EVROPSKÁ
KOMISE

V Bruselu dne 6.4.2016
COM(2016) 205 final

# SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

## Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost

## 1. ÚVOD

Evropa je mobilní společnost. Každý den překračují vnitřní a vnější hranice miliony občanů EU a státních příslušníků třetích zemí. V roce 2015 navštívilo EU více než 50 milionů státních příslušníků třetích zemí, což představuje více než 200 milionů překročení vnějších hranic schengenského prostoru.

Mimo tyto pravidelné cestovní toky jen v roce 2015 způsobil konflikt v Sýrii a krize na jiných místech 1,8 milionu nedovolených překročení vnějších hranic Evropy. Občané EU očekávají, že kontroly osob na vnější hranici budou účinné, že umožní účinné řízení migrace a budou mít přínos pro vnitřní bezpečnost. Teroristické útoky v Paříži v roce 2015 a v Bruselu v březnu 2016 byly hořkým projevem aktuální hrozby pro vnitřní bezpečnost Evropy.

Obě skutečnosti ještě více upozornily na potřebu spojit se a komplexně posílit rámce spolupráce a informační nástroje v oblasti správy hranic EU, migrace a bezpečnosti. Správa hranic, prosazování práva a řízení migrace jsou dynamicky provázány. Ví se o tom, že občané EU překračují vnější hranici na cestě do zón konfliktu za teroristickými účely a po svém návratu představují riziko. Existují důkazy, že teroristé využili ke vstupu do EU cest nelegální migrace a poté se v schengenském prostoru pohybují bez odhalení.

Evropské programy pro bezpečnost a migraci vytyčily směr pro vývoj a provádění politiky EU, jejímž úkolem je řešit souběžné problémy, jimiž je řízení migrace a boj proti terorismu a organizované trestné činnosti. Toto sdělení staví na synergiích mezi těmito dvěma programy a má být výchozím bodem pro diskusi o tom, jak by stávající a budoucí informační systémy mohly posílit správu vnějších hranic a vnitřní bezpečnost v EU. Doplňuje návrh z prosince 2015 týkající se vytvoření evropské pohraniční a pobřežní stráže a zlepšení prevence krizí a zásahů na vnějších hranicích.

Na úrovni EU funguje řada informačních systémů, které pohraniční stráži a policistům poskytují relevantní informace o osobách, ale architektura správy údajů v EU není dokonalá. Toto sdělení formuluje několik potenciálních možností pro maximalizaci přínosů stávajících informačních systémů a v případě potřeby vytvoření nových a doplňujících opatření pro řešení nedostatků. Jako dlouhodobý cíl podtrhuje též potřebu zlepšit interoperabilitu informačních systémů, což uznala i Evropská rada a Rada[1], a představuje nápady, jak by informační systémy mohly být rozvíjeny v budoucnosti, aby bylo zajištěno, že pohraniční stráž, celní orgány, policisté a soudní orgány budou mít k dispozici potřebné informace.

Jakákoli budoucí iniciativa by byla připravena na základě zásad zlepšování právní úpravy s veřejnou konzultací a hodnocením dopadů, a to i s ohledem na základní práva, a zejména právo na ochranu osobních údajů.

## 2. PROBLÉMY, KTERÉ JE NUTNÉ ŘEŠIT

Neexistence vnitřních hranic v schengenském prostoru vyžaduje silné a spolehlivé řízení pohybu osob přes vnější hranice. To je předpokladem pro zajištění vysoké úrovně vnitřní

[1] Závěry ze zasedání Evropské rady ze 17. a 18. prosince 2015, společné prohlášení ministrů spravedlnosti a vnitra členských států EU a zástupců orgánů EU k teroristickým útokům, k nimž došlo v Bruselu dne 22. března 2016 (24. března 2016); závěry Rady EU a členských států zasedajících v Radě o boji proti terorismu (20. listopadu 2015).

bezpečnosti a volného pohybu osob v tomto prostoru. Neexistence vnitřních hranic současně znamená, že donucovací orgány v členských státech mají i přístup k příslušným údajům o osobách. Na úrovni EU existuje řada informačních systémů a databází, které v souladu se svými účely poskytují relevantní informace o osobách pohraniční stráži, policistům a jiným orgánům[2].

Práci těchto vnitrostátních orgánů však brzdí nedostatky informačních systémů. Jako zásadní priorita byla tudíž v Evropském programu pro bezpečnost zdůrazněna lepší výměna informací. Hlavními nedostatky jsou: a) neoptimální fungování stávajících informačních systémů, b) mezery v architektuře správy údajů v EU, c) složité prostředí různě řízených informačních systémů a d) roztříštěná architektura správy údajů pro ochranu hranic a bezpečnost.

Stávající informační systémy v EU pro správu hranic a vnitřní bezpečnost mají širokou škálu funkcí. Nicméně, **stávající systémy stále nefungují dostatečně**. Při pohledu na procesy ochrany hranic v souvislosti s různými kategoriemi cestujících je zjevné, že v některých z těchto procesů a mezi příslušnými informačními systémy, které se používají k ochraně hranic, jsou nedostatky. Podobně je zapotřebí optimalizovat výkon stávajících nástrojů k prosazování práva. Proto je třeba zvážit opatření na zlepšení stávajících informačních systémů (oddíl 5).

Navíc existují **mezery v architektuře správy údajů v EU**. Zůstávají problémy týkající se ochrany hranic v souvislosti s konkrétními kategoriemi cestujících, jako jsou státní příslušníci třetích zemí, kteří mají dlouhodobé vízum. Existují též mezery v informacích před příjezdem k hranici, pokud jde o státní příslušníky třetích zemí, na které se vízová povinnost nevztahuje. Zvážit by se měla i otázka, zda je nutné řešit tyto mezery případným vývojem dalšího informačního systému (oddíl 6).

Pohraniční stráž a především policisté čelí **složitému prostředí různě řízených informačních systémů** na úrovni EU. Tato složitost vyvolává problémy v praxi týkající se zejména toho, ve kterých databázích by se v dané situaci mělo vyhledávat. Kromě toho ne všechny členské státy jsou připojeny ke všem stávajícím systémům[3]. Současnou složitost přístupu k informačním systémům na úrovni EU by mohlo snížit jednotné vyhledávací rozhraní na vnitrostátní úrovni, které by respektovalo různé účely přístupu (oddíl 7.1).

Současnou architekturu správy údajů v EU pro ochranu hranic a bezpečnost charakterizuje **roztříštěnost**. Tu způsobují různé institucionální, právní a politické souvislosti, v nichž byly systémy vyvinuty. Informace jsou uchovávány odděleně v různých systémech, které jsou zřídkakdy propojeny. Existuje nejednotnost mezi databázemi a odchylný přístup k údajům pro příslušné orgány. To může vést k nevyjasněným otázkám zejména pro donucovací orgány, jelikož rozpoznat spojení mezi fragmenty údajů může být velmi složité. Je tudíž nezbytné a naléhavé usilovat o ucelená řešení lepší přístupnosti údajů pro správu a bezpečnost hranic, a to plně v souladu se základními právy. Z tohoto důvodu je zapotřebí zahájit proces směřující k interoperabilitě stávajících informačních systémů (oddíl 7).

---

[2] Viz oddíl 4 s přehledem informačních systémů pro hranice a bezpečnost a příloha 2 s podrobnějším seznamem.

[3] S výhradou specifických podmínek protokolu 22, pokud jde o Dánsko, a protokolů 21 a 36, pokud jde o Spojené království a Irsko, a příslušných aktů o přistoupení.

## 3. ZÁKLADNÍ PRÁVA

Základním předpokladem řešení kterýchkoli z výše uvedených problémů je naprosté dodržování základních práv a pravidel ochrany údajů.

Dodržování základních práv vyžaduje kvalitně navržené a správně využívané technologické a informační systémy. Ty mohou orgánům veřejné moci pomáhat při ochraně základních práv občanů. Biometrické technologie mohou snížit riziko nesprávné totožnosti, diskriminace a profilování na základě rasového původu. Pokud jdou ruku v ruce se zárukami základních práv a ochrannými opatřeními, přispívají též k řešení rizik ochrany dětí, například dětí, které se ztratí nebo se stanou oběťmi obchodování s lidmi. Mohou snížit riziko, že lidé budou omylem zadrženi a zatčeni. Mohou též přispět ke zvýšení bezpečnosti občanů žijících v schengenském prostoru, jelikož pomohou v boji proti terorismu a závažné trestné činnosti.

Existence rozsáhlých informačních systémů znamená též případná rizika pro soukromí, která je nutné předvídat a náležitě řešit. Sběr a používání osobních údajů v těchto systémech má dopad na právo na soukromí a ochranu osobních údajů, které je zakotveno v Listině základních práv Evropské unie. Všechny systémy musí dodržovat zásady ochrany údajů a požadavky nezbytnosti, přiměřenosti, účelového omezení a kvality údajů. Musí být zavedena ochranná opatření, aby byla zajištěna práva subjektů údajů v souvislosti s ochranou jejich soukromého života a osobních údajů. Údaje by měly být uchovávány pouze po nezbytnou dobu pro účel, pro který byly shromážděny. Je nutné stanovit mechanismy zajišťující přesné řízení rizik a účinnou ochranu práv subjektů údajů.

V prosinci 2015 dosáhli společní normotvůrci politické dohody o reformě ochrany údajů. Po přijetí se nové obecné nařízení o ochraně údajů a směrnice o ochraně údajů orgány činnými v trestním řízení[4] stanou použitelnými v roce 2018 a zajistí harmonizovaný rámec pro zpracování osobních údajů.

Klíčovou zásadou ochrany údajů zakotvenou v Listině základních práv je účelové omezení. Z důvodu různých institucionálních, právních a politických souvislostí, v nichž byly informační systémy na úrovni EU vyvinuty, byla zásada účelového omezení provedena prostřednictvím roztříštěné struktury správy informací[5]. To je jeden z důvodů současné roztříštěnosti architektury správy údajů v EU pro ochranu hranic a bezpečnost. Zásadu účelového omezení lze snadněji provádět na úrovni přístupu a používání uchovávaných údajů plně v souladu s Listinou základních práv a poslední judikaturou Evropského soudního dvora díky novému komplexnímu rámci ochrany osobních údajů v EU a významným změnám v technologiích a bezpečnosti informačních technologií. Nezbytné účelové omezení v ucelených řešeních pro správu údajů by měla zajistit ochranná opatření, jako je rozčlenění údajů v rámci jednoho systému a specifická pravidla přístupu a používání u každé kategorie údajů a uživatelů. To otevírá cestu k interoperabilitě informačních systémů doprovázené nezbytnými přísnými pravidly pro přístup a používání bez toho, aby bylo dotčeno stávající účelové omezení.

Současnými zásadami pravidel EU pro ochranu údajů je „ochrana údajů již od návrhu“ a „standardní nastavení ochrany údajů“. Při vývoji nových nástrojů, které se budou opírat o používání informačních technologií, se Komise bude snažit postupovat v souladu s tímto přístupem. To znamená začlenění ochrany osobních údajů do technologického základu

[4] Viz http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
[5] KOM(2010) 385 v konečném znění.

navrhovaného nástroje, omezení zpracování údajů na míru nezbytnou pro specifikovaný účel a udělování přístupu k údajům pouze těm subjektům, které „je potřebují znát“[6].

Při řešení současných mezer a nedostatků v architektuře správy údajů v EU pro ochranu a bezpečnost hranic se Komise bude řídit požadavky Listiny základních práv, a zejména nových nástrojů pro reformu ochrany údajů. Tím bude zajištěno, že další vývoj informačních systémů v těchto oblastech bude v souladu s nejvyššími standardy ochrany údajů a že budou dodržovat základní práva zaručená Listinou základních práv a budou k nim přispívat.

## 4. PŘEHLED INFORMAČNÍCH SYSTÉMŮ PRO HRANICE A BEZPEČNOST[7]

Každý stávající informační systém v EU pro správu hranic a vnitřní bezpečnost má své vlastní cíle, účely, právní základy[8], skupiny uživatelů a institucionální souvislosti. Společně poskytují složité schéma příslušných databází.

Třemi hlavními **centralizovanými informačními systémy**, které EU vyvinula, jsou i) Schengenský informační systém (SIS) s širokým spektrem záznamů o osobách a věcech, ii) Vízový informační systém (VIS) s údaji o krátkodobých vízech a iii) systém EURODAC s otisky prstů žadatelů o azyl a státních příslušníků třetích zemí, kteří vnější hranice překročili neoprávněně. Tyto tři systémy se vzájemně doplňují a – s výjimkou systému SIS – se v první řadě zaměřují na státní příslušníky třetích zemí. Systémy podporují i vnitrostátní orgány v boji pro trestné činnosti a terorismu[9]. To se týká zejména SIS jako nejvíce využívaného nástroje pro sdílení informací v současnosti. Výměna informací pro tyto systémy probíhá v zabezpečené vyhrazené komunikační infrastruktuře, která se nazývá sTESTA[10].

Kromě těchto stávajících systémů Komise navrhuje čtvrtý centralizovaný systém správy hranic, **systém vstupu/výstupu** (EES)[11], který by měl být zaveden do roku 2020 a opět se bude zaměřovat na státní příslušníky třetích zemí.

---

6 Pro komplexní popis „soukromí coby aspektu návrhu“ viz stanovisko evropského inspektora ochrany údajů k podpoře důvěry v informační společnost prostřednictvím posílení ochrany údajů a soukromí, evropský inspektor ochrany údajů, 18.3.2010.

7 Viz příloha 2 se seznamem stávajících informačních systémů pro správu hranic a prosazování práva.

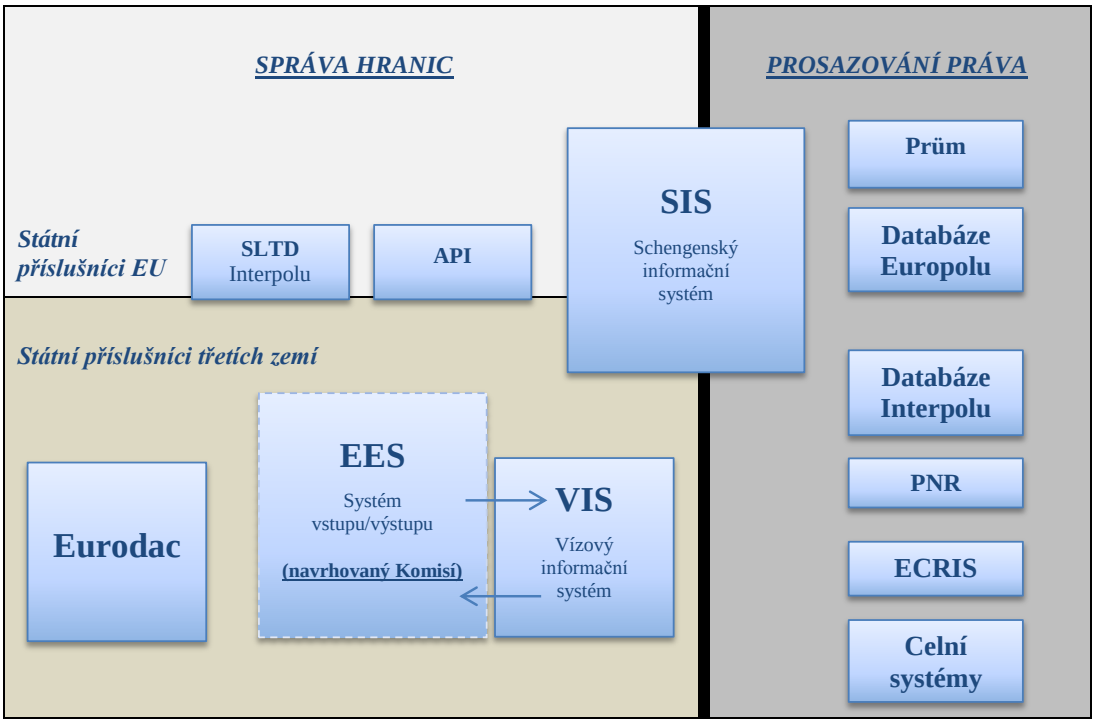
8 S výhradou specifických podmínek protokolu 22, pokud jde o Dánsko, a protokolů 21 a 36, pokud jde o Spojené království a Irsko.

9 Vzhledem ke skutečnosti, že prosazování práva je vedlejším cílem systémů VIS a EURODAC, lze přístup donucovacích orgánů do těchto systémů uplatňovat za omezených podmínek. Pokud jde o VIS, musí členské státy určit orgán, který bude odpovídat za kontrolu přístupu donucovacích orgánů, a policie musí doložit, že její přístup je nutný z důvodu vyšetřování trestné činnosti. Pokud jde o EURODAC, musí vyšetřovací orgán nejprve vyhledávat ve vnitrostátním systému AFIS, Prüm a VIS a teprve poté dostane přístup do systému EURODAC.

10 Brzy by měla být nahrazena infrastrukturou TESTA-NG.

11 COM(2016) 194 final.

***Obrázek 1*** *Schematický přehled hlavních informačních systémů pro správu hranic a prosazování práva:*




Dalšími stávajícími nástroji pro správu hranic jsou databáze Interpolu obsahující údaje o odcizených a ztracených cestovních dokladech (SLTD) a evidence předběžných informací o cestujících (API), která shromažďuje informace o cestujících přilétajících do EU. Tyto nástroje jsou relevantní pro občany EU i státní příslušníky třetích zemí.

Speciálně pro účely prosazování práva, vyšetřování trestné činnosti a soudní spolupráce vyvinula EU **decentralizované nástroje pro výměnu informací**, konkrétně i) prümský rámec pro výměnu DNA, otisků prstů a registračních údajů vozidel a ii) Evropský informační systém rejstříků trestů (ECRIS) pro výměnu informací z vnitrostátních rejstříků trestů. Systém ECRIS umožňuje prostřednictvím zabezpečené sítě výměnu informací o předchozích odsouzeních konkrétní osoby u trestních soudů v Evropské unii. Žádosti se opírají zejména o alfanumerické informace o totožnosti, je ale možná i výměna biometrických dat.

Výměnu informací mezi vnitrostátními policejními orgány podporuje jako centrála EU pro informace o trestné činnosti **Europol**. Informační systém Europolu (EIS) poskytuje centralizovanou databázi informací o trestné činnosti, v níž členské státy uchovávají a z níž požadují údaje o závažné trestné činnosti a terorismu. Kontaktní místa Europolu zajišťují analytické pracovní soubory zaměřené na určité téma, které obsahují informace o probíhajících operacích v členských státech. Aplikace sítě pro bezpečnou výměnu informací (SIENA), vedená Europolem, umožňuje členským státům rychlou a bezpečnou výměnu informací uživatelsky přívětivým způsobem mezi sebou vzájemně, s Europolem nebo se třetími stranami, které s Europolem uzavřely smlouvu o spolupráci. SIENA se současně výrazně soustřeďuje na interoperabilitu s jinými systémy v Europolu, například pro účely přímé výměny údajů s kontaktními místy. Nabízí možnost dodávat do databází Europolu informace, které si členské státy vyměňují mezi sebou. SIENA by tudíž měla být pro členské státy kanálem první volby, pokud jde o sdílení informací z oblasti prosazování práva v celé EU.

Dalším souborem systémů zpracování osobních údajů, které budou vyvíjeny napříč členskými státy, je **jmenná evidence cestujících** (PNR)[12]. Tato evidence obsahuje informace o rezervacích, které jsou poskytovány v době rezervace a odbavení.

A konečně, důležitým aktérem ve spolupráci mnoha agentur na vnějších hranicích jsou i **celní orgány**. Mají různé systémy[13] a databáze, které obsahují údaje o pohybu zboží, identifikaci hospodářských subjektů a informace o rizicích, které lze použít k posílení vnitřní bezpečnosti. Tyto systémy mají též svou vlastní řízenou, vyhrazenou a bezpečnou infrastrukturu (společnou komunikační síť), která již prokázala svou životaschopnost. Měly by být dále zkoumány synergie a sbližování informačních systémů a jejich odpovídajících infrastruktur pro správu hranic EU a celní operace.

## 5. ZLEPŠOVÁNÍ STÁVAJÍCÍCH INFORMAČNÍCH SYSTÉMŮ

Stávající informační systémy v EU pro správu hranic a vnitřní bezpečnost pokrývají širokou škálu funkcí. Systémy však stále mají **nedostatky**, které je nutné řešit, aby byl optimalizován jejich výkon.

*Schengenský informační systém (SIS)*

Hraniční kontroly podle **Schengenského informačního systému** (SIS) se v současnosti provádějí na základě alfanumerického vyhledávání (tj. podle jména a data narození). Otisky prstů lze využívat pouze k ověření a potvrzení totožnosti osoby, která již byla identifikována na základě svého jména. Tato bezpečnostní mezera umožňuje osobám se záznamem používat falešné doklady, aby unikly přesné shodě v SIS.

Tato kritická slabá stránka bude vyřešena přidáním funkce vyhledávání otisků prstů do SIS prostřednictvím **systému automatizované identifikace otisků prstů (AFIS)**, jak předpokládá stávající právní rámec[14]. AFIS by měl začít fungovat do poloviny roku 2017[15]. Jakmile bude vyvinut, bude mít k němu přístup Europol, a bude tak doplňovat systémy Europolu pro vyšetřování trestné činnosti a boj proti terorismu, jakož i pro výměnu otisků prstů podle prümského rámce. Komise a agentura eu-LISA prověří potenciál pro takové širší využití budoucího systému AFIS.

Na základě probíhajícího hodnocení a technické studie zkoumá Komise v současnosti **možné další funkce systému SIS** s cílem předložit návrhy na revizi jeho právního základu. Ke zvažovaným aspektům patří:

- vytvoření záznamů v SIS o nelegálních migrantech, v souvislosti s nimiž bylo vydáno rozhodnuto o navrácení,
- používání zobrazení obličeje pro biometrickou identifikaci navíc k otiskům prstů,

---

[12] Viz oddíl 6.2.

[13] Mezi celní informační systémy patří všechny systémy vytvořené podle celního kodexu Společenství (nařízení č. 2913/92) a budoucího celního kodexu Unie (nařízení č. 952/2013), rozhodnutí o bezpapírovém prostředí pro celnictví a obchod (rozhodnutí 70/2008/ES) a celní informační systém, který byl zřízen podle úmluvy SID z roku 1995. Jejich cílem je pomáhat v boji proti trestné činnosti související s cly tím, že usnadňují spolupráci mezi evropskými celními orgány.

[14] Ustanovení čl. 22 písm. c) 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) a 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 381, 28.12.2006, s. 4 a Úř. věst. L 2015, 7.8.2007, s. 63).

[15] V březnu 2016 předložila Komise Evropskému parlamentu a Radě zprávu Dostupnost a připravenost technologie pro zjišťování totožnosti osob na základě otisků prstů v Schengenském informačním systému druhé generace (SIS II).

- automatizovaný přenos informací o pozitivním nálezu po kontrole,
- uložení informací o pozitivním nálezu záznamů pořízených pro účely skrytých a zvláštních kontrol v centrálním systému SIS,
- vytvoření nové kategorie záznamů o „hledané neznámé osobě“, o níž mohou ve vnitrostátních databázích existovat forenzní údaje (např. latentní otisk zanechaný na místě činu)[16].

Komise bude provádění projektů, které umožňují současné vyhledávání v SIS a databázích Interpolu – databázi odcizených a ztracených cestovních dokladů (SLTD) a databázi hledaných zločinců, odcizených vozidel nebo nedovolených zbraní (iARMS), které se vzájemně doplňují s informačními systémy EU, i nadále podporovat finančními prostředky EU[17].

*Databáze odcizených a ztracených cestovních dokladů (SLTD)*

Pro účinnou správu hranic je zásadní, aby cestovní doklady všech státních příslušníků třetích zemí a občanů EU byly ověřeny podle **databáze SLTD**. Donucovací orgány by měly tuto databázi využívat i při vyhledávání v rámci schengenského prostoru. Po teroristických útocích v Paříži dne 13. listopadu 2015 vyzvala Rada k elektronickému napojení na příslušné databáze Interpolu na všech vnějších hraničních přechodech a k automatickým kontrolám cestovních dokladů do března 2016[18]. Příslušná elektronická napojení by měly provést všechny členské státy a měly by zavést systémy umožňující automatickou aktualizaci údajů o odcizených a ztracených cestovních dokladech v databázi SLTD.

*Předběžné informace o cestujících (API)*

V souladu se stávajícími osvědčenými postupy by členské státy měly zvýšit i přidanou hodnotu **předběžných informací o cestujících** (API) tím, že zavedou automatické křížové kontroly těchto údajů podle SIS a databáze SLTD Interpolu. Komise posoudí nutnost revize právního základu pro zpracování údajů z evidence API s cílem zajistit širší provádění a zahrnout povinnost, podle níž by členské státy musely žádat a používat údaje z evidence API u všech příletů a odletů. To je relevantní zejména v souvislosti s prováděním budoucí směrnice o jmenné evidenci cestujících, neboť kombinované využívání údajů z evidence PNR a API ještě více zlepšuje účinnost údajů z PNR při boji proti terorismu a závažné trestné činnosti[19].

*Vízový informační systém (SIS)*

Komise rovněž provádí celkové hodnocení **Vízového informačního systému** (VIS), které má být ukončeno v roce 2016. Při hodnocení si všímá mimo jiné způsobu, jakým je VIS využíván při kontrolách na vnějších hranicích a na území členských států a jakým přispívá k boji proti podvodnému zneužití totožnosti a víz. Na základě toho bude pak Komise zkoumat možnosti, jak vylepšit funkce VIS, mimo jiné tím, že:

- zvýší kvalitu zobrazení obličeje, aby umožnila porovnání biometrických údajů,

---

[16] Vytvoření tohoto nového záznamu bude posouzeno s cílem dosáhnout vzájemného doplňování se a vyvarovat se překrývání se stávajícím prümským rámcem k vyhledávání otisků prstů v různých vnitrostátních databázích členských států EU.

[17] Nástroje pro vyhledávání informací, které vyvinul Interpol, například stacionární databáze sítě Interpolu (FIND) a mobilní databáze sítě Interpolu (MIND), mají usnadnit souběžné vyhledávání v systémech Interpolu a v SIS.

[18] Závěry Rady EU a členských států zasedajících v Radě o boji proti terorismu, 20. listopadu 2015.

[19] Viz oddíl 6.2 o navrhované směrnici o jmenné evidenci cestujících.

- bude biometrické údaje žadatelů o víza používat k vyhledávání v budoucím systému automatické identifikace otisků prstů, který bude vyvinut pro SIS,
- sníží věkový limit pro odebírání otisků prstů u dětí ve věku od šesti do dvanácti let a současně stanoví důkladné záruky základních práv a ochranná opatření[20],
- usnadní vyhledávání v databázi Interpolu SLTD v průběhu žádosti o udělení víza.

Pokud jde o možnosti podle stávajícího právního rámce pro přístup k údajům VIS pro **účely prosazování práva**, uplatňují členské státy tyto možnosti různě. V této souvislosti členské státy uvádějí praktické problémy v postupech k přístupu donucovacích orgánů k systému VIS. Podobně se stále velmi omezeně provádí přístup pro účely prosazování práva k systému EURODAC. Komise bude zkoumat, zda není nutné znovu zvážit právní rámec pro přístup donucovacích orgánů do systémů VIS a EURODAC.

*EURODAC*

Jak uvádí sdělení nazvané Zlepšit společný evropský azylový systém a zdokonalit zákonné možnosti[21], Komise předloží návrh reformy systému **EURODAC** s cílem ještě více vylepšit jeho funkce související s nelegální migrací a navracením. Tím bude vyřešena současná mezera týkající se schopnosti sledovat druhotný pohyb nelegálních migrantů mezi členskými státy. Kromě toho se bude návrh snažit o zvýšení účinnosti postupů pro navracení a zpětné přebírání tím, že budou poskytnuty prostředky k prokazování totožnosti nelegálních migrantů a vydávání jejich nových dokladů pro účely navrácení. V této souvislosti návrh zahrne i výměnu informací obsažených v systému EURODAC se třetími zeměmi s tím, že nebudou opomíjena nezbytná ochranná opatření pro ochranu údajů.

*Europol*

EU udělila **Europolu** přístup do hlavních centrálních databází, ale agentura této příležitosti ještě v plné míře nevyužila. Europol má právo na přístup k údajům vloženým do SIS o zatčeních, skrytých a zvláštních kontrolách a věcech hledaných za účelem zabavení a tyto údaje přímo vyhledávat. Doposud Europol provedl v SIS jen poměrně omezený počet vyhledávání. Přístup Europolu do VIS za účelem nahlížení je z hlediska práva možný od září 2013. Od července 2015 umožňuje přístup Europolu právní základ systému EURODAC. Agentura by měla urychlit probíhající práce na připojení k systémům VIS a EURODAC. Obecněji řečeno, Komise posoudí, zda je nutné umožnit další přístup k informačním systémům i jiným agenturám EU v oblasti vnitřních věcí, především budoucí evropské pohraniční a pobřežní stráži.

*Prümský rámec*

**Prümský rámec** v současnosti nevyužívá svého potenciálu. Je to způsobeno tím, že ne všechny členské státy provedly své právní závazky z hlediska začlenění této sítě do svých vlastních systémů. Členské státy získaly na toto provádění významnou finanční a technickou podporu a nyní by měly prümský rámec provádět v plné míře. Komise využívá pravomocí, které jí byly uděleny, k tomu, aby zajistila plné provedení právních závazků členských států, a v lednu 2016 zahájila s dotčenými členskými státy strukturovaný dialog (EU Pilot). Pokud by se reakce členských států ukázaly jako neuspokojivé, nebude Komise váhat se zahájením řízení o nesplnění povinnosti.

*Evropský informační systém rejstříků trestů (ECRIS)*

[20] Jak je v studii JRC „Fingerprint Recognition for children“ (Rozpoznávání otisků prstů u dětí) označeno za technicky proveditelné, EUR 26193 EN; ISBN 978-92-79-33390-3Children', 2013.

[21] COM(2016) 197 final.

Evropský informační systém rejstříků trestů **ECRIS** umožňuje výměnu informací o odsouzeních týkajících se státních příslušníků třetích zemí a osob bez státní příslušnosti, ale není zaveden žádný postup, který by zajistil účinnost této činnosti. V lednu 2016 Komise přijala právní návrh k řešení tohoto nedostatku[22]. V této souvislosti navrhla, aby vnitrostátní orgány mohly v zájmu bezpečnější identifikace vyhledávat státní příslušníky třetích zemí na základě otisků prstů. Evropský parlament a Rada by měly legislativní text přijmout v roce 2016.

*Horizontální otázky*

Všeobecné znepokojení v souvislosti s informačními systémy vyvolává **úroveň provádění** ze strany členských států. Výmluvným příkladem je nerovné provádění prümského rámce a chybějící elektronická napojení na databázi SLTD. Pro zvýšení úrovně provádění v souvislosti s informačními systémy bude Komise úzce sledovat výkon každého členského státu[23]. Při sledování si bude všímat nejen toho, zda členské státy plní své právní závazky v oblasti informačních systémů, ale též toho, jak využívají stávající systémy a zda se řídí osvědčenými postupy. Komise bude při sledování a podpoře úrovně provádění čerpat z různých zdrojů, včetně oznámení od členských států a návštěv realizovaných v rámci schengenského hodnotícího a monitorovacího mechanismu.

Další všeobecné znepokojení v souvislosti s informačními systémy vyvolává **kvalita vkládaných údajů**. Pokud členské státy nerespektují minimální kvalitativní požadavky, stává se spolehlivost a hodnota uložených údajů velmi omezenou a riziko neodpovídajících výsledků a nenalezených shod snižuje hodnotu samotných systémů. Za účelem zlepšení kvality vkládaných údajů vytvoří eu-LISA pro všechny systémy spadající do její pravomoci **centrální mechanismus pro sledování kvality údajů**.

Většina informačních systémů v oblasti ochrany hranic a bezpečnosti pracuje s identifikačními údaji pocházejícími z cestovních dokladů a dokladů totožnosti. Pro posílení hranic a bezpečnosti, vedle dobře fungujících systémů, musí být ověřování cestovních dokladů a dokladů totožnosti snadné a bezpečné. Za tímto účelem představí Komise opatření pro zlepšení elektronické **bezpečnosti dokladů** a správy identifikačních údajů a pro posílení boje proti falešným dokladům. Možným prostředkem pro to by mohly být interoperabilní úrovně bezpečné identifikace dosažitelné prostřednictvím nařízení eIDAS[24].

**<u>Opatření ke zlepšení stávajících informačních systémů</u>**

**Schengenský informační systém (SIS)**

- Do poloviny roku 2017 Komise a agentura eu-LISA vyvinou a zavedou do SIS funkci automatické identifikace otisků prstů (AFIS).
- Do konce roku 2016 Komise předloží návrhy na revizi právního základu SIS s cílem zlepšit jeho fungování.
- Členské státy maximalizují své využití systému SIS jak vkládáním veškerých příslušných informací, tak nahlížením do systému v případě potřeby.

[22] COM(2016) 7 final, 19.1.2016.

[23] S výhradou specifických podmínek protokolu 22, pokud jde o Dánsko, a protokolů 21 a 36, pokud jde o Spojené království a Irsko.

[24] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

**Databáze Interpolu týkající se odcizených a ztracených cestovních dokladů (SLTD)**

- Členské státy se na všech svých vnějších hraničních přechodech elektronicky napojí na nástroje Interpolu.
- Členské státy budou plnit svůj závazek vkládat údaje o odcizených a ztracených cestovních dokladech zároveň do SIS a databáze SLTD a tyto údaje v nich vyhledávat.

**Předběžné informace o cestujících (API)**

- Členské státy zautomatizují porovnávání údajů z evidence API s údaji v SIS a databázi (Interpolu) odcizených a ztracených cestovních dokladů (SLTD) v souladu se stávajícími osvědčenými postupy.
- Komise posoudí potřebu revidovat právní základ pro zpracování údajů z evidence API.

**Vízový informační systém (VIS)**

- Do konce roku 2016 Komise prozkoumá, jak by se dal systém VIS dále vylepšit.

**EURODAC**

- Komise předloží návrh revize právního základu systému EURODAC s cílem dále zlepšit jeho fungování, pokud jde o nelegální migraci a navracení.

**Europol**

- Europol bude plně využívat svých stávajících práv na přístup do systémů SIS, VIS a EURODAC pro účely nahlížení.
- Komise a Europol prozkoumají a podpoří synergie mezi informačním systémem Europolu (EIS) a dalšími systémy, zejména systémem SIS.
- Komise a agentura eu-LISA prozkoumají, zda systém automatické identifikace otisků prstů (AFIS), který má být vyvinut pro SIS, může doplnit systémy Europolu pro účely vyšetřování trestné činnosti a boje proti terorismu.

**Prümský rámec**

- Členské státy plně provedou a budou využívat prümský rámec.
- V případě potřeby Komise zahájí proti členským státům, které se k prümskému rámci ještě nepřipojily, řízení o nesplnění povinnosti.
- Komise a agentura eu-LISA prozkoumají, zda systém automatické identifikace otisků prstů (AFIS), který má být vyvinut pro SIS, může doplnit výměny otisků prstů prováděné na základě prümského rámce.

**Evropský informační systém rejstříků trestů (ECRIS)**

- Evropský parlament a Rada by měly v roce 2016 přijmout legislativní návrh, aby vnitrostátním orgánům umožnily vyhledávat státní příslušníky třetích zemí v systému ECRIS na základě otisků prstů.

**Horizontální otázky**

- Komise bude **sledovat a podporovat úroveň provádění** v souvislosti s informačními systémy.
- Agentura eu-LISA vytvoří pro všechny systémy spadající do její pravomoci **centrální mechanismus pro sledování kvality údajů**.
- Komise představí opatření pro zlepšení elektronické **bezpečnosti dokladů a správy identifikačních údajů** a pro posílení boje proti falešným dokladům.

- Komise prozkoumá synergie a sbližování informačních systémů a jejich odpovídajících infrastruktur pro správu hranic EU a **celní operace**.

## 6. VÝVOJ DALŠÍCH INFORMAČNÍCH SYSTÉMŮ A ŘEŠENÍ NEDOSTATKŮ

Ačkoli stávající informační systémy zahrnují velmi široké spektrum údajů, které jsou vyžadovány v rámci správy hranic a prosazování práva, existují i významné nedostatky. Některými z těchto nedostatků se Komise zabývala v legislativních návrzích, konkrétně v návrzích systému vstupu/výstupu a systému jmenné evidence cestujících EU (PNR). V případě dalších nedostatků, které byly odhaleny, je nutné pečlivě posoudit, zda jsou zapotřebí další nástroje EU.

### 1. Systém vstupu/výstupu

Souběžně s tímto sdělením předložila Komise revidované legislativní návrhy na zřízení systému vstupu/výstupu (EES). Po přijetí společnými normotvůrci bude na agentuře eu-LISA, aby systém ve spolupráci s členskými státy schengenského prostoru vyvinula a zavedla.

EES bude registrovat překročení hranic (vstup a výstup) u všech státních příslušníků třetích zemí, kteří navštíví schengenský prostor za účelem krátkodobého pobytu (maximálně 90 dnů v jakémkoli období o délce 180 dnů), cestujících s vízovou povinností i cestujících osvobozených od vízové povinnosti, nebo pobytu na základě nového cestovního víza (až na jeden rok). Cílem EES je a) zlepšit správu vnějších hranic, b) omezit nelegální migraci řešením jevu, kterým je překračování povolené délky pobytu, a c) přispívat k boji proti terorismu a závažné trestné činnosti, a tím napomáhat k zajišťování vysoké úrovně vnitřní bezpečnosti.

EES bude registrovat totožnost státních příslušníků třetích zemí (alfanumerické údaje, čtyři otisky prstů a zobrazení obličeje) společně s podrobnostmi z jejich cestovních dokladů a propojí je s elektronickými záznamy vstupu a výstupu. V současné praxi razítkování cestovních dokladů se nebude pokračovat. EES umožní účinnou správu povolených krátkodobých pobytů, zvýšenou automatizaci při ochraně hranic a vylepšené odhalování podvodného zneužití dokladů a totožnosti. Centrální registrace umožní v schengenském prostoru odhalovat osoby překračující povolenou délku pobytu a identifikovat osoby bez dokladů. Navrhovaný EES tudíž řeší důležitý nedostatek v prostředí stávajících informačních systémů.

### 2. Jmenná evidence cestujících

Údaje ze jmenné evidence cestujících (PNR) zahrnují informace o rezervacích s kontaktními údaji, podrobnosti o celé cestě a rezervaci, zvláštní poznámky, informace o sedadle a zavazadlech a způsob placení. Údaje z PNR jsou prospěšné a nezbytné pro identifikaci vysoce rizikových cestujících v souvislosti s bojem proti terorismu, obchodu s drogami, obchodování s lidmi, pohlavnímu vykořisťování dětí a dalším závažným trestným činům. Navrhovaná směrnice o PNR zajistí lepší spolupráci mezi vnitrostátními systémy a zmenší bezpečnostní mezery mezi členskými státy. Řeší tudíž důležitou mezeru v dostupnosti údajů, které jsou nezbytné pro boj proti závažné trestné činnosti a terorismu. **Směrnice o PNR by tudíž měla být bezodkladně přijata a provedena**.

Budoucí směrnice stanoví, že členské státy musí zavést složky pro informace o cestujících, které budou přijímat údaje PNR od přepravců. Součástí nebude vytvoření centrálního systému nebo databáze, ale přínosem bude určitý stupeň standardizace vnitrostátních technických řešení a postupů. Jak předpokládá navrhovaná směrnice, usnadní to výměnu údajů z PNR mezi složkami pro informace o cestujících. Za tímto

účelem bude Komise členské státy podporovat při analýze různých scénářů pro vzájemné propojení složek pro informace o cestujících a jejím cílem bude nabídnout standardizovaná řešení a postupy. Jakmile bude směrnice přijata, Komise urychlí práce na společných protokolech a podporovaných formátech dat pro přenos údajů PNR od leteckých přepravců do složek. Do tří měsíců od přijetí směrnice Komise vypracuje návrh prováděcího aktu.

### 3. Nedostatek informací před příjezdem státních příslušníků třetích zemí bez vízové povinnosti

Ačkoli je ve VIS registrována totožnost, kontaktní údaje a základní informace o držitelích víza, informace o osobách bez vízové povinnosti pocházejí pouze z jejich cestovního dokladu. V případě cestujících, kteří přilétají letadlem nebo připlouvají lodí, mohou být tyto informace doplněny před příjezdem o údaje z evidence API. Podle navrhované směrnice o PNR budou sbírány i jejich údaje z PNR, pokud do EU přiletí. V případě osob vstupujících do EU přes pozemní hranici nejsou před jejich příjezdem na vnější hranici EU k dispozici žádné informace.

Zatímco o držitelích víz mohou donucovací orgány získat informace ze systému VIS, pokud je to nutné pro boj proti závažné trestné činnosti a terorismu, o osobách bez vízové povinnosti žádné srovnatelné údaje k dispozici nejsou. Tyto chybějící informace jsou pro správu pozemních hranic EU obzvláště významné v situaci, kdy podstatné počty cestujících bez vízové povinnosti přijíždějí vozem, autobusem nebo vlakem. Vízovou povinnost nemá již několik sousedních zemí EU a pokračují dialogy o uvolnění vízového režimu mezi EU a dalšími sousedními zeměmi. To pravděpodobně v blízké budoucnosti povede ke značnému nárůstu cestujících bez vízové povinnosti.

Komise posoudí, zda je pro řešení této otázky nezbytný, proveditelný a přiměřený nový nástroj EU. Možností ke zvážení je **systém EU pro cestovní informace a povolení** (ETIAS), kam by cestující bez vízové povinnosti zaznamenávali relevantní informace týkající se jejich zamýšlené cesty. Automatické zpracování těchto informací by mohlo pomoci pohraniční stráži při posuzování návštěvníků ze třetích zemí, kteří přijíždějí na krátkodobý pobyt. Podobné systémy již zavedly takové země, jako jsou USA, Kanada a Austrálie, a to i pro občany EU.

Systémy cestovních povolení se opírají o on-line žádosti, v nichž žadatel před odjezdem uvede podrobnosti o své totožnosti, kontaktní údaje, účel cesty, itinerář apod. Jakmile je povolení získáno, řízení na hranicích při příjezdu se zrychlí a budou probíhat hladčeji. Mimo výhody v oblasti bezpečnosti a správy hranic a svůj případný význam v souvislosti s vízovou vzájemností by systém jako ETIAS sloužil tedy i jako nástroj pro snadnější cestování.

### 4. Evropský informační systém policejních záznamů (EPRIS)

Jak je uvedeno v Evropském programu pro bezpečnost, v budoucnu je třeba pracovat na výměně informací v oblasti dostupnosti stávajících policejních údajů v reálném čase napříč členskými státy. Komise posoudí nezbytnost, technickou proveditelnost a přiměřenost evropského indexového systému policejních záznamů (EPRIS) pro usnadnění přeshraničního přístupu k informacím, které jsou vedeny ve vnitrostátních databázích donucovacích orgánů. V této souvislosti Komise podporuje finančními prostředky EU provádění pilotního projektu skupinou pěti členských států, jejichž cílem je vytvořit mechanismus pro automatická přeshraniční vyhledávání ve vnitrostátních

rejstřících na základě pozitivního či negativního nálezu[25]. Komise vezme výsledky projektu v úvahu při svém hodnocení.

**Opatření pro vývoj dalších informačních systémů a řešení informačních mezer**

**Systém vstupu/výstupu (EES)**

- Evropský parlament a Rada by se měly legislativními návrhy o EES zabývat přednostně s cílem přijmout návrhy do konce roku 2016.

**Jmenná evidence cestujících (PNR)**

- Evropský parlament a Rada by měly směrnici o PNR přijmout do dubna 2016.
- Členské státy by měly směrnici o PNR provést bezodkladně po jejím přijetí.
- Komise by měla podporovat výměnu údajů mezi složkami pro informace o cestujících prostřednictvím standardizovaných řešení a postupů.
- Do tří měsíců po přijetí směrnice o PNR vypracuje Komise návrh prováděcího rozhodnutí o společných protokolech a podporovaných formátech dat pro přenos údajů z PNR od leteckých přepravců do složek pro informace o cestujících.

**Informační mezera před příjezdem státních příslušníků třetích zemí bez vízové povinnosti**

- V roce 2016 Komise posoudí nezbytnost, technickou proveditelnost a přiměřenost zavedení nového nástroje EU, například systému EU pro cestovní informace a povolení.

**Evropský informační systém policejních záznamů (EPRIS)**

- V roce 2016 Komise posoudí nezbytnost, technickou proveditelnost a přiměřenost zavedení systému EPRIS.

## 7. K INTEROPERABILITĚ INFORMAČNÍCH SYSTÉMŮ

Interoperabilita je schopnost informačních systémů provádět výměnu údajů a umožňovat sdílení informací. Lze rozlišovat mezi **čtyřmi rozměry interoperability**, přičemž každý vyvolává právní[26], technické a provozní otázky a otázky týkající se ochrany údajů:

- jediné vyhledávací rozhraní k vyslání dotazu do několika informačních systémů současně a k získání kombinovaných výsledků na jediné obrazovce,
- propojitelnost informačních systémů, kde bude do údajů zapsaných v jednom systému automaticky nahlížet jiný systém,
- zavedení sdílené služby pro porovnávání biometrických údajů na podporu různých informačních systémů,
- společné úložiště údajů pro různé informační systémy (základní modul).

Za účelem zahájení procesu směřujícího k interoperabilitě informačních systémů na úrovni EU zřídí Komise **odbornou skupinu pro informační systémy a interoperabilitu**

[25] Cílem pilotního projektu automatického procesu výměny údajů (ADEP) je vytvořit technický systém, který prostřednictvím rejstříku ukáže, zda v jednom nebo několika dalších členských státech existují policejní záznamy o určitém jedinci nebo policejním vyšetřování trestného činu. Automatická odpověď při vyhledávání v rejstříku by pouze uváděla, zda jsou údaje k dispozici („hit“ – pozitivní nález), či nikoli („no hit“ – negativní nález). V případě pozitivního nálezu by bylo nutné požádat prostřednictvím obvyklých kanálů policejní spolupráce o další osobní údaje.

[26] S výhradou specifických podmínek protokolu 22, pokud jde o Dánsko, a protokolů 21 a 36, pokud jde o Spojené království a Irsko.

na úrovni vyššího managementu, do níž budou zapojeny agentury EU, vnitrostátní odborníci a příslušné zainteresované instituce. Tato odborná skupina dostane za úkol vypořádat se s právními, technickými a provozními aspekty různých možností dosažení interoperability informačních systémů, včetně nezbytnosti, technické proveditelnosti a přiměřenosti dostupných možností a jejich důsledků pro ochranu údajů. Měla by se zabývat aktuálními nedostatky a mezerami ve znalostech způsobenými složitostí a roztříštěností informačních systémů na evropské úrovni. Odborná skupina zaujme obecný a komplexní pohled na správu hranic a prosazování práva, přičemž vezme v úvahu i úlohy, povinnosti a systémy celních orgánů v tomto ohledu. Pracovní metoda skupiny bude směřovat k posilování koordinace všech příslušných zkušeností, které byly v minulosti příliš často vyhodnocovány odděleně.

Cílem tohoto procesu je poskytnout celkovou strategickou vizi architektury správy údajů EU pro ochranu hranic a bezpečnost, jakož i přinést řešení pro její realizaci.

Tento konzultační proces bude **veden následujícími cíli**:

- Informační systémy by se měly vzájemně doplňovat. Mělo by se předcházet překrývání a stávající překrývání by mělo být odstraněno. Nedostatky by měly být patřičně řešeny.
- Měl by být zvolen modulární přístup, který plně využije technologického vývoje a bude stavět na zásadách ochrany soukromí již od návrhu.
- Od samého začátku by mělo být v souladu s Listinou základních práv zajištěno plné dodržování všech základních práv občanů EU i státních příslušníků třetích zemí.
- V případě nutnosti a proveditelnosti by informační systémy měly být propojeny a měly by být interoperabilní. Mělo by být zjednodušeno současné prohledávání systémů s cílem zajistit, že pohraniční stráži nebo policistům budou k dispozici všechny příslušné informace, pokud to bude nutné pro jejich dané úkoly, aniž budou stávající přístupová práva změněna.

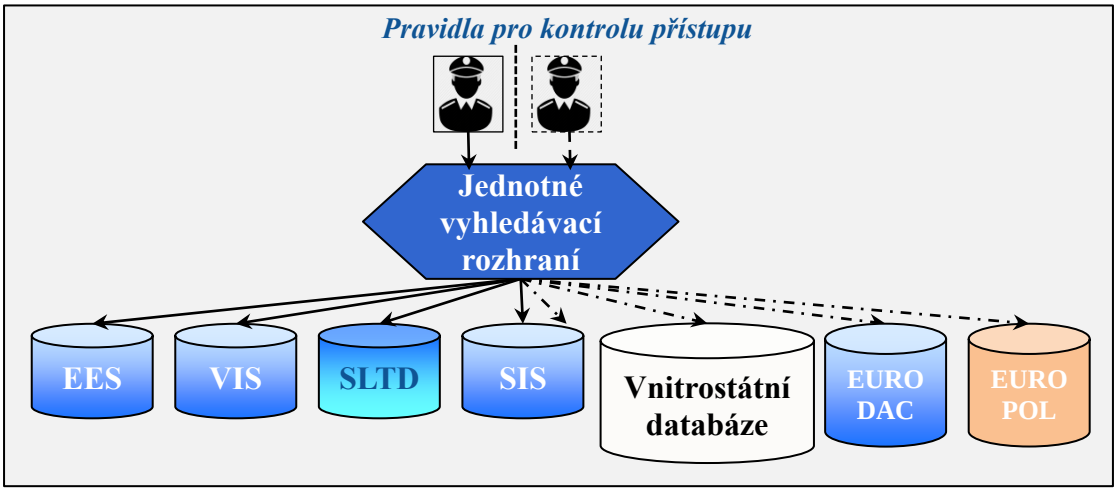
## 1. Jednotné vyhledávací rozhraní

Prvním rozměrem interoperability je **schopnost pohraniční stráže a policie dotazovat se několika informačních systémů současně a získat kombinované výsledky na jediné obrazovce** s plným dodržením jejich přístupových práv v souladu s danými účely. To vyžaduje platformy s jednotným vyhledávacím rozhraním, které budou schopny nahlížet v případně jednoho dotazu do více informačních systémů současně. Například prostřednictvím snímání čipu v cestovním dokladu nebo pomocí biometrických údajů by tato platforma mohla vydat dotaz do několika různých databází najednou. Jednotné vyhledávání platí pro všechny orgány, které potřebují mít přístup k údajům a využívat je (tj. pohraniční stráž, donucovací orgány, azylové služby) v souladu s účelovým omezením a přísnými pravidly pro kontrolu přístupu. Lze ho využít i na mobilním zařízení. Vytvořením jednotného vyhledávacího rozhraní se sníží složitost informačních systémů na evropské úrovni, jelikož pohraniční stráži a policistům dává možnost vydat dotaz do několika informačních systémů současně jedním postupem a v souladu s jejich přístupovými právy.

Několik členských států takové platformy s jednotným vyhledávacím rozhraním již nainstalovalo. Na základě těchto stávajících osvědčených postupů bude Komise společně s agenturou eu-LISA usilovat o zavedení standardizovaného řešení jednotného vyhledávacího rozhraní. K financování zavedení takové funkce by členské státy měly používat finanční prostředky EU v rámci svého vnitrostátního programu Fondu pro

vnitřní bezpečnost. Komise bude pozorně sledovat, jak členské státy funkci jednotného vyhledávacího rozhraní využívají na vnitrostátní úrovni.

***Obrázek 2** Jednotné vyhledávací rozhraní*




Vyhledávání v několika centralizovaných nebo vnitrostátních systémech (podle obrázku) je snadnější než vyhledávání v decentralizovaných systémech. Komise a agentura eu-LISA budou zkoumat, zda lze jednotné vyhledávací rozhraní využít i k provádění souběžných vyhledávání jednotných kontaktních míst v decentralizovaných systémech, jako jsou prümský rámec a systém ECRIS. Tuto analýzu provedou Komise a eu-LISA společně s odbornou skupinou pro informační systémy a interoperabilitu, aniž změní stávající přístupová práva.

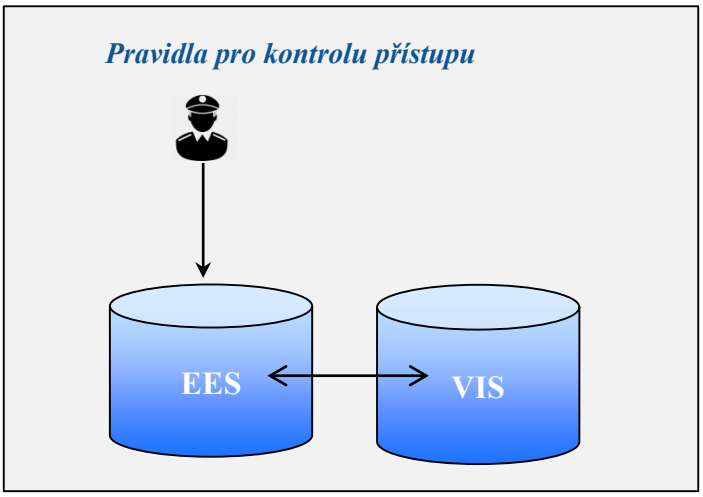
**2. Propojitelnost informačních systémů**

Druhým rozměrem interoperability je propojitelnost informačních systémů. To znamená, že různé systémy nebo databáze jsou technicky schopny „spolu hovořit“. **Do údajů zapsaných v jednom systému by na centrální úrovni mohl automaticky nahlížet jiný systém**. To vyžaduje technickou kompatibilitu systémů a interoperabilitu datových prvků v těchto systémech uložených (např. otisky prstů). Propojitelnost může omezit množství údajů obíhajících v komunikačních sítích a procházejících vnitrostátními systémy.

Propojitelnost vyžaduje vhodná ochranná opatření na ochranu údajů a přísná pravidla pro kontrolu přístupu. Politická dohoda, jíž společní normotvůrci dosáhli v prosinci 2015 ohledně reformy ochrany údajů, zavede v celé EU moderní rámec ochrany údajů, který tato ochranná opatření stanoví. Je důležité, aby společní normotvůrci neprodleně přijali obecné nařízení o ochraně údajů a směrnici o ochraně údajů.

Součástí budoucího systému EES je koncept propojitelnosti. Tento systém bude schopen komunikovat přímo se systémem VIS na centrální úrovni a naopak. To je důležitý krok při řešení současné roztříštěnosti architektury správy údajů v EU pro ochranu hranic a bezpečnost, jakož i souvisejících problémů. Automatické křížové kontroly zbaví členské státy nutnosti zadávat dotazy do VIS při hraničních kontrolách, sníží požadavky na údržbu a zlepší výkonnost systému.

***Obrázek 3*** *Propojitelnost systémů: příklad EES/VIS*



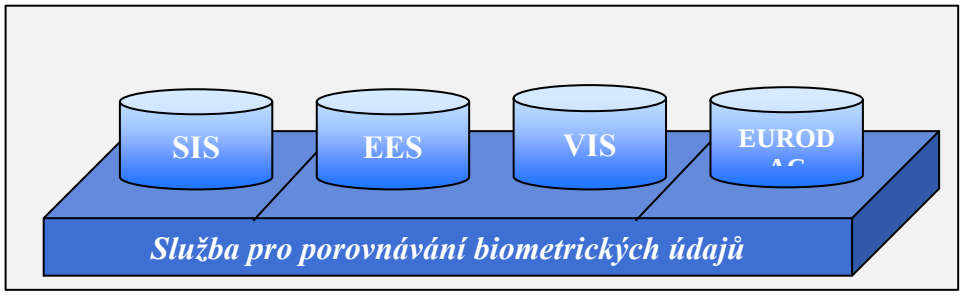

V dalším kroku Komise a agentura eu-LISA zanalyzují, zda bude moci být propojitelnost na centrální úrovni mezi budoucím EES a systémem VIS rozšířena na SIS a zda bude moci být zavedena propojitelnost mezi systémy EURODAC a SIS. Tuto analýzu Komise a eu-LISA provedou společně s odbornou skupinou pro informační systémy a interoperabilitu.

### 3. Sdílená služba pro porovnávání biometrických údajů

Třetí rozměr interoperability je v oblasti biometrických identifikátorů. Například když jsou otisky prstů odebrány na konzulátu jednoho členského státu se specifickým vybavením, je zásadní, aby tyto otisky mohly být porovnány prostřednictvím systému VIS na stanovišti hraniční kontroly jiného členského státu, který používá zařízení jiného typu. Stejný požadavek se týká dotazů na otisky prstů v jiných systémech: biometrické vzorky musí splňovat minimální požadavky na kvalitu a formát, aby bylo bez obtíží dosaženo tohoto typu interoperability.

Na úrovni systému umožňuje interoperabilita biometrických identifikátorů využívat sdílenou službu pro porovnávání biometrických údajů pro několik informačních systémů, přičemž jsou dodržována pravidla ochrany osobních údajů roztříštěním údajů s oddělenými pravidly kontroly přístupu pro každou kategorii údajů[27]. Takové sdílené služby přinášejí výrazné výhody z hlediska financí, údržby a provozu.

***Obrázek 4*** *Sdílená služba pro porovnávání biometrických údajů*




Komise a eu-LISA zanalyzují, zda je nutné a technicky proveditelné zavést sdílenou službu pro porovnávání biometrických údajů pro všechny příslušné informační systémy.

[27] Srovnatelné se sdílením jednoho fyzického serveru se soubory s velkým počtem uživatelů, z nichž každý má specifická přístupová práva pouze k určitým složkám.

Tuto analýzu Komise a agentura eu-LISA provedou společně s odbornou skupinou pro informační systémy a interoperabilitu.

## 4. Společné úložiště údajů

Nejambicióznějším dlouhodobým přístupem k interoperabilitě by bylo **společné úložiště údajů na úrovni EU pro různé informační systémy**. Společné úložiště by představovalo základní modul, který by obsahoval základní údaje (alfanumerické a biometrické údaje), zatímco jiné prvky údajů a specifické znaky různých informačních systémů (např. údaje o vízech) by se ukládaly ve specifických modulech. Základní modul a specifické moduly by byly vzájemně propojeny, aby spojily příslušné soubory údajů. To by vytvořilo **modulární a integrovanou správu identit pro hranice a bezpečnost.** Musel by být zajištěn soulad s pravidly pro ochranu údajů, například roztříštěním údajů, přičemž každá kategorie údajů by měla zvláštní pravidla pro kontrolu přístupu.

Zavedením společného úložiště údajů by se překonala současná roztříštěnost architektury správy údajů v EU pro ochranu hranic a bezpečnost. Toto roztříštění je v rozporu se zásadou minimalizace údajů, jelikož způsobuje, že stejné údaje jsou ukládány několikrát. Společné úložiště by v případě potřeby umožnilo rozpoznání propojení a poskytlo by celkový obraz spojením prvků jednotlivých údajů uložených v různých informačních systémech. Odstranily by se tak současné znalostní mezery a osvětlily pohraniční stráži a policistům nevyjasněné otázky.

***Obrázek 5*** *Společné úložiště údajů*

Možnost zavedení společného úložiště údajů na úrovni EU vyvolává důležité otázky definice účelu, nezbytnosti, technické proveditelnosti a přiměřenosti zpracovávání údajů. Vyžadovala by úplnou revizi právního rámce, který zavádí různé informační systémy, a mohlo by se jednat pouze o cíl, kterého má být dosaženo v dlouhodobém horizontu.

Odborná skupina pro informační systémy a interoperabilitu se zaměří na právní, technické a provozní otázky spojené se společným úložištěm údajů, včetně otázek ochrany údajů.

U všech čtyř rozměrů interoperability uvedených výše (jednotné vyhledávací rozhraní, propojitelnost systémů, jednotná služba pro porovnávání biometrických údajů a společné úložiště údajů) je nutné, aby údaje uložené v různých informačních systémech nebo modulech byly kompatibilní. Pro dosažení toho je důležité, aby za účelem vytvoření společné normy pro všechny příslušné informační systémy postoupily práce na **jednotném formátu zpráv** (UMF)[28].

**Opatření směřující k interoperabilitě informačních systémů**

- Komise zřídí společně s agenturami EU, členskými státy a příslušnými zúčastněnými subjekty **odbornou skupinu pro informační systémy a interoperabilitu** s cílem prozkoumat právní, technické a provozní aspekty posílení interoperability informačních systémů, včetně nezbytnosti, technické proveditelnosti a přiměřenosti dostupných možností a jejich důsledků pro ochranu údajů.

**Jednotné vyhledávací rozhraní**

- Komise a agentura eu-LISA podpoří členské státy při zavádění jednotného vyhledávacího rozhraní pro vysílání dotazů do centrálních systémů.
- Komise a agentura eu-LISA budou společně s odbornou skupinou zkoumat, zda by se jednotná vyhledávací rozhraní mohla používat k provádění souběžných vyhledávání přes jedno kontaktní místo ve všech příslušných systémech, aniž budou změněna stávající přístupová práva.

**Propojitelnost informačních systémů**

- Komise a agentura eu-LISA společně s odbornou skupinou zanalyzují, zda by mohla být dále podporována propojitelnost centralizovaných informačních systémů, a to nad rámec již navržené propojitelnosti mezi systémem vstupu/výstupu a vízovým informačním systémem.

**Služba pro porovnávání biometrických údajů**

- Komise a agentura eu-LISA společně s odbornou skupinou zanalyzují nezbytnost a technickou proveditelnost zavedení sdílené služby pro porovnávání biometrických údajů pro všechny příslušné informační systémy.

**Společné úložiště údajů (základní modul)**

- Komise a agentura eu-LISA společně s odbornou skupinou prozkoumají právní, technické, provozní a finanční aspekty dlouhodobějšího vývoje společného úložiště údajů.
- Komise a agentura eu-LISA se zapojí do probíhajících prací směřujících ke globálnímu jednotnému formátu zpráv pro všechny příslušné informační systémy.

[28] Komise podpořila pokračující vývoj UMF ve sdělení z roku 2012 o evropském modelu pro výměnu informací (EIXM) a v současnosti financuje třetí pilotní projekt UMF s cílem vytvořit společnou normu pro všechny příslušné databáze, která se bude používat na vnitrostátní úrovni (členských států), na úrovni EU (pro centrální systémy a agenturami) a na mezinárodní úrovni (Interpol).

## 8. ZÁVĚR

Toto sdělení zahajuje diskusi o tom, jak informační systémy v EU mohou ještě více zdokonalit správu hranic a vnitřní bezpečnost na základě významných synergií mezi evropskými programy pro bezpečnost a migraci. Pohraniční stráži a policistům poskytuje relevantní informace již celá řada informačních systémů, ty však nejsou dokonalé. EU čelí výzvě vybudovat silnější a inteligentnější architekturu správy údajů plně v souladu se základními právy, zejména s ochranou osobních údajů a její zásadou účelového omezení.

Pokud v architektuře správy údajů v EU existují nedostatky, musí být řešeny. Společně s tímto sdělením předložila Komise návrh systému vstupu/výstupu, který by měl být neprodleně přijat. V nadcházejících týdnech je rovněž nutné přijmout směrnici o jmenné evidenci cestujících. Návrh na zřízení evropské pohraniční a pobřežní stráže by měl být přijat do léta. Souběžně s tím bude Komise pokračovat v práci na posilování a v případě potřeby zefektivnění stávajících systémů, jako je vývoj funkce systému automatizované identifikace otisků prstů pro Schengenský informační systém.

Členské státy musí plně využívat stávající informační systémy a v souladu se svými právními závazky musí zavést nezbytná technické propojení se všemi informačními systémy a databázemi. Neprodleně musí být napraveny stávající nedostatky, zejména v prümském rámci. Zatímco toto sdělení otevírá diskusi a zahajuje proces řešení systémových mezer a slabin, musí členské státy naléhavě řešit přetrvávající nedostatky v doplňování databází EU a při výměně informací napříč Unií.

Za účelem strukturálního zlepšení architektury správy údajů v EU pro ochranu hranic a bezpečnost zahajuje toto sdělení proces směřující k interoperabilitě informačních systémů. Komise zřídí odbornou skupinu pro informační systémy a interoperabilitu, která se bude zabývat řešením právních, technických a provozních aspektů možností, jak dosáhnout interoperability informačních systémů a řešit jakékoli nedostatky a mezery. Na základě zjištění odborné skupiny Evropská komise představí Evropskému parlamentu a Radě jako základ pro společnou diskusi o cestě vpřed další konkrétní nápady. Komise bude též usilovat o příspěvek evropského inspektora ochrany údajů a vnitrostátních orgánů pro ochranu údajů působících společně v pracovní skupině zřízené podle článku 29.

Cílem by mělo být vytvoření společné strategie, aby správa údajů v EU byla účinnější a účelnější a zároveň se plně respektovaly požadavky na ochranu údajů, lépe chránily vnější hranice a posilovala vnitřní bezpečnost, a to ku prospěchu všech občanů.

## PŘÍLOHA 1: ZKRATKY

| | |
|---|---|
| API | Předběžné informace o cestujících |
| AFIS | Systém automatické identifikace otisků prstů: systém schopný zachycovat, ukládat, porovnávat a ověřovat otisky prstů. |
| CIS | Celní informační systém |
| ECRIS | Evropský informační systém rejstříků trestů |
| EES | (Navrhovaný) systém vstupu/výstupu |
| EIXM | Evropský model pro výměnu informací |
| EIS | Informační systém Europolu |
| EPRIS | Evropský informační systém policejních záznamů |
| EURODAC | Evropský systém pro porovnávání otisků prstů |
| EUROPOL | Evropský policejní úřad (donucovací agentura Evropské unie) |
| ETIAS | (Možný) systém EU pro cestovní informace a povolení |
| eu-LISA | Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva |
| FIND | Stacionární databáze sítě Interpolu |
| FRONTEX | Evropská agentura pro řízení operativní spolupráce na vnějších hranicích členských států Evropské unie |
| iARMS | Systém Interpolu pro správu záznamů o nedovolených zbraních a sledování jejich pohybu |
| INTERPOL | Mezinárodní organizace kriminální policie |
| MIND | Mobilní databáze sítě Interpolu |
| PIU | Složka pro informace o cestujících: složka, která musí být zřízena v každém členském státě, aby mohly být přijímány údaje PNR od přepravců |
| PNR | Jmenná evidence cestujících |
| Prüm | Mechanismus policejní spolupráce pro výměnu informací o DNA, otiscích prstů a registračních údajích vozidel |
| SafeSeaNet | Evropská platforma pro výměnu informací na moři mezi námořními orgány členských států |
| SBC | Schengenský hraniční kodex |
| SIENA | Aplikace sítě pro bezpečnou výměnu informací |
| SIS | Schengenský informační systém (někdy nazývaný i Schengenský informační systém druhé generace – SIS II) |
| SLTD | Databáze (Interpolu) odcizených a ztracených cestovních dokladů |
| sTESTA | Zabezpečené transevropské služby pro telematiku mezi správními orgány (bude zmodernizován na systém TESTA-NG (příští generace)) |
| UMF | Jednotný formát zpráv: formát zpráv umožňující kompatibilitu informačních systémů |
| VIS | Vízový informační systém |

| | |
|---|---|
| VRD | Registrační údaje vozidel |

**PŘÍLOHA 2: SEZNAM STÁVAJÍCÍCH INFORMAČNÍCH SYSTÉMŮ PRO SPRÁVU HRANIC A PROSAZOVÁNÍ PRÁVA**

## 1. Schengenský informační systém (SIS)

Systém SIS je největší a nejrozšířenější platforma pro výměnu informací o přistěhovalectví a prosazování práva. Je to centralizovaným systém, který využívá 25 členských států EU[29] a čtyři země přidružené k Schengenu[30] a který v současnosti obsahuje 63 milionů záznamů. Tyto záznamy vkládají příslušné orgány, jako je policie, orgány ochrany hranic a imigrační orgány, a nahlížejí do nich. Obsahuje záznamy o státních příslušnících třetích zemí, jimž je zakázán vstup do schengenského prostoru nebo pobyt v něm, jakož i záznamy o státních příslušnících EU a třetích zemí, kteří jsou hledáni nebo pohřešováni (včetně dětí), a o hledaných věcech (zbraních, vozidlech, dokladech totožnosti, průmyslovém zařízení apod.). Charakteristickým znakem systému SIS v porovnání s jinými nástroji pro sdílení informací je to, že jeho informace jsou doplněny o pokyn, jaké konkrétní opatření mají policisté na místě učinit, např. zatčení nebo zajištění.

Kontroly v SIS jsou povinné při zpracování krátkodobých víz, při hraničních kontrolách státních příslušníků třetích zemí a nesystematicky[31] u občanů EU a jiných osob s právem volného pohybu. Kromě toho by automatickou kontrolu v SIS měly zahrnovat i všechny policejní kontroly na území.

## 2. Vízový informační systém (SIS)

Systém VIS je centralizovaný systém pro výměnu údajů o krátkodobých vízech mezi členskými státy. Zpracovává údaje a rozhodnutí týkající se žádostí o krátkodobá víza pro návštěvu schengenského prostoru nebo průjezd schengenským prostorem. K systému byly připojeny všechny konzuláty schengenského prostoru (zhruba 2 000) a všechny hraniční přechody na vnějších hranicích (celkem asi 1 800).

Systém VIS obsahuje údaje o žádostech a rozhodnutích o vízech a informace o tom, zda vydaná víza byla zrušena, prohlášena za neplatná nebo zda byla prodloužena jejich platnost. V současnosti obsahuje údaje o 20 milionech žádostí o víza a ve špičkách zpracuje více než 50 000 operací za hodinu. Každý žadatel o vízum poskytne podrobné biografické informace, digitální fotografii a deset otisků prstů. Systém jako takový je spolehlivým prostředkem k ověřování totožnosti žadatelů o vízum, k posouzení možných případů nelegální migrace a bezpečnostních rizik a k předcházení spekulativnímu podávání žádostí o víza.

Na hraničních přechodech nebo na území členských států se VIS používá k ověření totožnosti držitelů víza porovnáním jejich otisků prstů s otisky uloženými v tomto systému. Tento proces zaručuje, že osoba, která zažádala o vízum, je tatáž osoba, která překračuje hranici. Vyhledávání otisků prstů ve VIS umožňuje identifikaci osoby, která podala žádost o vízum v posledních pěti letech, ale která nemá doklad totožnosti.

[29] Všechny kromě Irska, Kypru a Chorvatska.
[30] Švýcarsko, Lichtenštejnsko, Norsko a Island.
[31] Jak předpokládá návrh Komise COM/2015/0670 o změně Schengenského hraničního kodexu, je toto pravidlo předmětem změny.

## 3. EURODAC

Systém EURODAC (Evropský systém pro porovnávání otisků prstů) obsahuje otisky prstů žadatelů o azyl a státních příslušníků třetích zemí, kteří překračují vnější hranice schengenského prostoru nelegálně. Jeho současným primárním účelem je určit, která země EU odpovídá v souladu s dublinským nařízením za zpracování žádosti o azyl. Je k dispozici na hraničních přechodech, ale na rozdíl od systémů SIS a VIS není systémem správy hranic.

Otisky prstů nelegálních migrantů vstupujících do EU protiprávně jsou odebírány na hraničních přechodech. Ukládají se do systému EURODAC pro ověření totožnosti osoby v případě budoucí žádosti o azyl. Imigrační a policejní orgány mohou porovnávat i otisky prstů nelegálních migrantů nalezených v členských státech EU za účelem kontroly, zda nepožádali o azyl v jiném členském státě. Vyhledávat v systému EURODAC jsou oprávněny i donucovací orgány a Europol s cílem předcházet závažné trestné činnosti nebo teroristickým trestným činům, odhalovat je nebo vyšetřovat.

Díky registraci otisků prstů žadatelů o azyl nebo nelegálních migrantů v centralizovaném systému je možná i identifikace a sledování jejich druhotného pohybu[32] v EU, dokud není předložena žádost o mezinárodní ochranu nebo není vydáno rozhodnutí o navrácení (v budoucnosti, s odpovídajícím záznamem v SIS). Obecněji je prokazování totožnosti a sledování nelegálních migrantů vyžadováno pro zajištění vydání nových dokladů orgány v jejich zemích původu, a tím usnadnění jejich návratu.

## 4. Odcizené a ztracené cestovní doklady (SLTD)

Databáze (Interpolu) odcizených a ztracených cestovních dokladů (SLTD) je centrální databáze cestovních pasů a jiných cestovních dokladů, které vydávající orgány nahlásily Interpolu jako odcizené nebo ztracené. Obsahuje informace o odcizených nevyplněných cestovních pasech. Cestovní doklady, které byly orgánům zemí účastnících se SIS nahlášeny jako ztracené nebo odcizené, jsou zapisovány do SLTD i SIS. Databáze SLTD obsahuje též údaje o cestovních dokladech, které do ní zadaly země neúčastnící se SIS (Irsko, Chorvatsko, Kypr a třetí země).

Jak je uvedeno v závěrech Rady ze dne 9. a 20. listopadu 2015 a v návrhu Komise ze dne 15. prosince 2015 nařízení o cílené změně Schengenského hraničního kodexu[33], měly by být podle SLTD ověřovány cestovní doklady všech státních příslušníků třetích zemí a osob s právem volného pohybu. K SLTD musí být připojena všechna stanoviště hraniční kontroly. Navíc by další bezpečnostní výhody přineslo vyhledávání v SLTD při prosazování práva v zemi.

## 5. Předběžné informace o cestujících (API)

Úkolem systému API je shromáždit informace o totožnosti osoby před jejím vstupem na palubu letadla přilétajícího do EU a při příjezdu identifikovat nelegální migranty. Údaje z evidence API jsou tvořeny informacemi uvedenými v cestovním dokladu a zahrnují celé jméno cestujícího, datum narození, státní příslušnost, číslo a typ cestovního dokladu, informace o stanovišti hraniční kontroly při odjezdu a vstupu a podrobnosti o dopravě. Údaje z evidence API týkající se cestujícího jsou obvykle sbírány v okamžiku odbavení.

---

[32] Například uprchlíci přijíždějící do Řecka nemají v úmyslu požádat o azyl v Řecku, ale cestují po pevnině dále do jiných členských států.

[33] COM(2015) 670 final. Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení č. 562/2006 (ES), pokud jde o posílení kontrol na vnějších hranicích na základě příslušných databází.

Informace před příjezdem týkající se dopravy po moři musí být podle Úmluvy o usnadnění mezinárodní námořní dopravy předávány 24 hodin před plánovaným připlutím plavidla. Směrnice 2010/65/EU[34] stanoví elektronický přenos údajů prostřednictvím jednotného portálu spojujícího systémy SafeSeaNet, e-Customs a další elektronické systémy.

Pro záznamy údajů z evidence API neexistuje žádný centrální systém EU.

## 6. Informační systém Europolu

Informační systém Europolu (EIS) je centralizovaná databáze informací o trestné činnosti pro účely vyšetřování. Členské státy a Europol ho mohou využívat k ukládání údajů a dotazování na údaje o závažné trestné činnosti a terorismu. Informace uložené v EIS se týkají údajů o osobách, dokladů totožnosti, vozidel, zbraní, telefonních čísel, e-mailů, otisků prstů, DNA a informací o počítačové trestné činnosti, které lze různými způsoby vzájemně propojit a vytvořit podrobnější a strukturovaný obraz o trestném činu. EIS podporuje spolupráci donucovacích orgánů a není k dispozici pohraničním orgánům.

Výměna informací probíhá přes platformu SIENA[35], což je bezpečná elektronická komunikační síť mezi Europolem, styčnou kanceláří, národními jednotkami Europolu, určenými příslušnými orgány (jako jsou celní orgány, úřady pro vyhledávání majetku z trestné činnosti atd.) a připojenými třetími stranami.

V květnu 2017 nabude účinnosti nový právní rámec pro Europol. Tento rámec umožní vylepšenou operační schopnost Europolu pro účely provádění analýzy a pro lepší identifikaci vazeb mezi dostupnými informacemi.

## 7. Prümský rámec

Prümský rámec se opírá o mnohostrannou dohodu[36] mezi členskými státy, která umožňuje výměnu DNA, otisků prstů a registračních údajů vozidel (VRD). Koncept vychází z připojení vnitrostátního systému k vnitrostátním systémům všech ostatních členských států EU pro umožnění křížových vyhledávání informací na dálku. Pokud vyhledávání přinese pozitivní nález v databázi jiných členských států, proběhne výměna podrobností o pozitivním nálezu prostřednictvím dvoustranných mechanismů výměny.

## 8. Evropský informační systém rejstříků trestů (ECRIS)

ECRIS je elektronický systém pro výměnu informací o předchozích odsouzeních konkrétní osoby u trestních soudů v EU pro účely trestních řízení s určitou osobou, a umožňuje-li to vnitrostátní právo, pro další účely. Členské státy, které odsoudí státního příslušníka jiného členského státu, musí toto odsouzení oznámit členskému státu státní příslušnosti. Členský stát státní příslušnosti musí tyto informace uložit, a může tak na žádost poskytnout aktuální informace o svých státních příslušnících z rejstříku trestů bez ohledu na to, kde v EU k odsouzení došlo.

Systém ECRIS též umožňuje výměnu informací o odsouzeních státních příslušníků třetích zemí a osob bez státní příslušnosti. Určenými centrálními orgány v každém

[34] Směrnice Evropského parlamentu a Rady 2010/65/EU ze dne 20. října 2010 o ohlašovacích formalitách lodí připlouvajících do přístavů členských států nebo odplouvajících z nich a o zrušení směrnice 2002/6/ES.

[35] Aplikace sítě pro bezpečnou výměnu informací.

[36] Prümská smlouva z roku 2005. Smlouva byla zahrnuta do právních předpisů EU v roce 2008 rozhodnutím Rady 2008/615/SVV.

členském státě jsou kontaktní místa v síti ECRIS, která se zabývají všemi úkoly, jako je oznamování, ukládání, vyžádání a poskytování informací z rejstříků trestů.