 či 4 také na prodloužení doby uchování. Takové prodloužení musí být sděleno CS-SIS.

7. Záznamy o osobách se automaticky vymazávají po uplynutí doby pro přezkum uvedené v odstavcích 2, 3 a 4, s výjimkou případů, kdy vkládající členský stát informoval CS-SIS o prodloužení podle odstavce 6. O plánovaném výmazu údajů uvědomí CS-SIS vkládající členský stát automaticky čtyři měsíce před tímto výmazem.

8. Členské státy vedou statistiky o počtu záznamů o osobách, jejichž doba uchování byla prodloužena podle odstavce 6 tohoto článku, a předají je na žádost dozorovým úřadům uvedeným v článku 69.

9. Jakmile je některé centrále SIRENE zřejmé, že záznam o určité osobě splnil svůj účel a měl by být proto vymazán, oznámí to okamžitě orgánu, který záznam vytvořil. Daný orgán má 15 kalendářních dní od obdržení tohoto oznámení na to, aby sdělil, zda záznam byl či má být vymazán, nebo uvedl důvody pro uchování záznamu. Pokud v této patnáctidenní lhůtě k tomuto sdělení nedojde, zajistí centrála SIRENE výmaz záznamu. Dovolují-li to vnitrostátní právo, vymaže záznam centrála SIRENE. Centrály SIRENE hlásí svému dozorovému úřadu veškeré opakující se problémy, které se vyskytly při jejich činnosti podle tohoto odstavce.

Článek 54

Doba pro přezkum záznamů o věcech

1. Záznamy o věcech se uchovávají pouze po dobu nezbytnou pro splnění účelů, pro které byly vloženy.

2. Členský stát může záznam o věcech pro účely článků 36 a 38 vložit na dobu deseti let. Vkládající členský stát během těchto deseti let přezkoumá nutnost jej uchovávat.

3. Záznamy o věcech, které byly vloženy v souladu s články 26, 32, 34 a 36, se přezkoumávají podle článku 53, jsou-li tyto záznamy propojeny se záznamem o osobě. Tyto záznamy mohou být uchovávány pouze po dobu, po kterou je uchováván záznam o osobě.

4. Vkládající členský stát může během doby pro přezkum uvedené v odstavcích 2 a 3 rozhodnout o uchovávání záznamu o věci po delší dobu, je-li to nezbytné pro účely, pro něž byl záznam vložen. V těchto případech se odstavec 2 nebo 3 použije obdobně.

5. Komise může přijmout prováděcí akty, kterými stanoví kratší doby pro přezkum pro určité kategorie záznamů o věcech. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

6. Členské státy vedou statistiky o počtu záznamů o věcech, jejichž doba uchovávání byla prodloužena podle odstavce 4.

KAPITOLA XIV
VÝMAZ ZÁZNAMŮ

Článek 55

Výmaz záznamů

1. Záznamy za účelem zatčení a předání nebo vydání podle článku 26 se vymažou poté, co je osoba předána nebo vydána příslušným orgánům vkládajícího členského státu. Vymažou se rovněž v případě, že justiční rozhodnutí, na němž byl záznam založen, bylo prohlášeno za neplatné příslušným justičním orgánem podle vnitrostátního práva. Vymažou se rovněž po uplynutí platnosti záznamu podle článku 53.

2. Záznamy o pohřešovaných osobách nebo zranitelných osobách, kterým je třeba zabránit v cestování podle článku 32, se vymažou v souladu s těmito pravidly:

   a) v případě pohřešovaných dětí a dětí, kterým hrozí nebezpečí únosu, se záznam vymaže:

      (i) po vyřešení případu, například když bylo dítě nalezeno nebo repatriováno nebo příslušné orgány vykonávajícího členského státu přijaly rozhodnutí o péči o dítě;

      (ii) po uplynutí platnosti záznamu podle článku 53; nebo

      (iii) na základě rozhodnutí příslušného orgánu vkládajícího členského státu;

b) v případě pohřešovaných dospělých osob, pokud se nevyžadují ochranná opatření, se záznam vymaže:

(i) po vykonání opatření, jež má být přijato, pokud vykonávající členský stát potvrdí místo jejich pobytu;

(ii) po uplynutí platnosti záznamu podle článku 53; nebo

(iii) na základě rozhodnutí příslušného orgánu vkládajícího členského státu;

c) v případě pohřešovaných dospělých osob, pokud se vyžadují ochranná opatření, se záznam vymaže:

(i) po vykonání opatření, jež má být přijato, pokud je daná osoba umístěna pod ochranu;

(ii) po uplynutí platnosti záznamu podle článku 53; nebo

(iii) na základě rozhodnutí příslušného orgánu vkládajícího členského státu;

d) v případě zranitelných osob, které jsou zletilé a kterým je třeba zabránit v cestování v zájmu jejich vlastní ochrany, a dětí, kterým je třeba zabránit v cestování, se záznam vymaže:

(i) po vykonání opatření, jež má být přijato, například umístění osoby pod ochranu;

(ii) po uplynutí platnosti záznamu podle článku 53; nebo

(iii) na základě rozhodnutí příslušného orgánu vkládajícího členského státu.

Aniž je dotčeno vnitrostátní právo, může být u osoby, jež byla umístěna do ústavní péče na základě rozhodnutí příslušného orgánu, záznam uchováván, dokud není tato osoba repatriována.

3. Záznam o osobách hledaných za účelem předvolání justičními orgány podle článku 34 se vymaže:

a) poté, co je příslušnému orgánu vkládajícího členského státu sděleno místo pobytu hledané osoby;

b) po uplynutí platnosti záznamu podle článku 53; nebo

c) na základě rozhodnutí příslušného orgánu vkládajícího členského státu.

Pokud na základě zaslaných informací uvedených v písmeni a) nelze učinit další kroky, informuje centrála SIRENE vkládajícího členského státu za účelem vyřešení problému centrálu SIRENE vykonávajícího členského státu.

Jestliže byl učiněn pozitivní nález a vkládajícímu členskému státu byla zaslána adresa a následný pozitivní nález v tomtéž vykonávajícím členském státě odhalí stejnou adresu, zaznamená se pozitivní nález ve vykonávajícím členském státě, ale vkládajícímu členskému státu se znovu nezasílá ani adresa, ani doplňující informace. V takových případech vykonávající členský stát informuje vkládající členský stát o opakovaných pozitivních nálezech a vkládající členský stát provede souhrnné individuální posouzení nutnosti záznam uchovávat.

4. Záznam o skrytých, dotazovacích a zvláštních kontrolách podle článku 36 se vymaže:

a) po uplynutí platnosti záznamu podle článku 53; nebo

b) na základě rozhodnutí příslušného orgánu vkládajícího členského státu.

5. Záznam o věcech hledaných za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení podle článku 38 se vymaže:

a) po zabavení věci nebo rovnocenném opatření poté, co se uskutečnila nezbytná následná výměna doplňujících informací mezi dotčenými centrálami SIRENE, nebo se věc stala předmětem jiného soudního nebo správního řízení;

b) po uplynutí platnosti záznamu podle článku 53; nebo

c) na základě rozhodnutí příslušného orgánu vkládajícího členského státu o jeho vymazání.

6. Záznam o neznámých hledaných osobách podle článku 40 se vymaže:

a) po identifikaci dané osoby; nebo

b) po uplynutí platnosti záznamu podle článku 53; nebo

c) na základě rozhodnutí příslušného orgánu vkládajícího členského státu o jeho vymazání.

7. Pokud jsou záznamy o věcech, které byly vloženy v souladu s články 26, 32, 34 a 36, propojeny se záznamem o osobě, vymažou se poté, co byl vymazán záznam o osobě v souladu s tímto článkem.

KAPITOLA XV
OBECNÁ PRAVIDLA PRO ZPRACOVÁNÍ ÚDAJŮ

Článek 56

Zpracování údajů SIS

1. Členské státy mohou zpracovávat údaje uvedené v článku 20 pouze pro účely stanovené pro každou kategorii záznamů 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 příslušnými orgány uvedenými v článku 44. Na tyto kopie se použije toto nařízení. Členské státy nesmějí kopírovat údaje v záznamech nebo další údaje vložené jiným členským státem 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 po dobu nepřesahující 48 hodin.

   Členské státy uchovávají aktuální soupis těchto kopií, zpřístupňují tento soupis svým dozorovým úřadům a zajišťují, že se na tyto kopie použije toto nařízení, zejména článek 10.

4. Přístup vnitrostátních orgánů uvedených v článku 44 k údajům v SIS se povoluje pouze v mezích pravomocí těchto orgánů a pouze jejich řádně zmocněným pracovníkům.

5. Pokud jde o záznamy podle článků 26, 32, 34, 36, 38 a 40 tohoto nařízení, jakékoli zpracování informací v SIS pro jiné účely než účely, pro které do něj byly vloženy, musí být spojeno s konkrétním případem a odůvodněno nezbytností předcházet bezprostřednímu a závažnému ohrožení veřejného pořádku a veřejné bezpečnosti, a to z vážných důvodů národní bezpečnosti nebo s cílem předejít závažnému trestnému činu. Za tímto účelem musí být předem získáno povolení vkládajícího členského státu.

6. Jakékoli využití údajů SIS, které není v souladu s odstavci 1 až 5 tohoto článku, je podle vnitrostátního práva každého členského státu považováno za zneužití a podléhá sankcím podle článku 73.

7. Každý členský stát zašle agentuře eu-LISA seznam příslušných orgánů, které jsou podle tohoto nařízení oprávněny přímo vyhledávat v údajích 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 eu-LISA zajistí každoroční zveřejnění seznamu v *Úředním věstníku Evropské unie*. Agentura eu-LISA vede na svých internetových stránkách průběžně aktualizovaný seznam změn, které členské státy zasílají mezi ročními zveřejněními.

8. Neobsahuje-li právo Unie zvláštní ustanovení, použije se na údaje v N.SIS právo příslušného členského státu.

Článek 57

Údaje SIS a vnitrostátní soubory

1. Ustanovením čl. 56 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 nejvýše po dobu tří let s výjimkou případů, kdy konkrétní ustanovení vnitrostátního práva stanoví delší období uchovávání.

2. Ustanovením čl. 56 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 58

Informování v případě nevykonání záznamu

Nemůže-li být požadované opatření vykonáno, členský stát, který byl o jeho výkon požádán, o tom okamžitě uvědomí vkládající členský stát prostřednictvím výměny doplňujících informací.

Článek 59

Kvalita údajů v SIS

1. Vkládají členský stát odpovídá za zajištění toho, že údaje v SIS jsou správné, aktuální a jsou vloženy do SIS a v něm uchovávány v souladu se zákonem.

2. Pokud vkládající členský stát obdrží relevantní doplňující nebo odlišné údaje uvedené v čl. 20 odst. 3, neprodleně dotčený záznam doplní nebo upraví.

3. Pouze vkládající členský stát je oprávněn měnit, doplňovat, opravovat, aktualizovat nebo mazat údaje, které vložil do SIS.

4. Pokud má jiný než vkládající členský stát relevantní doplňující nebo odlišné údaje uvedené v čl. 20 odst. 3, neprodleně je předá prostřednictvím výměny doplňujících informací vkládajícímu členskému státu, aby mu umožnil záznam doplnit či upravit. Doplňující nebo odlišné údaje týkající se osob se předají, pouze pokud nejsou pochybnosti o totožnosti dané osoby.

5. Pokud má jiný než vkládající členský stát důkazy naznačující, že položka údaje je věcně nesprávná nebo je uchovávána protiprávně, informuje o tom co nejdříve a nejpozději do dvou pracovních dnů poté, co se o uvedeném důkazu dozvěděl, vkládající členský stát, prostřednictvím výměny doplňujících informací. Vkládající členský stát informaci prověří a v případě potřeby dotyčnou položku neprodleně opraví nebo vymaže.

6. Nemohou-li se členské státy dohodnout ve lhůtě dvou měsíců od okamžiku, kdy se důkazy poprvé objevily, jak je uvedeno v odstavci 5 tohoto článku, předloží členský stát, jenž záznam nevložil, příslušným dozorovým úřadům a evropskému inspektorovi ochrany údajů věc k rozhodnutí v rámci spolupráce podle článku 71.

7. 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 stěžovatel skutečně není osobou, k níž se má záznam vztahovat, je stěžovatel informován o opatřeních stanovených v článku 62 a o svém právu na ochranu podle čl. 68 odst. 1.

Článek 60

Bezpečnostní incidenty

1. Každá událost, která má nebo může mít dopad na bezpečnost SIS nebo může způsobit poškození nebo ztrátu údajů SIS nebo doplňujících informací, se považuje za bezpečnostní incident, zejména pokud mohlo dojít k protiprávnímu přístupu k údajům nebo 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. Aniž je dotčeno ohlašování a oznamování případů porušení zabezpečení osobních údajů podle článku 33 nařízení (EU) 2016/679 nebo článku 30 směrnice (EU) 2016/680, členské státy, Europol, Eurojust a Evropská agentura pro pohraniční a pobřežní stráž neprodleně ohlašují bezpečnostní incidenty Komisi, agentuře eu-LISA, příslušnému dozorovému úřadu a evropskému inspektorovi ochrany údajů. Agentura eu-LISA ohlašuje neprodleně Komisi a evropskému inspektorovi ochrany údajů každý bezpečnostní incident týkající se centrálního SIS.

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

5. V případě bezpečnostního incidentu členské státy a agentura eu-LISA spolupracují.

6. O závažných incidentech podá Komise okamžitě zprávu Evropskému parlamentu a Radě. Tyto zprávy jsou v souladu s příslušnými bezpečnostními pravidly označeny stupněm utajení EU RESTRICTED/RESTREINT UE.

7. Pokud je bezpečnostní incident způsoben zneužitím údajů, zajistí členské státy, Europol, Eurojust a Evropská agentura pro pohraniční a pobřežní stráž uložení sankcí v souladu s článkem 73.

Článek 61

Rozlišování mezi osobami s podobnými znaky

1. Pokud se při vkládání nového záznamu ukáže, že v SIS již existuje záznam o osobě se stejnými prvky popisu totožnosti, kontaktuje centrála SIRENE do 12 hodin vkládající členský stát prostřednictvím výměny doplňujících informací s cílem porovnat, zda se záznam týká stejné osoby či nikoli.

2. Prokáže-li porovnání, že osoba, jež je předmětem nového záznamu, a osoba, o níž již byl záznam do SIS vložen, je skutečně tatáž osoba, použije centrála SIRENE postup vkládání vícenásobných záznamů uvedený v článku 23.

3. Prokáže-li porovnání, že se ve skutečnosti jedná o dvě různé osoby, schválí centrála SIRENE požadavek na vložení dalšího záznamu, a to tak, že doplní potřebné údaje, které zabrání jakýmkoli chybným identifikacím.

Článek 62

Další údaje pro účely řešení zneužití totožnosti

1. Může-li dojít k záměně mezi osobou, která má být předmětem záznamu, a osobou, jejíž totožnost byla zneužita, doplní vkládající členský stát tento záznam o údaje týkající se osoby, jejíž totožnost byla zneužita, za podmínky jejího výslovného souhlasu, aby se předešlo nežádoucím důsledkům chybné identifikace. Kdokoliv, jehož totožnost byla zneužita, má právo odvolat svůj souhlas se zpracováním doplněných osobních údajů.

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 předmětem záznamu; a

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

3. Pro účely tohoto článku a s výhradou výslovného souhlasu osoby, jejíž totožnost byla zneužita, lze pro každou kategorii údajů do SIS vložit a dále v něm zpracovávat pouze tyto osobní údaje osoby, jejíž totožnost byla zneužita:

   a) příjmení;

   b) jméno(a);

c) rodné(á) příjmení;

d) dříve užívané(á) jméno(a) a alias, která mohou být vložena 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, otisky dlaní nebo oboje;

k) veškeré státní příslušnosti dotčené osoby;

l) druh dokladů totožnosti;

m) země vydání dokladů totožnosti;

n) číslo nebo čísla dokladů totožnosti;

o) datum vydání dokladů totožnosti;

p) adresa;

q) jméno otce;

r) jméno matky.

4. Komise přijme prováděcí akty, jimiž stanoví a dále rozvíjí technická pravidla nezbytná pro vkládání a další zpracování údajů uvedených v odstavci 3 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

5. Údaje uvedené v odstavci 3 se vymažou současně s výmazem odpovídajícího záznamu nebo dříve, pokud o to daná osoba požádá.

6. K údajům uvedeným v odstavci 3 mohou mít přístup pouze orgány mající právo přístupu k odpovídajícímu záznamu. Mohou tak učinit pouze za účelem předcházení chybné identifikaci.

Článek 63

Propojení záznamů

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

2. Vytvoření propojení nemá dopad na konkrétní opatření, které má být provedeno na základě jednotlivého záznamu opatřeného propojením, nebo na dobu pro přezkum jednotlivých propojených záznamů.

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

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

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

6. Komise přijme prováděcí akty, jimiž stanoví a dále rozvíjí technická pravidla pro propojování záznamů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

Článek 64

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 od výmazu souvisejícího záznamu ze SIS.

3. Odstavcem 2 není dotčeno právo členského státu uchovávat ve vnitrostátních souborech údaje týkající se konkrétního záznamu, který tento členský stát vložil, nebo záznamu, ve spojení s nímž bylo učiněno opatření na jeho území. Doba, po kterou mohou být takové údaje v těchto souborech uchovány, se řídí vnitrostátním právem.

Článek 65

Poskytnutí osobních údajů třetím stranám

Údaje zpracovávané v SIS a související doplňující informace vyměňované podle tohoto nařízení se nesmějí poskytovat ani zpřístupňovat žádným třetím zemím nebo mezinárodním organizacím.

KAPITOLA XVI
OCHRANA ÚDAJŮ

Článek 66

Příslušné právní předpisy

1. Na zpracování osobních údajů agenturou eu-LISA, Evropskou agenturou pro pohraniční a pobřežní stráž a Eurojustem podle tohoto nařízení se vztahuje nařízení (EU) 2018/...[+]. Na zpracování osobních údajů Europolem podle tohoto nařízení se vztahuje nařízení (EU) 2016/794.

2. Na zpracování osobních údajů příslušnými vnitrostátními orgány a subjekty pro účely prevence, odhalování, vyšetřování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení se vztahuje směrnice (EU) 2016/680.

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 31/18.

3. Na zpracování osobních údajů příslušnými vnitrostátními orgány a subjekty, s výjimkou zpracování pro účely prevence, odhalování, vyšetřování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, se vztahuje nařízení (EU) 2016/679.

Článek 67

Právo přístupu, oprava nesprávných údajů a výmaz protiprávně uchovávaných údajů

1. Subjekty údajů musí mít možnost vykonávat svá práva stanovená v článcích 15, 16 a 17 nařízení (EU) 2016/679 a v článku 14 a v čl. 16 odst. 1 a 2 směrnice (EU) 2016/680.

2. Jiný než vkládající členská stát může poskytnout subjektu údajů informace o zpracovávaných údajích, které jsou jeho osobními údaji pouze tehdy, pokud před tím poskytl vkládajícímu členskému státu příležitost zaujmout stanovisko. Komunikace mezi těmito členskými státy je zajišťována prostřednictvím výměny doplňujících informací.

3. 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 základním právům a oprávněným zájmům dotčeného subjektu údajů nezbytné a přiměřené opatření v demokratické společnosti s cílem:

   a) zabránit maření správních nebo soudních šetření, vyšetřování nebo řízení;

b) zabránit nepříznivému ovlivňování prevence, odhalování, vyšetřování či stíhání trestných činů nebo výkonu trestů;

c) chránit veřejnou bezpečnost;

d) chránit národní bezpečnost; nebo

e) chránit práva a svobody druhých.

V případech uvedených v prvním pododstavci členský stát písemně a bez zbytečného odkladu informuje subjekt údajů o jakémkoli odepření nebo omezení přístupu a o důvodech tohoto odepření nebo omezení. Tyto informace není třeba uvádět, pokud by jejich poskytnutí ohrožovalo některý z účelů uvedených v prvním pododstavci písm. a) až e). Členský stát informuje subjekt údajů o možnosti podat stížnost u dozorového úřadu nebo žádat soudní ochranu.

Členský stát zdokumentuje věcné či právní důvody, na nichž se rozhodnutí o neposkytnutí informací subjektu údajů zakládá. Tyto informace se zpřístupní dozorovým úřadům.

V takových případech musí mít subjekt údajů možnost vykonávat svá práva i prostřednictvím příslušných dozorových úřadů.

4. Po podání žádosti o přístup, opravu či výmaz daný členský stát co nejdříve, a v každém případě ve lhůtách uvedených v čl. 12 odst. 3 nařízení (EU) 2016/679, subjekt údajů informuje o opatřeních navazujících na výkon práv podle tohoto článku, bez ohledu na to, zda se nachází ve třetí zemi, či nikoliv.

Článek 68

Právní ochrana

1. Aniž jsou dotčena ustanovení nařízení (EU) 2016/679 a směrnice (EU) 2016/680 týkající se právní ochrany, má jakákoliv osoba právo podat návrh na zahájení řízení u jakéhokoli orgánu příslušného podle práva kteréhokoliv členského státu, včetně soudu, zejména ve věci přístupu, opravy, výmazu, obdržení informace nebo náhradu újmy v souvislosti se záznamem, který se ho týká.

2. Aniž je dotčen článek 72, zavazují se členské státy navzájem vymáhat pravomocná rozhodnutí vydaná soudy nebo orgány uvedenými v odstavci 1 tohoto článku.

3. Členské státy podávají Evropskému sboru pro ochranu osobních údajů každoročně zprávy uvádějící:

   a) počet žádostí o přístup, které byly podány správci údajů, a počet případů, v nichž byl přístup k údajům poskytnut;

   b) počet žádostí o přístup, které byly podány dozorovému úřadu, a počet případů, v nichž byl přístup k údajům poskytnut;

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

   d) počet žádostí o opravu nesprávných údajů a výmaz protiprávně uchovávaných údajů, které byly podány dozorovému úřadu;

e) počet zahájených soudních řízení;

f) počet případů, v nichž soud rozhodl ve prospěch žalobce;

g) jakékoli připomínky k případům vzájemného uznávání pravomocných rozhodnutí vydaných soudy nebo orgány jiných členských států v souvislosti se záznamy vloženými vkládajícím členským státem.

Komise vypracuje vzor pro podávání zpráv uvedených v tomto odstavci.

4. Zprávy členských států se zahrnou do společné zprávy uvedené v čl. 71 odst. 4.

Článek 69

Dohled nad N.SIS

1. Každý členský stát zajistí, aby nezávislý dozorový úřad, který byl v každém členském státě určen a který má pravomoci uvedené v kapitole VI nařízení (EU) 2016/679 nebo kapitole VI směrnice (EU) 2016/680, kontroloval zákonnost zpracování osobních údajů v SIS na svém území a jejich předávání mimo své území, včetně výměny a dalšího zpracování doplňujících informací na svém území.

2. Dozorové úřady zajistí, aby byl alespoň jednou za čtyři roky v souladu s mezinárodními auditorskými standardy proveden audit činností zpracování údajů v N.SIS. Audit provádějí dozorové úřady, nebo si jej dozorové úřady přímo vyžádají od nezávislého auditora pro ochranu údajů. Dozorové úřady si za všech okolností zachovají kontrolu nad nezávislým auditorem a přebírají za něj odpovědnost.

3. Členské státy zajistí, aby jejich dozorové úřady měly dostatek zdrojů k plnění úkolů, které jim toto nařízení ukládá, a měly přístup k poradenství poskytovanému osobami s dostatečnými znalostmi týkajícími se biometrických údajů.

Článek 70

Dohled nad agenturou eu-LISA

1. Evropský inspektor ochrany údajů je zodpovědný za kontrolu zpracovávání osobních údajů agenturou eu-LISA a za zajištění toho, aby toto zpracovávání bylo prováděno v souladu s tímto nařízením. Úkoly a pravomoci uvedené v článcích 57 a 58 nařízení (EU) 2018/...[+] se použijí obdobně.

2. Evropský inspektor ochrany údajů provede alespoň jednou za čtyři roky v souladu s mezinárodními auditorskými standardy audit zpracovávání osobních údajů agenturou eu-LISA. Zpráva o tomto auditu se zasílá Evropskému parlamentu, Radě, agentuře eu-LISA, Komisi a dozorovým úřadům. Agentura eu-LISA má možnost se ke zprávě před jejím přijetím vyjádřit.

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 31/18.

Článek 71

Spolupráce dozorových úřadů s evropským inspektorem ochrany údajů

1. Dozorové úřady 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. Dozorové úřady a evropský inspektor ochrany údajů, každý z nich v rozsahu svých příslušných pravomocí, si vyměňují příslušné informace, poskytují si navzájem pomoc při provádění auditů a kontrol, přezkoumávají obtíže týkající se výkladu nebo použití tohoto nařízení nebo jiných použitelných 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 dozorové úřady a evropský inspektor ochrany údajů setkávají alespoň dvakrát ročně v rámci Evropského sboru pro ochranu osobních údajů. Náklady na tato setkání nese a jejich organizaci zajišťuje Evropský sbor pro ochranu osobních údajů. Na prvním setkání přijmou jednací řád. Podle potřeby se společně vypracují další pracovní metody.

4. Evropský sbor pro ochranu osobních údajů zasílá každoročně Evropskému parlamentu, Radě a Komisi společnou zprávu o činnosti týkající se koordinovaného dohledu.

KAPITOLA XVII
ODPOVĚDNOST A SANKCE

Článek 72

Odpovědnost

1. Aniž jsou dotčeny právo na náhradu újmy a odpovědnost podle nařízení (EU) 2016/679, směrnice (EU) 2016/680 a nařízení (EU) 2018/…[+]:

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

   b) každá osoba nebo členský stát, jimž vznikla majetková či nemajetková újma v důsledku jakéhokoliv činu agentury eu-LISA neslučitelného s tímto nařízením, má nárok na náhradu vzniklé újmy od agentury eu-LISA.

   Členský stát nebo agentura eu-LISA jsou zcela nebo zčásti zproštěny odpovědnosti podle prvního pododstavce, pokud prokáží, že nenesou odpovědnost za událost vedoucí ke vzniku újmy.

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 31/18.

2. Pokud jakékoli nesplnění povinností členského státu podle tohoto nařízení způsobí SIS újmu, odpovídá za ni tento členský stát, ledaže by agentura eu-LISA nebo jiný členský stát účastnící se SIS opomenuly přijmout přiměřená opatření k zabránění vzniku újmy nebo zmírnění jejích následků.

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

Článek 73

Sankce

Členské státy zajistí, aby jakékoli zneužití údajů SIS nebo zpracovávání těchto údajů nebo jakákoli výměna doplňujících informací v rozporu s tímto nařízením podléhaly sankcím v souladu s vnitrostátním právem.

Stanovené sankce musí být účinné, přiměřené a odrazující.

KAPITOLA XVIII
ZÁVĚREČNÁ USTANOVENÍ

Článek 74

Sledování a statistiky

1. Agentura eu-LISA 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, podávání zpráv, podávání zpráv o kvalitě údajů a pro účely statistik má agentura eu-LISA přístup k potřebným informacím, které se týkají operací zpracovávání údajů prováděných v centrálním SIS.

3. Agentura eu-LISA vypracovává denní, měsíční a roční statistiky, a to pro každý členský stát i souhrnně, o počtu evidovaných vstupů podle kategorie záznamů. Agentura eu-LISA rovněž poskytuje roční zprávy o počtu pozitivních nálezů podle kategorie záznamů, počtu vyhledávání v SIS a počtu přístupů do SIS za účelem vložení, aktualizace nebo výmazu záznamu, a to pro každý členský stát i souhrnně. Vypracované statistiky neobsahují osobní údaje. Roční statistická zpráva se zveřejní.

4. Členské státy, Europol, Eurojust a Evropská agentura pro pohraniční a pobřežní stráž poskytnou agentuře eu-LISA a Komisi informace nezbytné pro vypracování zpráv uvedených v odstavcích 3, 6, 8 a 9.

5. Tyto informace zahrnují oddělené statistiky o počtu vyhledávání provedených subjekty v členských státech odpovědnými za vydávání osvědčení o registraci vozidel a subjekty v členských státech odpovědnými za vydávání osvědčení o registraci nebo za zajištění řízení provozu u plavidel, včetně lodních motorů, a dále letadel, včetně leteckých motorů, a střelných zbraní, nebo jménem těchto subjektů. Statistiky rovněž uvádějí počet pozitivních nálezů podle kategorie záznamů.

6. Agentura eu-LISA poskytne Evropskému parlamentu, Radě, členským státům, Komisi, Europolu, Eurojustu, Evropské agentuře pro pohraniční a pobřežní stráž a evropskému inspektorovi ochrany údajů všechny statistické zprávy, které vypracuje.

Za účelem sledování toho, jak jsou prováděny právní akty Unie, mimo jiné i pro účely nařízení (EU) č. 1053/2013, může Komise požádat agenturu eu-LISA o předložení dalších konkrétních statistických zpráv, pravidelných nebo účelových, o výkonnosti a využívání SIS a o výměně doplňujících informací.

Evropská agentura pro pohraniční a pobřežní stráž může požádat agenturu eu-LISA o předložení dalších konkrétních statistických zpráv, pravidelných nebo účelových, za účelem provádění analýz rizik a hodnocení zranitelnosti ve smyslu článků 11 a 13 nařízení (EU) 2016/1624.

7. Pro účely čl. 15 odst. 4 a odstavců 3, 4 a 6 tohoto článku agentura eu-LISA zřídí, vytvoří a provozuje ve svých technických prostorách centrální úložiště obsahující údaje uvedené v čl. 15 odst. 4 a v odstavci 3 tohoto článku, které nedovolí individuální identifikaci, ale umožní Komisi a agenturám uvedeným v odstavci 6 tohoto článku získat příslušné zprávy a statistiky. Agentura eu-LISA poskytne členským státům, Komisi, Europolu, Eurojustu a Evropské agentuře pro pohraniční a pobřežní stráž na žádost a v rozsahu, v jakém je to nezbytné pro plnění jejich úkolů, přístup do centrálního úložiště přes zabezpečený přístup prostřednictvím komunikační infrastruktury. Agentura eu-LISA provádí kontroly přístupu a zavede specifické uživatelské profily k zajištění toho, aby se přístup k centrálnímu úložišti omezil pouze na zprávy a statistiky.

8. Dva roky ode dne použitelnosti tohoto nařízení podle čl. 79 odst. 5 prvního pododstavce a poté každé dva roky předloží agentura eu-LISA Evropskému parlamentu a Radě zprávu o technickém fungování centrálního SIS a komunikační infrastruktury, včetně jejich zabezpečení, o systému automatizované identifikace otisků prstů (AFIS) a dvoustranné a mnohostranné výměně doplňujících informací mezi členskými státy. Tato zpráva rovněž obsahuje hodnocení využití zobrazení obličeje k identifikaci osob, jakmile se tato technologie začne používat.

9. Tři roky ode dne použitelnosti tohoto nařízení podle čl. 79 odst. 5 prvního pododstavce a poté každé čtyři roky 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 toho, zda přetrvávají důvody pro existenci systému, použití tohoto nařízení ve vztahu k centrálnímu SIS, zabezpečení centrálního SIS, jakož i všechny dopady jeho budoucího provozování. Tato hodnotící zpráva zahrnuje rovněž posouzení systému automatizované identifikace otisků prstů (AFIS) a informačních kampaní o SIS organizovaných Komisí v souladu s článkem 19.

Komise předá hodnotící zprávu Evropskému parlamentu a Radě.

10. Komise přijme prováděcí akty, jimiž stanoví podrobná pravidla týkající se fungování centrálního úložiště uvedeného v odstavci 7 tohoto článku a pravidla pro ochranu údajů a zabezpečení vztahující se na toto úložiště. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 76 odst. 2.

Článek 75

Výkon přenesené pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedené v čl. 38 odst. 3 a v čl. 43 odst. 4 je svěřena Komisi na dobu neurčitou od … [den vstupu tohoto nařízení v platnost].

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 38 odst. 3 a čl. 43 odst. 4 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm určené. Rozhodnutí nabývá platnosti prvním dnem po zveřejnění v *Úředním věstníku Evropské unie*, nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Před přijetím aktu v přenesené pravomoci vede Komise konzultace s odborníky jmenovanými jednotlivými členskými státy v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů.

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

6. Akt v přenesené pravomoci přijatý podle čl. 38 odst. 3 nebo čl. 43 odst. 4 vstoupí v platnost pouze tehdy, pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

Článek 76

Postup projednávání ve výboru

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

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

Článek 77

Změny rozhodnutí 2007/533/SVV

Rozhodnutí 2007/533/SVV se mění takto:

1) Článek 6 se nahrazuje tímto:

„*Článek 6*

Vnitrostátní systémy

1. Každý členský stát je odpovědný za zřízení, provoz, údržbu a další rozvoj svého N.SIS II a jeho připojení k NI-SIS.

2. Každý členský stát je odpovědný za zajištění nepřetržité dostupnosti údajů SIS II pro koncové uživatele.“.

2) Článek 11 se nahrazuje tímto:

„*Článek 11*
Důvěrnost – členské státy

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

2. Pokud členský stát při provádění jakéhokoliv úkolu souvisejícího se systémem SIS II spolupracuje s externími dodavateli, pečlivě kontroluje činnosti dodavatele, aby bylo zajištěno dodržování všech ustanovení tohoto rozhodnutí, zejména pokud jde o bezpečnost, důvěrnost a ochranu údajů.

3. Provozní řízení N.SIS II nebo jakýchkoliv technických kopií nesmí být svěřeno soukromým společnostem nebo soukromým organizacím.“.

3) Článek 15 se mění takto:

a) vkládá se nový odstavec, který zní:

„3a. Řídící orgán vytvoří a spravuje mechanismus a postupy pro provádění kontrol kvality údajů v CS-SIS. Pravidelně o tom předkládá zprávy členským státům.

Řídící orgán pravidelně předkládá Komisi zprávu o zjištěných problémech a o tom, kterých členských států se týkají.

Komise pravidelně předkládá Evropskému parlamentu a Radě zprávu o problémech, které se vyskytly ohledně kvality údajů.“;

b) odstavec 8 se nahrazuje tímto:

„8. Provozní řízení centrálního SIS II sestává ze všech úkolů nezbytných pro zachování funkčnosti centrálního SIS II 24 hodin denně sedm dní v týdnu v souladu s tímto rozhodnutím, zejména z údržby a technického rozvoje nezbytných pro plynulý chod systému. Mezi tyto úkoly patří také koordinace, řízení a podpora činností testování centrálního SIS II a N.SIS II, která zajišťuje, aby centrální SIS II a N.SIS II fungovaly v souladu s požadavky na technický soulad stanovenými v článku 9.“.

4) V článku 17 se doplňují nové odstavce, které znějí:

„3. Pokud řídící orgán při provádění jakéhokoliv úkolu souvisejícího se systémem SIS II spolupracuje s externími dodavateli, pečlivě kontroluje činnost dodavatele, aby bylo zajištěno dodržování všech ustanovení tohoto rozhodnutí, zejména ustanovení o bezpečnosti, důvěrnosti a ochraně údajů.

4. Provozní řízení CS-SIS nesmí být svěřeno soukromým společnostem nebo soukromým organizacím.“

5) V článku 21 se doplňuje nový pododstavec, který zní:

„Pokud je osoba nebo věc hledána na základě záznamu, který souvisí s teroristickým trestným činem, je tento případ považován za dostatečně přiměřený, relevantní a závažný pro to, aby odůvodňoval vložení záznamu do SIS II. Z důvodů veřejné nebo národní bezpečnosti mohou ve výjimečných případech členské státy od vložení záznamu upustit, pokud je pravděpodobné, že bude bránit úředním nebo právním šetřením, vyšetřováním nebo postupům.“.

6) Článek 22 se nahrazuje tímto:

„*Článek 22*
Zvláštní pravidla pro vkládání, ověřování nebo vyhledávání fotografií a otisků prstů

1. Fotografie a otisky prstů se vloží pouze po provedení zvláštní kontroly kvality s cílem ověřit, že splňují minimální normy kvality údajů. Specifikace této zvláštní kontroly kvality se stanoví postupem podle článku 67.

2. Pokud jsou fotografie a údaje o otiscích prstů dostupné v záznamu v SIS II, použijí se tyto fotografie a údaje o otiscích prstů k potvrzení totožnosti osoby, která byla nalezena na základě alfanumerického vyhledávání v SIS II.

3. V údajích o otiscích prstů lze za účelem identifikace osoby vyhledávat ve všech případech. Nelze-li však osobu identifikovat jinými prostředky, musí být za účelem její identifikace provedeno vyhledávání v údajích o otiscích prstů. Za tímto účelem obsahuje centrální SIS II systém automatizované identifikace otisků prstů (AFIS).

4. Údaje o otiscích prstů v SIS II v souvislosti se záznamy vloženými podle článků 26, 32 a 36 lze vyhledávat též s použitím úplných či neúplných souborů otisků prstů zajištěných na místě spáchání vyšetřovaných závažných trestných činů nebo teroristických trestných činů, u nichž lze s vysokou mírou pravděpodobnosti stanovit, že patří pachateli daného trestného činu, a to za předpokladu, že jsou současně vyhledávány i v příslušných vnitrostátních databázích otisků prstů.“.

7) Článek 41 se nahrazuje tímto:

„*Článek 41*
Přístup Europolu k údajům v SIS II

1. Je-li to pro výkon jejích pravomocí nezbytné, má Agentura Evropské unie pro spolupráci v oblasti prosazování práva (Europol), zřízená nařízením Evropského parlamentu a Rady (EU) 2016/794*, právo přístupu k údajům v SIS II a právo v těchto údajích vyhledávat. Europol může rovněž provádět výměnu doplňujících informací a požadovat další doplňující informace v souladu s ustanoveními příručky SIRENE.

2. Pokud vyhledávání provedené Europolem odhalí existenci záznamu v SIS II, informuje o tom Europol vkládající členský stát formou výměny doplňujících informací prostřednictvím komunikační infrastruktury a v souladu s ustanoveními příručky SIRENE. Do doby, než bude Europol moci využívat funkcí pro výměnu doplňujících informací, informuje vkládající členské státy způsobem vymezeným v nařízení (EU) 2016/794.

3. Europol může zpracovávat doplňující informace, které mu byly poskytnuty členskými státy, pro účely jejich srovnání s vlastními databázemi a projekty operativní analýzy s cílem nalézt souvislosti nebo jiné důležité spojitosti a pro účely strategických, tematických nebo operativních analýz uvedených v čl. 18 odst. 2 písm. a), b) a c) nařízení (EU) 2016/794. Veškeré zpracování doplňujících informací Europolem pro účely uvedené v tomto článku se provádí v souladu s uvedeným nařízením.

4. Použití informací získaných vyhledáváním v SIS II nebo ze zpracování doplňujících informací Europolem podléhá souhlasu vkládajícího členského státu. Pokud členský stát povolí použití takové informace, nakládá s ní Europol v souladu s nařízením (EU) 2016/794. Europol může takovou informaci sdělit třetím zemím a třetím subjektům pouze se souhlasem vkládajícího členského státu a při plném dodržování práva Unie v oblasti ochrany údajů.

5. Europol:

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

b) vymaže, bez ohledu na čl. 31 odst. 1 nařízení (EU) 2016/794, doplňující informace obsahující osobní údaje nejpozději jeden rok od výmazu souvisejícího záznamu. Odchylně může Europol, pokud má informace ve svých databázích nebo projektech operativní analýzy o případu, jehož se doplňující informace týkají za účelem plnění svých úkolů, výjimečně i nadále uchovávat doplňující informace, je-li to nezbytné. Europol informuje vkládající členský stát a vykonávající členský stát o dalším uchovávání těchto doplňujících informací a toto uchovávání zdůvodní;

c) omezí přístup k údajům v SIS II, včetně doplňujících informací, na konkrétně oprávněné pracovníky Europolu, pro něž je přístup k těmto údajům nezbytný k plnění jejich úkolů;

d) přijme a uplatňuje opatření pro zajištění bezpečnosti, důvěrnosti a vlastní kontroly v souladu s články 10, 11 a 13;

e) zajistí, aby jeho pracovníci oprávnění zpracovávat údaje SIS II absolvovali odpovídající odbornou přípravu a obdrželi informace v souladu s článkem 14; a

f) umožní evropskému inspektorovi ochrany údajů, aniž je dotčeno nařízení (EU) 2016/794, aby sledoval a přezkoumával činnost Europolu při výkonu svého práva přístupu k údajům v SIS II a na vyhledávání v těchto údajích, jakož i výměnu a zpracování doplňujících informací.

6. Europol může pořizovat kopie údajů ze SIS II pouze pro technické účely, pokud jsou potřebné k tomu, aby řádně zmocnění pracovníci Europolu mohli provádět přímé vyhledávání. Na tyto kopie se použije toto rozhodnutí. Technická kopie se použije pouze pro účely uchovávání údajů SIS II v průběhu vyhledávání údajů. Po dokončení vyhledávání se údaje vymažou. Tato použití nejsou považována za protiprávní stahování ani kopírování údajů ze SIS II. Europol nesmí kopírovat údaje ze záznamů ani další údaje vložené členskými státy nebo získané z CS-SIS II do jiných systémů Europolu.

7. Za účelem ověření zákonnosti zpracování údajů, pro vlastní kontrolu a pro zajištění řádného zabezpečení údajů a jejich neporušenosti vede Europol v souladu s ustanovením článku 12 protokoly o každém přístupu do SIS II a vyhledávání v tomto systému. Tyto protokoly a dokumentace nejsou považovány za protiprávní stahování ani kopírování jakékoli části SIS II.

8. Členské státy sdělí Europolu prostřednictvím výměny doplňujících informací jakýkoli pozitivní nález záznamů týkajících se teroristických trestných činů. Členské státy nemusí ve výjimečných případech informovat Europol, pokud by to ohrozilo probíhající vyšetřování, bezpečnost fyzické osoby, nebo bylo v rozporu s podstatnými zájmy bezpečnosti vkládajícího členského státu.

9. Odstavec 8 se použije ode dne, kdy bude Europol schopen získat doplňující informace podle odstavce 1.

---

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

8) Vkládá se nový článek, který zní:

„*Článek 42a*

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

1. V souladu s čl. 40 odst. 8 nařízení Evropského parlamentu a Rady (EU) 2016/1624* mají příslušníci jednotek a členové týmů ve smyslu čl. 2 bodů 8 a 9 uvedeného nařízení v rámci svých pravomocí a za předpokladu, že jsou oprávněni provádět kontroly v souladu s čl. 40 odst. 1 tohoto rozhodnutí a že absolvovali odpovídající odbornou přípravu v souladu s článkem 14 tohoto rozhodnutí, právo přístupu k údajům v SIS II a právo v těchto údajích vyhledávat v rozsahu, v jakém je to nezbytné pro plnění jejich úkolů a v jakém je vyžaduje operační plán pro konkrétní operaci. Přístup k údajům v SIS II nelze rozšířit na žádné jiné příslušníky jednotek a členy týmu.

2. Příslušníci jednotek a členové týmů uvedení v odstavci 1 vykonávají toto právo přístupu k údajům v SIS II a právo v těchto údajích vyhledávat podle odstavce 1 prostřednictvím technického rozhraní. Toto technické rozhraní vytvoří a spravuje Evropská agentura pro pohraniční a pobřežní stráž a umožňuje přímé propojení s centrálním SIS II.

3. Pokud vyhledávání provedené příslušníky jednotek nebo členy týmů uvedenými v odstavci 1 tohoto článku odhalí existenci záznamu v SIS II, musí být o tom informován vkládající členský stát. V souladu s článkem 40 nařízení (EU) 2016/1624 mohou příslušníci jednotek a členové týmů jednat v reakci na záznam v SIS II pouze pod velením a zpravidla za přítomnosti příslušníků pohraniční stráže hostitelského členského státu, v němž působí, nebo pracovníků tohoto státu, kteří se podílejí na úkolech spojených s navracením. Hostitelský členský stát může příslušníky jednotek a členy týmů zmocnit k tomu, aby jednali jeho jménem.

4. Za účelem ověření zákonnosti zpracování údajů, pro vlastní kontrolu a pro zajištění řádného zabezpečení údajů a jejich neporušenosti vede Evropská agentura pro pohraniční a pobřežní stráž v souladu s ustanoveními článku 12 protokoly o každém přístupu do SIS II a vyhledávání v tomto systému.

5. Evropská agentura pro pohraniční a pobřežní stráž přijme a uplatňuje opatření pro zajištění bezpečnosti, důvěrnosti a vlastní kontroly v souladu s články 10, 11 a 13 a zajistí, aby jednotky a týmy uvedené v odstavci 1 tohoto článku tato opatření uplatňovaly.

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

7. Aniž je dotčen odstavec 2, žádné části SIS II se nepropojí s jakýmkoli systémem pro sběr a zpracování údajů provozovaným týmy uvedenými v odstavci 1 nebo Evropskou agenturou pro pohraniční a pobřežní stráž ani se do takového systému nepřenesou údaje v SIS II, k nimž mají tyto jednotky a týmy přístup. Žádná část SIS II se nesmí stahovat ani kopírovat. Protokolování přístupu ani vyhledávání nejsou považovány za protiprávní stahování nebo kopírování údajů ze SIS II.

8. Evropská agentura pro pohraniční a pobřežní stráž umožní evropskému inspektorovi ochrany údajů sledovat a přezkoumávat činnosti jednotek a týmů uvedených v tomto článku při výkonu jejich práva přístupu k údajům v SIS II a na vyhledávání v těchto údajích. Tím nejsou dotčena další ustanovení nařízení Evropského parlamentu a Rady (EU) 2018/...**[+].

---

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

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

[+] Pro Úř. věst.: vložte prosím v textu číslo nařízení obsaženého v dokumentu PE-CONS 31/18 a v poznámce pod čarou jeho číslo, datum přijetí a odkaz na vyhlášení v Úředním věstníku.

Článek 78

Zrušení

Nařízení (ES) č. 1986/2006 a rozhodnutí 2007/533/SVV a 2010/261/EU se zrušují s účinkem ode dne použitelnosti tohoto nařízení, jak je stanoveno v čl. 79 odst. 5 prvním pododstavci.

Odkazy na zrušené nařízení (ES) č. 1986/2006 a rozhodnutí 2007/533/SVV se považují za odkazy na toto nařízení v souladu se srovnávací tabulkou obsaženou v příloze.

Článek 79

Vstup v platnost, zahájení provozu a použitelnost

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

2. Nejpozději do… [tři roky ode dne vstupu tohoto nařízení v platnost] přijme Komise rozhodnutí, kterým se stanoví datum zahájení provozu SIS podle tohoto nařízení, a to po ověření, že byly splněny tyto podmínky:

   a) byly přijaty prováděcí akty nezbytné pro používání tohoto nařízení;

   b) členské státy oznámily Komisi, že přijaly nezbytná technická a právní opatření pro zpracovávání údajů SIS a výměnu doplňujících informací podle tohoto nařízení; a

c) agentura eu-LISA oznámila Komisi úspěšné ukončení veškerých činností testování v souvislosti s CS-SIS a s interakcí mezi CS-SIS a N.SIS.

3. Komise pečlivě sleduje proces postupného plnění podmínek stanovených v odstavci 2 a informuje Evropský parlament a Radu o výsledku ověřování podle uvedeného odstavce.

4. Do dne … [jeden rok ode dne vstupu tohoto nařízení v platnost] a poté každý rok až do přijetí rozhodnutí Komise uvedeného v odstavci 2 předkládá Komise Evropskému parlamentu a Radě zprávu o aktuálním stavu příprav provedení tohoto nařízení v plném rozsahu. Tato zpráva obsahuje rovněž podrobné informace o vzniklých nákladech a informace o jakémkoli riziku, které může mít dopad na celkové náklady.

5. Toto nařízení se použije ode dne stanoveného v souladu s odstavcem 2.

Odchylně od prvního pododstavce se:

a) čl. 4 odst. 4, článek 5, čl. 8 odst. 4, čl. 9 odst. 1 a 5, čl. 12 odst. 8, čl. 15. odst. 7, článek 19, čl. 20 odst. 4 a 5, čl. 26 odst. 6, čl. 32 odst. 9, čl. 34 odst. 3, čl. 36. odst. 6, čl. 38 odst. 3 a 4, čl. 42 odst. 5, čl. 43 odst. 4, čl. 54 odst. 5, čl. 62 odst. 4, čl. 63 odst. 6, čl. 74 odst. 7 a 10, články 75 a 76, čl. 77 body 1 až 5 a odstavce 3 a 4 tohoto článku použijí ode dne vstupu tohoto nařízení v platnost;

b) čl. 77 body 7 a 8 použijí ode dne … [jeden rok ode dne vstupu tohoto nařízení v platnost];

c) čl. 77 bod 6 použije ode dne … [dva roky ode dne vstupu tohoto nařízení v platnost].

6. Rozhodnutí Komise uvedené v odstavci 2 se zveřejní v *Úředním věstníku Evropské unie*.

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

V Bruselu dne

Za Evropský parlament
předseda

Za Radu
předseda nebo *předsedkyně*

PŘÍLOHA

Srovnávací tabulka

Rozhodnutí 2007/533/SVV	Toto nařízení
Článek 1	Článek 1
Článek 2	Článek 2
Článek 3	Článek 3
Článek 4	Článek 4
Článek 5	Článek 5
Článek 6	Článek 6
Článek 7	Článek 7
Článek 8	Článek 8
Článek 9	Článek 9
Článek 10	Článek 10
Článek 11	Článek 11
Článek 12	Článek 12
Článek 13	Článek 13
Článek 14	Článek 14
Článek 15	Článek 15
Článek 16	Článek 16
Článek 17	Článek 17
Článek 18	Článek 18
Článek 19	Článek 19
Článek 20	Článek 20
Článek 21	Článek 21
Článek 22	Články 42 a 43

Rozhodnutí 2007/533/SVV	Toto nařízení
Článek 23	Článek 22
–	Článek 23
Článek 24	Článek 24
Článek 25	Článek 25
Článek 26	Článek 26
Článek 27	Článek 27
Článek 28	Článek 28
Článek 29	Článek 29
Článek 30	Článek 30
Článek 31	Článek 31
Článek 32	Článek 32
Článek 33	Článek 33
Článek 34	Článek 34
Článek 35	Článek 35
Článek 36	Článek 36
Článek 37	Článek 37
Článek 38	Článek 38
Článek 39	Článek 39
–	Článek 40
–	Článek 41
Článek 40	Článek 44
–	Článek 45
–	Článek 46
–	Článek 47

Rozhodnutí 2007/533/SVV	Toto nařízení
Článek 41	Článek 48
Článek 42	Článek 49
–	Článek 51
Článek 42a	Článek 50
Článek 43	Článek 52
Článek 44	Článek 53
Článek 45	Článek 54
–	Článek 55
Článek 46	Článek 56
Článek 47	Článek 57
Článek 48	Článek 58
Článek 49	Článek 59
–	Článek 60
Článek 50	Článek 61
Článek 51	Článek 62
Článek 52	Článek 63
Článek 53	Článek 64
Článek 54	Článek 65
Článek 55	–
Článek 56	–
Článek 57	Článek 66
Článek 58	Článek 67
Článek 59	Článek 68
Článek 60	Článek 69

Rozhodnutí 2007/533/SVV	Toto nařízení
Článek 61	Článek 70
Článek 62	Článek 71
Článek 63	–
Článek 64	Článek 72
Článek 65	Článek 73
Článek 66	Článek 74
–	Článek 75
Článek 67	Článek 76
Článek 68	–
–	Článek 77
Článek 69	–
–	Článek 78
Článek 70	–
Článek 71	Článek 79

Nařízení (ES) č. 1986/2006	Toto nařízení
Články 1, 2 a 3	Článek 45