VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2007

Částka 46 **5. října 2007** **Cena 96,– Kč**

OBSAH

Úvod 2686

I. Registrace

Přehled zrušených registrací za období od 16. 7. 2007 do 24. 9. 2007 2687

II. Stanoviska Úřadu

Stanovisko č. 2/2007: Zdravotnická dokumentace a ochrana osobních údajů z pohledu nové úpravy 2688

III. Sdělení Úřadu

a) Úřad pro ochranu osobních údajů k problémům z praxe – č. 1/2007: K problematice narušování soukromí prostřednictvím funkce hlasitého odposlechu mobilních telefonů 2691

b) Společná koordinační skupina pro EURODAC – zpráva o koordinované inspekci 2691

c) Stanovisko č. 4/2007 Pracovní skupiny pro ochranu dat podle článku 29 směrnice 95/46/ES k pojmu osobní údaje (Překlad pořízený Evropskou komisí, přetisk v původní podobě) 2693

IV. Materiály z Úředního věstníku Evropské unie

Rozhodnutí Rady 2007/533/SV ze dne 12. června 2007 o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II) (Přetisk z Úředního Věstníku EU) 2719

ÚVOD

Částka 46 Věstníku Úřadu pro ochranu osobních údajů obsahuje přehled zrušených registrací za období od 16. 7. 2007 do 24. 9. 2007.

Rubrika Stanoviska Úřadu přináší Stanovisko č. 2/2007 „Zdravotnická dokumentace a ochrana osobních údajů z pohledu nové úpravy". Dokument vyjadřuje postoj Úřadu k novelizované právní úpravě zákona o péči o zdraví lidu. Z hlediska ochrany osobních údajů je zřejmé, že zákon o péči o zdraví lidu přináší do oblasti ochrany osobních údajů novou zvláštní úpravu, která se týká zejména pacienta, osob jemu blízkých a jejich práv na informace o zdravotním stavu, ale také povinností zdravotnických pracovníků při zabezpečování těchto práv pacienta a dalších osob zákonem stanovených.

V oddíle K problémům z praxe, který je součástí rubriky Sdělení Úřadu, najdete v informaci „K problematice narušování soukromí prostřednictvím funkce hlasitého odposlechu mobilních telefonů" vyjádření Úřadu k riziku možného průlomu do soukromí občanů a k porušení práva na ochranu osobních údajů, které je spojeno s funkcí hlasitého odposlechu v mobilních telefonech.

V rubrice Sdělení je také začleněna informace Úřadu o zprávě „Společná koordinační skupina pro EURODAC – zpráva o koordinované inspekci". Zprávu společné koordinační skupiny o výsledcích inspekce systému EURODAC (evropská databáze otisků prstů, vytvořená na základě nařízení Rady /ES/) publikoval Evropský inspektor pro ochranu údajů, který je garantem, že při využívání systému EURODAC nedochází k porušování práva občanů na ochranu před nezákonným zpracováním osobních údajů a k porušování souvisejícího práva na ochranu soukromí.

Součástí rubriky sdělení je Stanovisko č. 4/2007 Pracovní skupiny pro ochranu dat podle článku 29 směrnice 95/46/ES (WP29) k pojmu osobní údaje. Z informací o současné praxi v členských státech EU vyplývá, že mezi členskými státy existuje ohledně důležitých aspektů tohoto pojmu určitá nejistota a rozdílnost v přístupech. Cílem tohoto stanoviska pracovní skupiny je dosáhnout společného porozumění pojmu osobní údaje, situacím, v nichž by se měly používat vnitrostátní právní předpisy o ochraně údajů, a správnému způsobu jejich použití.

Rubrika Materiály z Úředního věstníku Evropské unie přináší „Rozhodnutí Rady 2007/533/SV ze dne 12. června 2007 o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II)". Úřad publikuje výše uvedený materiál v návaznosti na skutečnost, že se ode dne 1. září 2007 v souvislosti s připravovaným vstupem do schengenského prostoru Česká republika plně zapojila do fungování Schengenského informačního systému (tzv. SIS) a veškeré aktivity v této oblasti se ČR bezprostředně týkají. Bližší informace jsou k dispozici na webových stránkách Úřadu http://www.uoou.cz v rubrice Schengen. Souhrnné informace o Schengenu jsou umístěny na webových stránkách Euroskop.cz a také na www.mvcr.cz/schengen .

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00003607/001	JIHOČESKÁ PLYNÁRENSKÁ A.S.	13. 8. 2007

II. STANOVISKA ÚŘADU

Stanovisko č. 2/2007

září 2007

Zdravotnická dokumentace a ochrana osobních údajů z pohledu nové úpravy

Základní právní úpravu vedení zdravotnické dokumentace a poskytování informací o zdravotním stavu nejen pacientům, ale i příbuzným, případně pozůstalým, představuje zákon č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů, zejména ve znění poslední novelizace, provedené zákonem č. 111/2007 Sb. (dále jen „zákon o péči o zdraví lidu"). Problematikou vedení zdravotnické dokumentace, jakožto „citlivých údajů" a vztahu k zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění (dále jen „zákon o ochraně osobních údajů") se již Úřad pro ochranu osobních údajů (dále jen „Úřad") zabýval ve svých předchozích stanoviscích, zejména ve Stanovisku č. 1/2000 a 1/2002, která však již byla s ohledem na citovaný zákon č. 111/2007 Sb. částečně překonána, a proto se vydává toto nové stanovisko.

V případě zdravotnické dokumentace se jedná o zpracování osobních údajů ve smyslu ustanovení § 4 písm. e) zákona o ochraně osobních údajů. Takové zpracování lze označit za zpracování osobních údajů, probíhající v souladu s ustanovením § 5 odst. 2 písm. a) zákona o ochraně osobních údajů, obsahující výjimku pro zpracování osobních údajů bez souhlasu pacienta (subjektu údajů) nebo souhlasu jeho zákonného zástupce. Vzhledem k tomu, že zdravotnická dokumentace obsahuje informace o zdravotním stavu pacienta, je zpracování takových osobních údajů nutno posuzovat také v mezích § 9 tohoto zákona, který upravuje podmínky pro zpracování citlivých údajů. V tomto ustanovení lze pro daný právní rámec zákona o péči o zdraví lidu nalézt několik zvláštních výjimek. Nejvýznamnější z nich je § 9 písm. c), podle něhož lze zpracovávat osobní údaj vypovídající o zdravotním stavu subjektu údajů v případě, že **jde o poskytování zdravotní péče, ochrany veřejného zdraví, zdravotního pojištění a výkon státní správy v oblasti zdravotnictví**, jakož i jiné posuzování zdravotního stavu podle zvláštního právního předpisu, zejména pro účely sociálního zabezpečení, nebo je tak stanoveno zvláštním zákonem. Jedná se tedy o zpracování bez výslovného souhlasu subjektu údajů. Z hlediska dané problematiky přicházejí v úvahu ještě další ustanovení § 9 připouštějící zpracování osobních údajů při vedení zdravotnické dokumentace, a to § 9 písm. b), f) nebo h).

Povinnosti správce nebo zpracovatele při zpracování osobních údajů jsou upraveny v několika základních ustanoveních zákona o ochraně osobních údajů, z nichž nejdůležitější jsou § 5 odst. 1, § 6, § 11 a § 13 zákona o ochraně osobních údajů.

Jedním z nejčastějších způsobů zpracování osobních údajů obsažených ve zdravotnické dokumentaci je nahlížení do této dokumentace (zpřístupnění). S právem nahlížet pak bývalo spojeno výkladem *per analogiam* i právo pořizovat si výpisy, opisy, respektive kopie jednotlivých dokumentů. To vše se až dosud netýkalo práva pacienta nebo práva jeho příbuzných. Tato práva však výslovně obsahuje až zákon č. 111/2007 Sb., kterým se mění zákon č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů, a některé další zákony (dále jen „zákon č. 111/2007 Sb."). Poprvé je tak nesporně upraveno dosud absentující výslovné právo na pořízení výpisů, opisů nebo kopií zdravotnické dokumentace, když v § 67b odst. 10 bylo doplněno závěrečné ustanovení, které zní: „Osoby, které mohou nahlížet do zdravotnické dokumentace, mají též právo na pořízení jejich výpisů, opisů nebo kopií v rozsahu nezbytně nutném pro splnění konkrétního úkolu".[1)]

Novelizovaná právní úprava přebírá stávající znění § 67b odst. 12 zákona o péči o zdraví lidu, tedy práva na poskytnutí veškerých informací shromážděných ve zdravotnické dokumentaci vedené o pacientovi nebo v jejích částech nebo v jiných zápisech vztahujících se k jeho zdravotnímu stavu. **Nově však dává pacientovi právo v přítomnosti zdravotnického pracovníka nejen nahlížet do zdravotnické dokumentace vedené o jeho osobě nebo jejích částí nebo jiných zápisů vztahujících se k jeho zdravotnímu stavu, obojí s výjimkou informací z autorizovaných psychologických metod a popisu léčby psychologickými prostředky, ale i právo na pořízení výpisů, opisů nebo kopií dokumentů s omezením zde přímo uvedeným.**

Současně je uvedená právní úprava vztahující se ke zpracování údajů o zdravotním stavu pacienta jednou ze zvláštních právních úprav, která upravuje právo občana na informace. Obecnou právní úpravou, pokud se jedná o zpracování osobních údajů, je právo na informace garantované pacientovi ustanovením § 12 zákona o ochraně osobních údajů, neboť při vedení zdravotnické dokumentace jde vždy o zpracování osobních údajů. Každému pacientovi je tak vždy přiznáno právo na informace, respektive na informaci o tom, jaké osobní údaje jsou o něm zpracovávány. Vedle tohoto ustanovení však zákon 101/2000 Sb. v ustanovení § 21 reguluje podmínky práva na přístup k informacím – osobním údajům, a to za situace, kdy subjekt údajů zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem o ochraně osobních údajů.

Myšlenka využít pouze zákon o ochraně osobních údajů k zaplnění právní mezery spočívající v absenci výslovné mož-

---

[1)] Touto novelou byl také rozšířen okruh osob, které mohou do zdravotnické dokumentace nahlížet.

nosti získat opisy a výpisy ze zdravotnické dokumentace by byla chybná. I Úřad se touto myšlenkou zabýval a k problematice se vyjádřil ve svém stanovisku k problémům z praxe, kde vyjádřil názor, že k tomu, aby pacient získal opis celé zdravotnické dokumentace či její části se na § 12 odst. 2 zákona o ochraně osobních údajů dovolávat nelze.[2)] Z pohledu ochrany osobních údajů je zákon č. 111/2007 Sb. první ucelenou a zdařilou právní úpravou vedoucí k zaplnění právní mezery v právech pacienta na pořízení výpisů, opisů nebo kopií zdravotnické dokumentace. Touto právní úpravou dochází nepochybně k odstranění nutnosti získávat informace o svém zdravotním stavu „náhradním způsobem“ za použití jiných právních předpisů, které by se informací o pacientovi mohly dotýkat, čímž je myšlen zejména, jak výše uvedeno, zákon o ochraně osobních údajů. Nyní existuje jasná právní úprava řešící uvedená práva, která však nevylučuje aplikaci práva na informace o osobních údajích upraveného zákonem o ochraně osobních údajů (zda se jedná o uplatnění práva na získání opisu, výpisu či kopie zdravotní dokumentace nebo práva na informace o zpracování osobních údajů bude třeba rozlišovat v jednotlivých případech dle obsahu žádosti).

Z nové právní úpravy provedené zákonem č. 111/2007 Sb. vyplývá, že pacient má právo určit osobu, která může být informována o jeho zdravotním stavu, a zároveň může rozhodnout o tom, zda této osobě náleží též právo nahlížet do zdravotnické dokumentace a právo na pořízení výpisů, opisů nebo kopií. Při tom platí, že pacient může určení osoby nebo vyslovení zákazu kdykoliv odvolat. Subjekt údajů (pacient) tak přímo určuje, komu a v jakém rozsahu mohou být informace (osobní údaje) poskytnuty a jaká práva na takto ustanovenou osobu převádí. Tento způsob dispozice je obdobný základnímu právu fyzické osoby rozhodovat o informacích o své osobě. Ostatně tento princip je včleněn do zákona o ochraně osobních údajů jako jeden ze základních principů ochrany osobních údajů, podle něhož je základním právem fyzické osoby rozhodovat o informacích o své osobě, které je naplněním základního práva na ochranu soukromí vyjádřeného v Listině základních práv a svobod.

Vyslovení zákazu podávání informací o zdravotním stavu podle § 67b odst. 12 se může vztahovat k jediné konkrétní osobě nebo se bude týkat všech osob. Zakotvení této výjimky (tj. zákazu poskytnutí informací) je nezbytné s ohledem na právo každého na ochranu soukromí ve vztahu k informacím o svém zdraví, jak je upraveno v čl. 10 odst. 1 Úmluvy o lidských právech a biomedicíně. Zákaz nahlížet do zdravotnické dokumentace však nikdy nemůže být absolutní, neboť vždy musí být zachován právní rámec povinností týkajících se podávání informací pro účely stanovené jak zákonem o péči o zdraví lidu (vyslovení zákazu se nemůže týkat práva nahlížet do zdravotnické dokumentace nebo jejích částí nebo pořizování výpisů, opisů nebo kopií podle § 67b odst. 10 a 11) nebo dále zvláštními právními předpisy. Zákaz nelze rovněž vztahovat na poučení o povaze onemocnění a o potřebných výkonech, které je lékař povinen osobám blízkým pacientovi, popřípadě členům jeho domácnosti poskytnout, neboť toto poučení je nezbytné pro jejich součinnost při poskytování zdravotní péče.[3)]

Způsob a postup při určení osoby, která bude informována o zdravotním stavu pacienta nebo při stanovení zákazu podávání informací, popřípadě odvolání určení osoby nebo zákazu podávání informací, upravuje přímo sám zákon o péči o zdraví lidu tak, že se pořídí záznam do zdravotnické dokumentace vedené o pacientovi a opatří podpisem ošetřujícího lékaře a pacienta. Jestliže však pacient nemůže s ohledem na svůj zdravotní stav záznam podepsat, ale je schopen projevit svou vůli, podepíše záznam svědek určený pacientem; svědkem v tomto případě může být pouze zletilá osoba způsobilá k právním úkonům v plném rozsahu. V záznamu je pak uveden způsob, jakým pacient svou vůli projevil, popřípadě zdravotní důvody, které zabránily pacientovi v podpisu. Bez ohledu na to, zda se jedná o výkon práva na informace pacienta, zákonného zástupce pacienta nebo jiné osoby, která může nahlížet do zdravotnické dokumentace, jejích částí nebo jiných zápisů vztahujících se ke zdravotnímu stavu pacienta, anebo si může pořizovat výpisy, opisy nebo kopie těchto dokumentů, musí zdravotnické zařízení vždy dodržet určitý postup, respektive pravidla stanovená zákonem.

Zdravotnické zařízení je povinno zajistit, aby oprávněné osoby, kterým je umožněno nahlížet do zdravotnické dokumentace a seznamovat se s informacemi v rozsahu stanoveném zvláštním zákonem, nemohly zjistit osobní údaje třetích osob (§ 67bb odst. 2). Zde je nepochybně přímý vztah k ustanovení § 13 zákona o ochraně osobních údajů, tj. k povinnosti přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.

Zákonným pravidlům rovněž podléhá pořízení výpisů, opisů nebo kopií zdravotnické dokumentace nebo jejích částí nebo jiných zápisů vztahujících se ke zdravotnímu stavu pacienta, jejichž vydání je zdravotnické zařízení povinno zajistit do 10 dnů ode dne obdržení žádosti, a to pro osoby uvedené v § 67b odst. 10 zákona o péči o zdraví lidu, tedy pro osoby, které mají ze zákona ke zdravotnické dokumentaci přístup, pokud není zvláštním právním předpisem stanoveno jinak nebo pokud není dohodnuta jiná lhůta. Delší lhůta, a to 30denní, platí pro žádost pacienta a jiné osoby, která má podle zákona právo na pořízení výpisů, opisů nebo kopií zdravotnické dokumentace nebo jejích částí. Zdravotnické zařízení může za pořízení výpisů, opisů nebo kopií zdravotnické dokumentace nebo jejích částí nebo jiných zápisů požadovat úhradu ve výši, která nesmí přesáhnout náklady spojené s jejich pořízením; to neplatí, je-li pořízení výpisů, opisů nebo kopií hrazeno z veřejného zdravotního pojiš-

---

[2)] K problémům z praxe č. 1/2002, Úřad pro ochranu osobních údajů, Výpisy ze zdravotní dokumentace.

[3)] Důvodová zpráva k návrhu zákona, kterým se mění zákon č. 20/1966 Sb. Sněmovní tisk 1045.

tění nebo na základě zvláštního právního předpisu. Tato právní úprava odpovídá ustanovení § 12 zákona o ochraně osobních údajů, tj. právu subjektu údajů na přístup k informacím (ve smyslu, že není v rozporu) a je k ní speciální.

Především z evidenčních důvodů je stanovena povinnost zaznamenávat každé nahlédnutí do zdravotnické dokumentace nebo jejích částí nebo pořízení jejích výpisů, opisů nebo kopií. V záznamu bude uvedeno: jméno, popřípadě jména, příjmení a datum narození osoby, která do zdravotnické dokumentace nebo jejích částí nahlédla nebo na jejíž žádost byl pořízen výpis, opis nebo kopie, dále rozsah, účel a datum nahlédnutí nebo pořízení výpisů, opisů nebo kopií. Stanovení těchto identifikačních údajů osoby je nepochybně konformní s principy ochrany osobních údajů. Záznam podepíše zdravotnický pracovník, který byl přítomen nahlížení do zdravotnické dokumentace nebo jejích částí nebo zdravotnický pracovník, který pořídil výpis, opis nebo kopii této zdravotnické dokumentace, a „nahlížející osoba".

Zvláštní právní úpravě podléhá rodné číslo pacienta. Ač je povinnou součástí zdravotnické dokumentace, lze jej poskytnout pouze osobám blízkým nebo osobám, které mají právo na informace podle § 67b odst. 12 zákona o péči o zdraví lidu, pokud tyto osoby prokáží, že jim pacient nebo jeho zákonný zástupce udělil na základě zvláštního právního předpisu upravujícího nakládání s rodnými čísly souhlas k využití jeho rodného čísla. Zvláštním právním předpisem je zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů, který jednak stanoví, že o užívání rodného čísla rozhoduje v zásadě jeho nositel (§ 13 odst. 7), respektive, že rodná čísla lze využívat jen v souladu s ustanovením § 13c odst. 1 zákona o evidenci obyvatel. V tomto případě se jedná o speciální případ, kdy lze rodné číslo využívat se souhlasem nositele.

Z á v ě r :

Z hlediska ochrany osobních údajů je zřejmé, že zákon č. 111/2007 Sb. přináší do této oblasti novou zvláštní úpravu, která se týká zejména pacienta, osob jemu blízkých a jejich práv na informace o zdravotním stavu, ale také povinností zdravotnických pracovníků při zabezpečování těchto práv pacienta a dalších osob zákonem stanovených.

Nová úprava však současně rozšiřuje možnosti pro předávání informací o zdravotním stavu, tedy citlivých osobních údajů, které podléhají speciální ochraně podle zákona o ochraně osobních údajů. Na základě platné právní úpravy bude nezbytné ze strany zdravotnických pracovníků a dalších osob, které s těmito citlivými osobními údaji budou přicházet do styku, řádné dodržování povinností vycházejících z nové právní úpravy podmínek vedení zdravotnické dokumentace a současně z příslušných ustanovení zákona o ochraně osobních údajů. Pozornost věnovaná dodržování povinností stanovených oběma výše uvedenými zákony by měla být o to větší, neboť se zde jedná o údaje o zdravotním stavu, tedy o údaje velmi citlivé. Patřičná ochrana těchto údajů je nezbytná i z toho důvodu, že její porušení lze bezesporu označit za velmi citelný zásah do soukromého a osobního života nejen samotného subjektu údajů, ale rovněž i dalších, jemu blízkých osob.

V souvislosti s vývojem technologií podporujících zpracovávání informací o zdravotním stavu pacienta je nyní možné vést zdravotnickou dokumentaci rovněž v elektronické podobě. S tím souvisí i řada dalších problémů a opatření, která je nezbytná přijmout k zabezpečení ochrany osobních údajů pacienta za současného umožnění přístupu dalším oprávněným osobám k těmto údajům.

Poznámka: Publikované stanovisko je k dispozici na internetové adrese Úřadu http://www.uoou.cz v rubrice Názory Úřadu.

III. SDĚLENÍ ÚŘADU

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ K PROBLÉMŮM Z PRAXE

č. 1/2007

září 2007

K problematice narušování soukromí prostřednictvím funkce hlasitého odposlechu mobilních telefonů

Funkce tzv. hlasitého odposlechu, která je v současné době součástí většiny nových modelů mobilních telefonů, s sebou nese otázky, do jaké míry ji lze zneužít pro narušení soukromí osob a pro porušení jejich práva na ochranu osobních údajů. Případy, kdy někdo nechá telefon s aktivovaným hlasitým odposlechem v jedné místnosti bez vědomí těch, kteří tam jsou a z jiné místnosti je může pomocí druhého telefonu poslouchat, jsou vnímány jako společensky nepřípustné a právem nedovolené.

Na otázku, nakolik je výše popsané soukromoprávní jednání porušením zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“) lze v zásadě aplikovat přístup vyjádřený ve Stanovisku Úřadu pro ochranu osobních údajů č. 1/2006 týkajícím se kamerových systémů.

I v případě použití hlasitého odposlechu mobilních telefonů k monitorování osob v zásadě platí, že o zpracování osobních údajů ve smyslu zákona o ochraně osobních údajů se jedná v případě, že informace ze zvukové stopy je zachycena na záznamové zařízení a nebo jinak zpracována. V případě, že se jedná o on-line odposlech bez zpracování zvukové stopy, se také může jednat o zásah do soukromí. Ten je však nutno řešit jinými právními předpisy, například zákonem č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů, který v ustanovení § 11 a násl. upravuje ochranu osobnosti.

Úřad již zodpovídal několik dotazů na možnost využívání hlasitého odposlechu rodiči k monitorování jejich dětí. I v tomto případě platí výše uvedené obecné zásady. Je však nutno dodat, že na takové případy se zákon o ochraně osobních údajů nevztahuje ani za situace, kdy je získaná zvuková stopa dále zaznamenávána či jinak zpracovávána. Uplatňuje se zde totiž ustanovení § 3 odst. 3 zákona o ochraně osobních údajů, které vyjímá z působnosti citovaného zákona takové zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu. Ani v tomto případě však nelze vyloučit ochranu soukromí podle jiných právních předpisů, např. podle výše uvedeného občanského zákoníku.

Poznámka: Publikovaný materiál je k dispozici na internetové adrese Úřadu http://www.uoou.cz v rubrice Názory Úřadu.

Společná koordinační skupina pro EURODAC – zpráva o koordinované inspekci

Sdělení úvodem:

Dne 17. července 2007 publikoval Evropský inspektor pro ochranu údajů (European Data Protection Supervisor, dále jen „EDPS“)[1] *zprávu společné koordinační skupiny o výsledcích inspekce systému EURODAC* [2]*. Úřad tímto předkládá informaci o uvedené zprávě.*

EURODAC je evropská databáze otisků prstů vytvořená na základě nařízení Rady (ES) č. 2725/2000 ze dne 11. prosince 2000 [3] *(dále jen „nařízení EURODAC“), s cílem napomáhat při určování, který členský stát EU je příslušný k posouzení žádosti o azyl, a současně usnadňovat naplňování společné azylové politiky.*

EDPS odpovídá za kontrolu činnosti centrální jednotky systému EURODAC (zřízeného při Evropské komisi). Je garantem, že při využívání tohoto systému nedochází k porušování práv žadatelů o azyl (zejména práva na ochranu před nezákonným zpracováním osobních údajů a souvisejícího práva na ochranu soukromí). V každé členské zemi je dále dohledem nad využíváním osobních údajů uchovávaných v systému EURODAC pověřen nezávislý dozorový úřad (v České republice je jím Úřad pro ochranu osobních údajů).

EDPS při výkonu dohledu nad EURODAC úzce spolupracuje s jednotlivými národními dozorovými úřady, zejména prostřednictvím společné koordinační skupiny, kterou za tímto účelem pravidelně svolává. Výsledkem činnosti této skupiny je i zmíněná zpráva o výsledcích inspekce systému EURODAC.

Koordinovaná inspekce

Vzhledem ke struktuře systému EURODAC (centrální databáze a síť národních přístupových míst) je zřejmé, že efektivní kontrolu zpracování osobních údajů lze provést pouze v součinnosti EDPS a národních dozorových úřadů, na obou úrovních současně. V praxi byl v daném případě vypracován stručný seznam problematických oblastí, které byly nejprve prověřeny na národní úrovni (formou dotazníků směřovaných na příslušné orgány) v každém členském státě, tedy i v ČR, a následně předloženy EDPS.

---

[1] Více informací o činnosti Evropského inspektora viz www.edps.europa.eu .

[2] Celá zpráva je (v anglickém jazyce) zpřístupněna na webových stránkách EDPS (viz http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/39) a také na webových stránkách Úřadu pro ochranu osobních údajů (www.uoou.cz).

[3] Nařízení Rady (ES) č. 2725/2000 ze dne 11. prosince 2000 o zřízení systému „EURODAC“ pro porovnávání otisků prstů za účelem účinného uplatňování Dublinské úmluvy.

Oblasti, na které byla koordinovaná inspekce zaměřena:

1. využití tzv. zvláštního vyhledávání (tj. konzultace systému EURODAC na základě práva přístupu k údajům uplatněného osobou, která se domnívá, že její údaje jsou v tomto informačním systému zpracovávány),
2. případné využití údajů z EURODAC k jiným účelům než stanoveným v citovaném nařízení Rady (č. 2725/2000),
3. technická kvalita údajů (otisků prstů).

Zvláštní vyhledávání

Právo přístupu k údajům o své osobě je jedním ze základních principů ochrany osobních údajů, který je uplatňován napříč veškerou legislativou EU (i národními právními předpisy). Projevem tohoto práva ve vztahu k systému EURODAC je možnost každého občana požadovat informaci o tom, zda jsou jeho osobní údaje v tomto systému zaznamenány a pokud ano, o jaké údaje se jedná, kdy a kým byly vloženy apod. Vzhledem k tomu, že dotaz do EURODAC v tomto případě není standardním využitím této databáze (ačkoli je zcela v souladu s nařízením EURODAC), je pro tento postup užíván výraz „zvláštní vyhledávání". Důvodem zaměření inspekce na tento druh využití EURODAC byly značné statistické rozdíly mezi jednotlivými členskými státy a zejména velký počet těchto dotazů v některých zemích, indikující odlišný přístup k tomuto způsobu využití EURODAC, případně až zneužití k jiným účelům (např. lustrování osob, na které se nařízení EURODAC nevztahuje, pod záminkou, že se jedná o osoby, které uplatnily své právo přístupu k údajům).

Závěry inspekce v této oblasti jsou takové, že v případě, kdy nebyla kategorie „zvláštní vyhledávání" využita v souladu s nařízením EURODAC (tj. obvykle nebylo možné doložit existenci dotazu subjektu údajů), jednalo se vedle chyb personálu o využití pro školení uživatelů a pro testování systému. Současně bylo konstatováno, že se ve všech zjištěných případech chybného využití EURODAC jednalo o chyby učiněné v dobré víře, přičemž na základě této inspekce došlo (prostřednictvím národních dozorových orgánů pro ochranu osobních údajů) ve většině případů k upozornění na závadný stav, popř. k nápravě nevhodných postupů.

Využití k jiným účelům

Účel, k němuž má systém EURODAC (tj. údaje v něm uložené) sloužit, je jasně stanoven v čl. 1 odst. 1 nařízení EURODAC a je jím pomoc při určování členského státu, který je příslušný pro posouzení žádosti o azyl podané v některém z členských států a také jinak usnadňovat uplatňování společné azylové politiky EU. Systém EURODAC není přípustné (pod hrozbou sankce) využít k jiným účelům, než k prosazování azylové politiky příslušnými orgány. Vzhledem k tomu, že v některých členských zemích je tento systém provozován v rámci policejních složek, byla na místě otázka, zda je zmíněná limitace jeho využití důsledně uplatňována také v praxi.

Z této části inspekce vyplynulo zjištění, že ačkoli je EURODAC v mnoha státech provozován (zcela nebo částečně) v rámci policie, nebylo zjištěno žádné zneužití systému vyplývající z tohoto uspořádání. Jako jisté riziko se může dle předmětné zprávy jevit situace v některých zemích, kde je do procesu odebírání, odesílání a komparace otisků prstů zainteresováno více orgánů, a kde v důsledku roztříštění odpovědnosti za zpracování osobních údajů mohou být tyto údaje ohroženy. Obecně však zpráva konstatuje, že v souvislosti s respektováním daného účelu databáze nebo s přístupem neoprávněných subjektů nebyly zjištěny významné problémy.

Kvalita otisků prstů

Kvalita a správnost údajů je jedním ze základních principů (vyjádřených i v nařízení EURODAC) při zpracování osobních údajů, otisky prstů nevyjímaje. Důvodem zaměření inspekce na tuto oblast byla snaha dosáhnout snížení počtu odmítnutých vkládaných dat (otisků) z důvodu jejich nízké kvality, který se v době kontroly pohyboval zhruba na úrovni 6%. Z tohoto důvodu se jevilo vhodné zjistit, jaká technická zařízení jednotlivé země používají, jaké mají zkušenosti nebo s jakými překážkami se setkaly. Současně byla sledována i možnost výměny zkušeností mezi státy, které vykazují vyšší míru odmítnutých záznamů, se státy, u nichž je tato hodnota nižší.

Tato část inspekce, logicky, poukázala mimo jiné na výhody nových technických řešení (optické scannery), jejichž prostřednictvím odebrané otisky vykazují obecně vyšší kvalitu. Důležitým závěrem však byl i fakt, že minimálně stejnou pozornost jako technickému vybavení je nutno věnovat školení personálu v zacházení s přístroji pro odebírání otisků prstů. Samostatnou a stále výraznější problematiku představují osoby, jimž nelze z nejrůznějších důvodů (invalidita, věk, záměrné poškození apod.) otisky odebrat – řešení těchto situací je nutno dle prezentované zprávy věnovat zvýšenou pozornost.

Závěr:

Výše nastíněné závěry jsou ve společné zprávě shrnuty do doporučení pro každou ze sledovaných oblastí.

Závěrem lze uvést, že předmětná zpráva EDPS a koordinační skupiny byla publikována ve stejné době, kdy Evropská komise vydala svoji hodnotící zprávu týkající se implementace a funkčnosti tzv. Dublinského systému[4)] (tzn. opatření vyplývající z Dublinské úmluvy, respektive právních předpisů, které ji nahrazují[5)]), který zahrnuje i systém EURODAC. Zpráva o koordinované inspekci EURODAC hodnotící zprávu Komise vhodně doplňuje o aspekty z oblasti ochrany osobních údajů.

[4)] Report From the Commission to the European Parliament and the Council on the evaluation of the Dublin system, Brussels, 6. 6. 2007, COM(2007) 299 final (text v anglickém jazyce viz http://ec.europa.eu/commission_barroso/frattini/doc/2007/com_2007_299_en.pdf).

[5)] Úmluva o určení státu příslušného pro posuzování žádosti o azyl podané v některém z členských států Evropských společenství („Dublinská úmluva"). Nařízení Rady (ES) č. 343/2003 ze dne 18. února 2003, kterým se stanoví kriteria a postupy pro určení členského státu příslušného k posuzování žádosti o azyl podané státním příslušníkem třetí země v některém z členských států a Nařízení Komise (ES) č. 1560/2003 ze dne 2. září 2003, kterým se stanoví prováděcí pravidla k nařízení Rady (ES) č. 343/2003 (tato nařízení jsou běžně označována jako „Dublin II").

PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

01248/07/CS
WP 136

Stanovisko č. 4/2007 k pojmu osobní údaje

přijaté dne 20. června 2007

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jde o nezávislý evropský poradní orgán pro ochranu údajů a soukromí. Jeho úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát skupiny zajišťuje ředitelství C (Civilní soudnictví, práva a občanství) Generálního ředitelství pro spravedlnost, svobodu a bezpečnost Evropské komise, B-1049 Brusel, Belgie, kancelář č. LX-46 01/43.

Internetová stránka: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995[1],

s ohledem na článek 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice a čl. 15 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002,

s ohledem na článek 255 Smlouvy o ES a na nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise,

s ohledem na svůj jednací řád,

PŘIJALA TOTO STANOVISKO:

[1] Úřední věstník L 281, 23.11.1995, s. 31; dostupná na adrese: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.

I. ÚVOD 3

II. OBECNÉ ÚVAHY A POLITICKÉ OTÁZKY 4

III. ANALÝZA DEFINICE POJMU „OSOBNÍ ÚDAJE“ PODLE SMĚRNICE O OCHRANĚ ÚDAJŮ 5

1. PRVNÍ SLOŽKA: „VEŠKERÉ INFORMACE“ 6

2. DRUHÁ SLOŽKA: „O“ (VZTAH MEZI INFORMACEMI A OSOBOU) 9

3. TŘETÍ SLOŽKA: „IDENTIFIKOVANÁ NEBO IDENTIFIKOVATELNÁ“ (FYZICKÁ OSOBA) 12

4. ČTVRTÁ SLOŽKA: (FYZICKÁ) „OSOBA“ 21

IV. CO SE STANE, KDYŽ SE NA ÚDAJE DEFINICE NEVZTAHUJE? 24

V. ZÁVĚRY 25

I. ÚVOD

Pracovní skupina si uvědomuje potřebu provést hloubkovou analýzu pojmu osobní údaje. Z informací o současné praxi v členských státech EU vyplývá, že mezi členskými státy existuje ohledně důležitých aspektů tohoto pojmu určitá nejistota a rozdílnost v přístupech, což může v různých souvislostech nepříznivě ovlivnit řádné fungování stávajícího rámce ochrany údajů. Výsledek této analýzy jednoho z ústředních prvků z hlediska používání a výkladu pravidel ochrany údajů bude mít nutně zásadní vliv na řadu důležitých otázek. Zvláštní význam pak bude mít pro témata, jako je správa identit v rámci elektronické veřejné správy (e-Government) a elektronického zdravotnictví (e-Health), jakož i v souvislosti s identifikací na základě rádiové frekvence (RFID).

Cílem tohoto stanoviska pracovní skupiny je dosáhnout společného porozumění pojmu osobní údaje, situacím, v nichž by se měly používat vnitrostátní právní předpisy o ochraně údajů, a správnému způsobu jejich použití. Pracovat na společné definici pojmu osobní údaje znamená vymezit, co spadá a co nespadá do působnosti pravidel ochrany údajů. Dalším výsledkem této práce bude poskytnutí vodítka k tomu, jak by se měla vnitrostátní pravidla ochrany údajů používat v určitých kategoriích situací, jež se vyskytují v celé Evropě. Tím pracovní skupina zřízená podle článku 29 přispěje k jednotnému používání těchto norem, což patří k jejím hlavním úkolům.

V tomto dokumentu jsou na podporu a pro ilustraci analýzy použity příklady z vnitrostátní praxe evropských orgánů pro ochranu údajů. Většina příkladů byla upravena pouze s ohledem na vhodnost použití v tomto kontextu.

II. OBECNÉ ÚVAHY A POLITICKÉ OTÁZKY

Směrnice obsahuje široké pojetí osobních údajů.

Definice osobních údajů uvedená ve směrnici 95/46/ES (dále jen „směrnice o ochraně údajů“ nebo „směrnice“) zní takto:

„Osobními údaji (se rozumí) *veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity.“*

Zde je třeba poznamenat, že tato definice odráží úmysl evropského zákonodárce směřující k širokému pojetí „osobních údajů“, který trval v průběhu celého legislativního procesu. V původním návrhu Komise je vysvětleno, že „*stejně jako v Úmluvě 108 se přijímá široká definice s cílem zahrnout veškeré informace, které mohou souviset s jednotlivcem*“[2]. V pozměněném návrhu Komise se uvádí, že „*pozměněný návrh odpovídá přání Parlamentu, aby definice „osobních údajů“ byla co nejobecnější, a tedy zahrnovala veškeré informace o identifikovatelném jednotlivci*“[3], a toto přání vzala v potaz i Rada ve svém společném postoji[4].

Cílem pravidel obsažených ve směrnici je ochrana jednotlivců.

V článku 1 směrnice 95/46/ES a článku 1 směrnice 2002/58/ES je jasně stanoven konečný účel pravidel obsažených v těchto směrnicích: ochrana základních práv a svobod fyzických osob, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů. To je velmi důležitý prvek, který je třeba brát v úvahu při výkladu a používání pravidel obou právních nástrojů. Podstatnou úlohu může hrát při rozhodování o tom, jak ustanovení směrnice používat v řadě situací, v nichž práva jednotlivců nejsou ohrožena, a může také varovat před jakýmkoli výkladem těchto pravidel, který by jednotlivce o ochranu jejich práv připravoval.

Z oblasti použití směrnice je vyloučena řada činností a její znění počítá s pružností umožňující vhodnou právní reakci na okolnosti, které mohou nastat.

Navzdory širokému pojetí pojmů „osobní údaje“ a „zpracování“ ve směrnici pouhá skutečnost, že lze nějakou situaci považovat za situaci zahrnující „zpracování osobních údajů“ ve smyslu příslušné definice, bez dalšího neznamená, že se na tuto situaci mají vztahovat pravidla směrnice. To je dáno především článkem 3 této směrnice. Kromě výjimek vyplývajících z působnosti práva Společenství jsou u výjimek podle článku 3 zohledněny také technický způsob zpracování (manuální neuspořádané záznamy) a záměr, pro který se údaje používají (výlučně osobní či domácí činnosti fyzické osoby). Pro určitý konkrétní případ nemusejí být použitelná všechna pravidla obsažená ve směrnici ani tehdy, jedná-li se o zpracování osobních údajů spadající do oblasti její působnosti. Řada ustanovení směrnice obsahuje značnou míru pružnosti, aby bylo dosaženo vhodné rovnováhy mezi ochranou práv subjektu údajů na jedné straně a legitimními zájmy správců údajů a třetích osob, jakož i případným veřejným zájmem, na straně druhé. Z mnoha případů takových ustanovení lze uvést například článek 6

[2] KOM(90) 314 v konečném znění, 13.9.1990, s. 19 (komentář k článku 2).
[3] KOM(92) 422 v konečném znění, 28.10.1992, s. 10 (komentář k článku 2).
[4] Společný postoj (ES) č. 1/95 přijatý Radou dne 20. února 1995, Úř. věst. C 93, 13.4.1995, s. 20.

(doba uchování údajů závisející na jejich nezbytnosti), čl. 7 písm. f) (zpracování údajů opodstatněné rovnováhou zájmů), poslední část čl. 10 písm. c) a poslední část čl. 11 odst. 1 písm. c) (informování subjektu údajů, je-li to nezbytné pro zajištění řádného zpracování) či článek 18 (výjimky z oznamovací povinnosti).

Oblast působnosti pravidel ochrany údajů by se neměla nadměrně rozšiřovat.

Nežádoucím výsledkem by bylo, kdyby se pravidla ochrany údajů používala v situacích, na které se podle původního záměru nemají vztahovat a pro které je zákonodárce nevytvořil. Způsob ochrany údajů, který chtěl zákonodárce zavést, je patrný z výše uvedených hmotněprávních výjimek podle článku 3 směrnice a z vysvětlení ve 26. a 27. bodu jejího odůvodnění.

Jedno omezení se týká způsobu zpracování údajů. V tomto ohledu je užitečné připomenout, že důvody přijetí prvních právních předpisů na ochranu údajů v sedmdesátých letech vyplývaly z toho, že nová technologie v podobě elektronického zpracování údajů umožňuje snadnější a širší přístup k osobním údajům než tradiční způsoby práce s údaji. Ochrana údajů podle směrnice je proto zaměřena na způsoby zpracování, pro něž je typické vyšší riziko „snadného přístupu k osobním údajům“ (27. bod odůvodnění). Zpracování osobních údajů neautomatizovanými postupy je do oblasti působnosti směrnice zahrnuto pouze v případě, že jsou údaje obsaženy v rejstříku nebo do něj mají být zařazeny (článek 3).

Další obecné omezení pro použití ochrany údajů podle směrnice se týká zpracování údajů za okolností, kdy o prostředcích pro identifikaci subjektu údajů neplatí, že „mohou být rozumně použity“ (26. bod odůvodnění). Touto otázkou se zabývá samostatná část tohoto stanoviska.

Je však třeba se vyvarovat také nepatřičného zužování výkladu pojmu osobní údaje.

V případech, kdy by mechanické použití každého jednotlivého ustanovení směrnice na první pohled vedlo k nadměrně zatěžujícím, či dokonce absurdním důsledkům, je třeba nejprve zkontrolovat, 1) zda situace spadá do oblasti působnosti směrnice, zvláště podle jejího článku 3 a, 2) pokud do její oblasti působnosti spadá, zda sama směrnice nebo na jejím základě přijaté vnitrostátní právní předpisy nepočítají s výjimkami nebo zjednodušeními s ohledem na zvláštní situace v zájmu dosažení vhodné právní reakce při současném zajištění ochrany práv jednotlivce a příslušných zájmů. Lepší možnost než nepatřičně zužovat výklad definice osobních údajů je uvědomit si, že při používání pravidel pro tyto údaje je k dispozici značná pružnost.

V tomto ohledu hrají zásadní úlohu vnitrostátní orgány dozoru nad ochranou údajů, a to v rámci svého úkolu sledovat používání právních předpisů o ochraně údajů, který zahrnuje podávání výkladu právních ustanovení a vydávání konkrétních pokynů pro správce a subjekty údajů. Tyto orgány by měly podporovat definici natolik širokou, aby dokázala předjímat další vývoj a aby její rozsah zahrnoval všechny „šedé zóny“, a zároveň by měly legitimně využívat pružnost, která je ve směrnici obsažena. Znění směrnice totiž vyzývá k vypracování politiky spojující široký výklad pojmu osobní údaje s vhodnou rovnováhou při používání pravidel směrnice.

III. ANALÝZA DEFINICE POJMU „OSOBNÍ ÚDAJE“ PODLE SMĚRNICE O OCHRANĚ ÚDAJŮ

Definice uvedená ve směrnici má čtyři hlavní složky, které jsou v tomto stanovisku analyzovány odděleně. Jedná se o tyto složky:

- „veškeré informace“,
- „o“ (vztah mezi informacemi a osobou),
- „identifikovaná nebo identifikovatelná“,
- (fyzická) „osoba“.

Uvedené čtyři složky jsou těsně provázány a vzájemně se podporují. Kvůli metodice použité v tomto stanovisku se však každou z nich zabýváme odděleně.

1. PRVNÍ SLOŽKA: „VEŠKERÉ INFORMACE“

Výraz „veškeré informace“ použitý ve směrnici jasně signalizuje záměr zákonodárce definovat pojem osobní údaje široce. Toto znění vyžaduje širokou interpretaci.

Z hlediska povahy informací pojem osobní údaje zahrnuje všechny druhy tvrzení o osobě. Zahrnuje tedy jak „objektivní“ informace, jako je přítomnost určité látky v krvi, tak „subjektivní“ informace, názory či hodnocení. Na druhý z uvedených typů tvrzení připadá značný podíl osobních údajů zpracovávaných například v bankovnictví pro účely posouzení spolehlivosti dlužníků („Titius je spolehlivý dlužník“), v pojišťovnictví („není pravděpodobné, že Titius brzy zemře“) nebo v souvislosti se zaměstnáním („Titius je dobrý pracovník a zaslouží si povýšení“).

Informace mohou být „osobními údaji“ bez ohledu na to, zda jsou pravdivé či prokázané. Pravidla ochrany údajů ve skutečnosti počítají s tím, že informace mohou být nesprávné, a stanovují právo subjektu údajů mít k těmto informacím přístup a napadnout je pomocí vhodných prostředků pro zajištění nápravy[5].

Z hlediska obsahu informací se pojem osobní údaje vztahuje na údaje poskytující libovolný typ informací. Patří sem samozřejmě osobní informace považované za „citlivé údaje“ podle článku 8 směrnice kvůli jejich zvláště rizikové povaze, ale i obecnější druhy informací. Výraz „osobní údaje“ označuje informace dotýkající se soukromého a rodinného života jednotlivce v úzkém smyslu, ale také informace o jakémkoli druhu činnosti, kterou se jednotlivec zabývá, například informace o jeho pracovních vztazích nebo ekonomickém či společenském chování. Zahrnuje tudíž informace o jednotlivcích bez ohledu na postavení nebo roli, v jaké daná osoba vystupuje (spotřebitel, pacient, zaměstnanec, zákazník atd.).

Příklad č. 1: profesní zvyklosti a postupy

Informace o předepisování léků (např. identifikační číslo léčivého přípravku, název léku, obsah účinné látky, výrobce, prodejní cena, informace, zda jde o první nebo opakovaný předpis na daný lék, důvody pro nasazení léku, odůvodnění zákazu nahrazení léku jiným lékem, jméno a příjmení předepisujícího lékaře, telefonní číslo atd.), ať v podobě jednotlivého předpisu nebo informací o způsobu předepisování získaných z většího počtu předpisů, lze považovat za osobní údaje o lékaři, který daný

[5] Opravu lze provést připojením opačných tvrzení nebo pomocí příslušných právních nástrojů, jako jsou mechanismy opravných prostředků.

lék předepisuje, přestože pacient je anonymní. Poskytování informací o předpisech vystavených identifikovanými nebo identifikovatelnými lékaři výrobcům léků na předpis tak představuje sdělování osobních údajů třetím osobám ve smyslu směrnice.

Tento výklad je podpořen samotným zněním směrnice. Na jedné straně je třeba vzít v úvahu, že soukromý a rodinný život je široký pojem, jak jasně stanovil Evropský soud pro lidská práva[6]. Na druhé straně jdou pravidla pro ochranu osobních údajů nad rámec ochrany uvedeného širokého pojetí práva na respektování soukromého a rodinného života. Je třeba poznamenat, že v Listině základních práv Evropské unie je ochrana osobních údajů zakotvena v článku 8 jakožto autonomní právo, které je oddělené a odlišné od práva na soukromý život uvedeného v článku 7 Listiny, a totéž platí v některých členských státech na vnitrostátní úrovni. Tomu odpovídá znění čl. 1 odst. 1 směrnice, jehož účelem je zajistit ochranu „základních práv a svobod fyzických osob, *zejména* [ale nikoli výlučně] jejich soukromí". V souladu s tím směrnice výslovně zmiňuje zpracování osobních údajů mimo rámec domácího a rodinného prostředí, například zpracování stanovené pracovněprávními předpisy (čl. 8 odst. 2 písm. b)), zpracování v souvislosti s rozsudky v trestních věcech, správními sankcemi nebo rozsudky v občanských věcech (čl. 8 odst. 5) či zpracování pro účely přímého marketingu (čl. 14 písm. b)). Tento široký přístup podpořil i Evropský soudní dvůr.[7]

Pokud jde o formát informací a nosič, který je obsahuje, zahrnuje pojem osobní údaje informace bez ohledu na formu, v jaké jsou k dispozici. Mohou mít tedy například textovou, číselnou, grafickou, fotografickou či zvukovou podobu. Patří sem mimo jiné informace na papíře stejně jako informace uložené v paměti počítače pomocí binárního kódu nebo informace na videokazetě. To logicky vyplývá ze skutečnosti, že se tento pojem vztahuje na automatické zpracování osobních údajů. Zvláště je z tohoto hlediska za osobní údaje třeba považovat zvukové a obrazové údaje, a to v míře, v jaké mohou představovat informace o jednotlivci. V tomto ohledu musí být konkrétní odkaz na údaje tvořené zvuky nebo obrazy v článku 33 směrnice chápán jako potvrzení a objasnění toho, že tento druh údajů pod uvedený pojem skutečně spadá (za předpokladu splnění všech ostatních podmínek) a že se na něj směrnice vztahuje. Jedná se o logický předpoklad ohledně ustanovení v uvedeném článku, kde je účelem posouzení otázky, zda pravidla směrnice představují vhodnou právní reakci v těchto oblastech. Tuto záležitost dále objasňuje 14. bod odůvodnění, v němž se uvádí, že „*s ohledem na význam současného rozvoje technologií pro příjem, přenos, úpravu, zaznamenání, uchování či sdělování zvukových a obrazových údajů týkajících se fyzických osob v rámci informační společnosti se tato směrnice použije i na zpracování těchto údajů*". Na druhé straně mohou být informace pokládány za osobní údaje, i když nejsou obsaženy v uspořádané databázi nebo záznamu. Jsou-li splněna další kritéria definice osobních údajů, mohou být jako osobní údaje klasifikovány rovněž informace

---

6 Rozsudek Evropského soudu pro lidská práva ve věci Amann v. Švýcarsko ze dne 16. února 2000, bod 65: „*(...) výraz „soukromý život" se nesmí vykládat restriktivně. Respektování soukromého života zahrnuje zejména právo navazovat a rozvíjet vztahy s ostatními lidmi; navíc neexistuje žádný zásadní důvod, který by ospravedlňoval vyloučení činností profesní nebo pracovní povahy z pojmu „soukromý život" (viz rozsudek ve věci Niemietz v. Německo ze dne 16. prosince 1992, řada A, č. 251-B, bod 29, s. 33–34 a výše uvedený rozsudek ve věci Halford, bod 42, s. 1015–1016). Tento široký výklad odpovídá výkladu obsaženému v Úmluvě Rady Evropy ze dne 28. ledna 1981 (...)*"

7 Rozsudek Evropského soudního dvora ve věci C-101/2001 (Lindqvist) ze dne 6. listopadu 2003, bod 24: „*Výraz osobní údaje použitý v čl. 3 odst. 1 směrnice 95/46 zahrnuje podle definice v čl. 2 písm. a) této směrnice veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Tento výraz nepochybně zahrnuje jméno osoby ve spojení s jejím telefonním číslem či informacemi o jejích pracovních podmínkách nebo zájmových činnostech.*"

ve volném textu elektronického dokumentu. „Osobní údaje“ tak mohou být obsaženy například ve zprávě elektronické pošty.

Příklad č. 2: telefonní bankovnictví

Jestliže je v rámci telefonního bankovnictví nahráván na pásku hlas zákazníka, který dává pokyny bance, nahrávky těchto pokynů by se měly považovat za osobní údaje.

Příklad č. 3: dohled pomocí videokamer

Obrazové záznamy jednotlivců zachycené systémem dohledu pomocí videokamer mohou být osobními údaji v té míře, do jaké je na nich tyto jednotlivce možné poznat.

Příklad č. 4: dětská kresba

Na základě neurologicko-psychiatrického vyšetření dívky, které se provede v rámci soudního řízení o tom, komu má být svěřena do péče, je předložena dívčina kresba představující její rodinu. Kresba poskytuje informace o její náladě a jejích pocitech vůči různým rodinným příslušníkům. Z toho důvodu lze výkres považovat za „osobní údaje“. Kresba skutečně podává informace o dítěti (o jeho duševním zdraví) a například také o chování jeho otce či matky. V důsledku toho mohou mít rodiče v tomto případě možnost uplatnit právo na přístup k této konkrétní informaci.

Zde je třeba se samostatně zmínit o biometrických údajích. Tyto údaje lze definovat jako biologické vlastnosti, fyziologické rysy, znaky živého organismu nebo opakovatelné úkony, které jsou jedinečné pro daného jednotlivce a současně měřitelné, bez ohledu na to, že technické metody jejich měření používané v praxi zahrnují určitou míru pravděpodobnosti. K typickým příkladům biometrických údajů patří otisky prstů, struktura sítnice, struktura obličeje či hlas, ale také geometrie ruky, struktura žil, nebo dokonce některé hluboce zakořeněné dovednosti či jiné behaviorální rysy (například vlastnoruční podpis, úhozy na klávesnici, charakteristický způsob chůze nebo řeči atd.).

Biometrické údaje jsou zvláštní tím, že je lze považovat jak za *obsah* informace o určitém jednotlivci (Titius má tyto otisky prstů), tak za prvek uvádějící nějakou informaci do *souvislosti* s tímto jednotlivcem (tohoto předmětu se dotkl někdo s těmito otisky prstů a tyto otisky prstů odpovídají Titiovým; tohoto předmětu se tudíž dotkl Titius). Z tohoto důvodu mohou fungovat jako „identifikátory“. Vzhledem k tomu, že mají jedinečnou souvislost s konkrétním jednotlivcem, mohou biometrické údaje sloužit k identifikaci tohoto jednotlivce. Uvedenou dvojí povahu mají také údaje o DNA, které podávají informace o lidském těle a umožňují jednoznačnou a jedinečnou identifikaci osoby.

Vzorky lidských tkání (například krve) jsou zdrojem, z něhož jsou biometrické údaje získávány, ale samy biometrickými údaji nejsou (podobně jako je biometrickým údajem vzor otisku prstu, avšak nikoli sám prst). Získávání informací ze vzorků tkání je proto shromažďováním osobních údajů, na které se vztahují pravidla směrnice. Shromažďování, uchovávání a využívání samotných vzorků tkání může podléhat samostatným souborům pravidel.[8]

[8] Viz doporučení Výboru ministrů Rady Evropy členským státům č. Rec (2006) 4 ze dne 15. března 2006 o výzkumu biologických materiálů lidského původu.

2. DRUHÁ SLOŽKA: „O“ (VZTAH MEZI INFORMACEMI A OSOBOU)

Tato složka definice je zásadní, protože je velmi důležité přesně zjistit, na kterých vztazích či souvislostech záleží a jak by se měly rozlišovat.

Obecně lze mít za to, že se informace nějakého jednotlivce „týkají“, pokud jsou o tomto jednotlivci.

V mnoha situacích lze tento vztah stanovit snadno. Například údaje evidované v osobním spisu v personálním oddělení se zjevně „týkají“ postavení dané osoby jakožto zaměstnance. Obdobně je to s údaji ve výsledcích lékařského testu pacienta, které jsou součástí jeho lékařských záznamů, nebo s obrazem osoby, se kterou byl natočen rozhovor na video.

Je ovšem možné uvést řadu jiných situací, u nichž nelze vždy stanovit, že se informace „týkají“ jednotlivce, se stejnou samozřejmostí jako v předchozích případech.

V některých situacích se informace, které údaje poskytují, týkají v první řadě věcí, a nikoli jednotlivců. Tyto věci obvykle někomu patří nebo mohou být určitým způsobem ovlivňovány jednotlivci nebo mít naopak vliv na jednotlivce, případně se mohou nějak nacházet ve fyzické či zeměpisné blízkosti jednotlivců nebo jiných věcí. V takovém případě je třeba mít za to, že se informace těchto jednotlivců nebo jiných věcí týkají jen nepřímo.

Příklad č. 5: hodnota domu

Hodnota konkrétního domu je informací o věci. Pokud tato informace bude sloužit pouze pro ilustraci cenové hladiny nemovitostí v nějakém okrese, pravidla ochrany údajů se nepochybně nepoužijí. Za určitých okolností by se však takové informace také měly považovat za osobní údaje. Dům je totiž majetkem svého vlastníka, a informace o něm se tudíž může použít například k vyměření nějaké daňové povinnosti této osoby. V této souvislosti by se taková informace bezpochyby měla považovat za osobní údaj.

Stejným způsobem lze analyzovat situaci, kdy se údaje týkají v první řadě procesů nebo událostí, například jedná-li se o informace o fungování stroje, který vyžaduje lidské zásahy. I zde lze mít za určitých okolností za to, že se tyto informace „týkají“ jednotlivce.

Příklad č. 6: servisní záznamy o automobilu

Servisní záznamy o automobilu, které má v držení automechanik nebo autoopravna, obsahují informace o daném vozidle, počtu ujetých kilometrů, datech servisních prohlídek, technických problémech a stavu materiálu. Tyto informace jsou v záznamech přiřazeny ke státní poznávací značce a číslu motoru, které lze uvést do souvislosti s majitelem. Jestliže autoopravna uvede vozidlo do souvislosti s majitelem pro účely fakturace, informace se budou „týkat“ majitele nebo řidiče. Je-li automobil uveden do souvislosti s automechanikem, který na něm pracoval, za účelem posouzení produktivity daného pracovníka, tyto informace se budou „týkat“ také tohoto automechanika.

Otázce, kdy lze informace pokládat za informace „týkající se“ osoby, již pracovní skupina věnovala pozornost. V rámci diskuzí o otázkách ochrany údajů souvisejících se štítky RFID pracovní skupina konstatovala, že „*údaje se týkají jednotlivce, jestliže se vztahují k totožnosti, charakteristickým znakům či chování jednotlivce nebo pokud použití těchto informací určuje nebo ovlivňuje způsob zacházení s touto osobou nebo způsob jejího hodnocení*[9]“.

Vzhledem k výše uvedeným případům by se ve stejném duchu dalo říci, že aby bylo možné údaje považovat za údaje, které se „týkají“ jednotlivce, měl by být přítomen prvek „**obsahu**“ NEBO prvek „**účelu**“ NEBO prvek „**výsledku**“.

Prvek „**obsahu**“ je přítomen v případech, kdy – v souladu s nejzjevnějším a nejběžnějším chápáním výrazu „týkat se“ ve společnosti – se informace podávají o konkrétní osobě, a to bez ohledu na jakýkoli účel, který sleduje správce údajů nebo třetí osoba, nebo na dopad těchto informací na subjekt údajů. Informace se „týkají“ nějaké osoby, jsou-li „o“ této osobě, a to je nutné posuzovat ve světle všech okolností daného případu. Výsledky lékařského rozboru se například jasně týkají pacienta a informace ve firemní složce uvedené pod jménem určitého klienta se jasně týkají tohoto klienta. Stejně tak se určité osoby týkají informace obsažené ve štítku RFID nebo čárovém kódu, který je součástí jejího dokladu totožnosti. Tak tomu bude například u budoucích cestovních pasů s čipem RFID.

Skutečnost, že se informace „týkají“ určité osoby, může vyplývat také z jejich „**účelu**“. Existenci tohoto prvku „účelu“ lze předpokládat, jestliže – při zohlednění všech okolností daného konkrétního případu – je účelem, za kterým se údaje používají nebo pravděpodobně budou používat, hodnotit jednotlivce, zacházet s ním určitým způsobem nebo ovlivnit jeho postavení či chování.

[9] Dokument pracovní skupiny č. WP 105: „Pracovní dokument o otázkách ochrany údajů souvisejících s technologií RFID“, přijatý dne 19. ledna 2005, s. 8.

Příklad č. 7: záznam hovorů z telefonu

Záznam hovorů z telefonního přístroje umístěného v kanceláři podniku poskytuje informace o hovorech provedených z tohoto telefonu, který je připojen k určité telefonní lince. Tyto informace mohou být uvedeny do souvislosti s různými subjekty. Linka byla dána k dispozici podniku a ten má také smluvní povinnost za hovory platit. V pracovní době je telefonní přístroj pod kontrolou určitého zaměstnance, který by z něj měl telefonovat. Záznam hovorů může obsahovat také informace o volaných osobách. Telefon mohou používat rovněž osoby, které mají do budovy případně přístup za nepřítomnosti daného zaměstnance (např. pracovníci úklidu). Informace o používání tohoto telefonního přístroje tak mohou být pro různé účely vztaženy k podniku, k uvedenému zaměstnanci nebo k pracovníkům úklidu (například pro kontrolu času, kdy tito pracovníci opouštějí pracoviště, protože mají povinnost telefonicky potvrzovat čas svého odchodu před zamknutím budovy). Je třeba uvést, že pojem osobní údaje se zde vztahuje jak na odchozí, tak na příchozí hovory, a to do té míry, do jaké obsahují informace o soukromém životě lidí, jejich společenských vztazích a komunikaci.

Třetí způsob, kterým se údaje mohou „týkat“ konkrétních osob, je založen na prvku „**výsledku**“. I když chybí prvek „obsahu“ a prvek „účelu“, o údajích lze mít za to, že se „týkají“ jednotlivce, jestliže – při zohlednění všech okolností daného konkrétního případu – bude mít jejich použití pravděpodobně dopad na práva a zájmy určité osoby. Přitom je třeba uvést, že není nutné, aby se u možného výsledku jednalo o velký dopad. Stačí možnost, že se v důsledku zpracování těchto údajů bude s daným jednotlivcem zacházet jinak než s ostatními osobami.

Příklad č. 8: monitorování polohy vozů taxi pro optimalizaci služeb, které má dopad na řidiče

Taxislužba zavede systém satelitního sledování, který jí umožňuje zjišťovat v reálném čase polohu volných vozů. Účelem zpracování údajů je poskytovat lepší služby a šetřit pohonné hmoty tím, že se každému zákazníkovi, který si objedná taxi, přiřadí vůz, jenž se nachází nejblíže k jeho adrese. Údaje, které takovýto systém vyžaduje, jsou přísně vzato údaji o automobilech, a nikoli o řidičích. Účelem zpracování není hodnotit výkonnost řidičů taxi, například z hlediska optimalizace jejich tras. Systém ovšem umožňuje sledovat výkonnost řidičů a kontrolovat, zda dodržují omezení rychlosti, zda používají vhodné trasy, zda jsou v daném okamžiku za volantem, nebo odpočívají mimo vůz atd. Z toho důvodu může mít značný dopad na tyto jednotlivce, a příslušné údaje tedy lze považovat za údaje, které se týkají také fyzických osob. Na jejich zpracování by se měla vztahovat pravidla ochrany údajů.

Uvedené tři prvky (obsah, účel a výsledek) je nutné chápat jako alternativní, a nikoli kumulativní podmínky. Zvláště platí, že je-li přítomen prvek obsahu, informaci lze posoudit jako informaci týkající se jednotlivce, i když zbývající prvky přítomny nejsou. Z toho nutně vyplývá, že se stejná informace může současně týkat různých jednotlivců podle toho, který prvek je přítomen ve vztahu ke každému z nich. Stejná informace se tak může týkat jednotlivce jménem Titius kvůli svému „obsahu“ (údaje jsou zjevně o Titiovi) A jednotlivce jménem Gaius kvůli svému „účelu“ (bude použita tak, aby se s Gaiem zacházelo určitým způsobem) A jednotlivce jménem Sempronius kvůli svému „výsledku“ (je pravděpodobné, že bude mít dopad na Semproniova práva a zájmy). To také znamená, že lze mít za to, že se údaje někoho týkají, i když na tohoto

člověka nejsou „zaměřeny“. Z předchozí analýzy vyplývá, že otázku, zda se údaje týkají určité osoby, je u každého jednotlivého údaje třeba zodpovědět podle jeho konkrétních vlastností. Že se informace mohou týkat různých osob je třeba mít obdobně na paměti, i při použití hmotněprávních ustanovení (např. o rozsahu práva na přístup).

Příklad č. 9: informace obsažené v zápisu ze schůze

Nutnost provádět výše uvedenou analýzu pro každou jednotlivou informaci zvlášť ilustruje příklad informací obsažených v zápisu ze schůze, kde je v souladu s obvyklým postupem zaznamenána přítomnost účastníků Titia, Gaia a Sempronia, dále výroky Titia a Gaia a konečně záznam z jednání o určitých tématech, které shrnul zapisovatel Sempronius. Za osobní údaje týkající se Titia lze pokládat pouze informace o tom, že se Titius v určitém čase a na určitém místě zúčastnil této schůze a že pronesl určité výroky. K osobním údajům týkajícím se Titia NEPATŘÍ účast Gaia na schůzi, Gaiovy výroky ani záznam z jednání o určité otázce pořízený Semproniem. Tak je tomu i v případě, že jsou tyto informace obsaženy ve stejném dokumentu a že projednání dané otázky na schůzi inicioval Titius. Na tyto informace se proto nevztahuje Titiovo právo na přístup k jeho vlastním osobním údajům. Zda a v jaké míře lze uvedené informace považovat za osobní údaje Gaia a Sempronia, bude třeba stanovit zvlášť pomocí výše popsané analýzy.

3. TŘETÍ SLOŽKA: „IDENTIFIKOVANÁ NEBO IDENTIFIKOVATELNÁ“ (FYZICKÁ OSOBA)

Směrnice vyžaduje, aby se informace týkaly fyzické osoby, která je „identifikovaná nebo identifikovatelná“, což vede k následujícím úvahám.

Obecně lze fyzickou osobu považovat za „identifikovanou“, jestliže je ve skupině osob „odlišena“ ode všech ostatních příslušníků této skupiny. V souladu s tím je fyzická osoba „identifikovatelná“, jestliže je možné ji identifikovat (přípona „-elná“ vyjadřuje možnost), ačkoli dosud identifikována nebyla. Tato druhá alternativa proto v praxi představuje prahovou podmínku určující, zda informace vyhovuje třetí složce definice.

Identifikace se obvykle provádí pomocí určitých zvláštních informací, které můžeme nazývat „identifikátory“ a které mají zvláště výsadní a těsný vztah ke konkrétnímu jednotlivci. Patří k nim vnější znaky vzhledu dané osoby, jako je výška, barva vlasů, oblečení atd., nebo vlastnosti osoby, které nejsou bezprostředně vnímatelné, jako je její povolání, funkce, jméno atd. Směrnice tyto „identifikátory“ zmiňuje v definici „osobních údajů“ v článku 2, kde je uvedeno, že fyzickou osobu „*lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity*“.

„Přímo“ či „nepřímo“ identifikovatelná

Věc je dále objasněna v komentáři k článkům pozměněného návrhu Komise, kde se uvádí, že „*osoba může být identifikována přímo jménem nebo nepřímo podle telefonního čísla, registračního čísla automobilu, čísla sociálního pojištění nebo čísla cestovního pasu nebo pomocí kombinace významných kritérií, která ji umožňuje rozeznat zúžením skupiny, do které patří (věk, povolání, bydliště atd.)*“. Ze znění tohoto tvrzení jasně vyplývá, že míra dostatečnosti určitých identifikátorů z hlediska provedení identifikace závisí na souvislostech konkrétní situace. Velmi běžné příjmení

nepostačí k identifikaci – tj. jednoznačnému určení – osoby v celé populaci země, ale pravděpodobně bude stačit k identifikaci žáka ve třídě. K identifikaci chodce ve skupině čekající u semaforu mohou stačit i vedlejší informace typu „muž v černém obleku“. Otázka, zda jednotlivec, jehož se informace týká, je, nebo není identifikovaný, tedy závisí na okolnostech daného případu.

Pokud jde o „přímo“ identifikované nebo identifikovatelné osoby, je nejběžnějším identifikátorem skutečně **jméno** a pojem „identifikovaná osoba“ v praxi nejčastěji znamená, že je známo jméno dané osoby.

Pro ověření identity je někdy jméno osoby nutné spojit s dalšími informacemi (datum narození, jména rodičů, adresa nebo fotografie obličeje), aby se zabránilo záměně této osoby za její případné jmenovce. Například informaci, že Titius dluží nějakou finanční částku, lze považovat za informaci týkající se identifikovaného jednotlivce, protože je spojena se jménem osoby. Jméno je informace, která ukazuje, že daný jednotlivec používá danou kombinaci písmen a zvuků, aby se odlišil a aby ho mohly odlišit ostatní osoby, s nimiž navazuje vztahy. Jméno může být také východiskem vedoucím k informacím o tom, kde dotyčná osoba bydlí nebo kde je k zastižení, a může být zdrojem informací o rodinných příslušnících (prostřednictvím příjmení) a o řadě různých právních a společenských vztahů s tímto jménem spojených (záznamy o vzdělání, lékařské záznamy, bankovní účty). Pokud je se jménem spojeno vyobrazení, může být dokonce možné dozvědět se o vzhledu dané osoby. Všechny tyto nové informace spojené se jménem mohou někomu dovolit, aby „zaostřil“ na konkrétního člověka, a původní informace je tak pomocí identifikátorů spojena s fyzickou osobou, kterou lze odlišit od jiných osob.

Co se týče „nepřímo“ identifikovaných nebo identifikovatelných osob, tato kategorie se obvykle vztahuje k jevu „jedinečných kombinací“, ať malého či velkého rozsahu. I v případech, kdy rozsah dostupných identifikátorů *prima facie* nikomu neumožňuje jednoznačně určit konkrétní osobu, může být tato osoba přesto „identifikovatelná“, protože ve spojení s dalšími informacemi (které může, ale nemusí mít v držení správce údajů) tyto informace umožní odlišení daného jednotlivce od jiných osob. Právě zde se uplatní směrnice se svým odkazem na „jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity“. Některé charakteristiky jsou natolik jedinečné, že lze danou osobu identifikovat velmi snadno („současný předseda vlády Španělska“), ale za určitých okolností může být dosti směrodatná i kombinace údajů v rovině kategorií (věková kategorie, regionální původ atd.), zvláště pokud existuje přístup k nějakému druhu doplňkových informací. Tento jev důkladně prostudovali statistici, kteří vždy věnují velkou pozornost prevenci porušení důvěrnosti.

Příklad č. 10: útržkovité informace v tisku

Jsou zveřejněny informace o případu trestné činnosti z minulosti, který si ve své době získal velkou pozornost veřejnosti. V současném zveřejnění není uveden žádný z tradičních identifikátorů, především žádná jména či data narození zúčastněných osob.

Zdá se však, že není nepřiměřeně obtížné získat dodatečné informace, které by umožnily zjistit totožnost hlavních aktérů – např. vyhledáním novin z příslušného období. Lze skutečně předpokládat, že není zcela nepravděpodobné, že někdo podnikne kroky (jako je vyhledání starých novin), kterými s největší pravděpodobností získá jména a další identifikátory osob, jichž se případ týká. Zdá se tedy, že informace v tomto příkladu je možné opodstatněně považovat za „informace o identifikovatelných osobách", a tedy za „osobní údaje".

Zde je třeba poznamenat, že i když je identifikace pomocí jména v praxi nejběžnější, jméno nemusí být nutné pro identifikaci jednotlivce ve všech případech. Tak tomu může být, jsou-li k jednoznačnému určení osoby použity jiné „identifikátory". Například počítačové záznamy evidující osobní údaje evidovaným osobám obvykle přiřazují jedinečné identifikátory, aby nemohlo dojít k záměně dvou osob v záznamech. Také na internetu je díky nástrojům pro sledování internetového provozu snadné identifikovat chování určitého počítače, a tedy i jeho uživatele. Z různých prvků se tak složí osobnost jednotlivce, aby jí mohla být připisována určitá rozhodnutí. I bez jakýchkoli dotazů na jméno a adresu daného jednotlivce je možné tuto osobu zařadit na základě socioekonomických, psychologických, filozofických a dalších kritérií a připisovat jí určitá rozhodnutí, protože kontaktní bod (počítač), který používá, již nezbytně nevyžaduje odhalení její identity v úzkém slova smyslu. Jinými slovy možnost identifikovat jednotlivce již nutně neznamená schopnost zjistit jeho jméno a definice osobních údajů tuto skutečnost odráží[10].

Evropský soudní dvůr se v tomto smyslu vyjádřil, když konstatoval, že „*uvádění různých osob na internetové stránce a jejich identifikace jménem nebo jinými prostředky, například uvedením jejich telefonních čísel nebo informací o jejich pracovních podmínkách a zájmových činnostech, představuje zpracování osobních údajů (...) ve smyslu (...) směrnice 95/46/ES*"[11].

Příklad č. 11: žadatelé o azyl

Žadatelům o azyl, kteří skrývají svá skutečná jména, byly v azylovém zařízení přiděleny číselné kódy pro správní účely. Tato čísla budou sloužit jako identifikátory, takže ke každému z nich budou připojovány různé informace o pobytu daného žadatele o azyl v tomto zařízení. Ve spojení s fotografií nebo jinými biometrickými ukazateli bude mít číselný kód těsný a bezprostřední vztah k fyzické osobě, kterou tak bude možné odlišit od ostatních žadatelů o azyl a přiřazovat k ní různé informace. Tyto informace se pak budou týkat „identifikované" fyzické osoby.

[10] Zpráva o použití zásad ochrany údajů v případě celosvětových telekomunikačních sítí, T-PD (2004) 04 v konečném znění, kterou vypracoval Yves Poullet a kolektiv pro výbor T-PD Rady Evropy, bod 2.3.1.

[11] Rozsudek Evropského soudního dvora ve věci C-101/2001 (Lindqvist) ze dne 6. listopadu 2003, bod 27.

V čl. 8 odst. 7 je také stanoveno, že „členské státy určí podmínky, za kterých může být předmětem zpracování vnitrostátní identifikační číslo nebo jakýkoli jiný identifikátor obecného významu“. Je důležité uvědomit si smysl tohoto ustanovení, které neobsahuje žádnou konkrétní zmínku o tom, jaký druh podmínek by měly členské státy zvolit, ale přesto je součástí článku, který se týká citlivých údajů. V 33. bodu odůvodnění je tento druh údajů popsán jako „*údaje, které svou povahou mohou porušit základní svobody nebo soukromí*“. Je možné se rozumně domnívat, že zákonodárce mohl mít s ohledem na vnitrostátní identifikační čísla obdobné obavy vzhledem k tomu, jak výrazný potenciál tato čísla mají pro snadné a jednoznačné propojení různých informací o daném jednotlivci.

Prostředky identifikace

Zvláštní pozornost výrazu „identifikovatelný“ je věnována ve 26. bodu odůvodnění směrnice, kde je uvedeno, že „*pro určení, zda je osoba identifikovatelná, je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem tak jakoukoli jinou osobou pro identifikaci dané osoby*“. To znamená, že pouhá hypotetická možnost jednoznačného určení nějaké osoby nepostačuje k tomu, aby tato osoba byla považována za „identifikovatelnou“. Jestliže s přihlédnutím ke „*všem prostředkům, které mohou být rozumně použity jak správcem tak jakoukoli jinou osobou*“, taková možnost neexistuje nebo je zanedbatelná, daná osoba by se neměla považovat za „identifikovatelnou“ a informace o ní za „osobní údaje“. Při uplatňování kritéria přihlédnutí ke „*všem prostředkům, které mohou být rozumně použity jak správcem tak jakoukoli jinou osobou*“ je třeba zvláště dbát na zohlednění všech faktorů, které v daném případě hrají roli. Jedním, avšak ne jediným faktorem jsou náklady na provedení identifikace. Kromě nich by měly být vzaty v potaz zamýšlený účel zpracování a jeho struktura, výhody očekávané správcem údajů, zájmy jednotlivců, které jsou v sázce, i riziko organizačních selhání (např. porušení povinnosti zachovávat důvěrnost) a technických problémů. Na druhé straně se jedná o dynamické kritérium, při jehož použití by měly být zohledněny aktuální stav technologií v době zpracování údajů a možnosti jejich vývoje za dobu, po kterou bude zpracování trvat. Je možné, že s prostředky, které mohou být rozumně použity v současnosti, nelze identifikaci provést. Je-li zamýšlená doba uchování údajů jeden měsíc, lze předpokládat, že identifikace nebude možná po dobu existence daných informací, které by se proto neměly považovat za osobní údaje. Pokud se však plánuje údaje uchovávat 10 let, správce by měl vzít v úvahu, že identifikace může být proveditelná například v devátém roce jejich existence, kdy by se z nich v důsledku toho mohly stát osobní údaje. Systém by měl být navržen tak, aby se dokázal přizpůsobovat takovým změnám v okamžiku, kdy nastanou, a aby do něj bylo možné včas začleňovat vhodná technická a organizační opatření.

Příklad č. 12: zveřejnění rentgenových snímků spolu s rodným jménem pacienta

Ve vědeckém časopise byl zveřejněn rentgenový snímek pacientky spolu s jejím rodným jménem, které je velice neobvyklé. Uvedení rodného jména této osoby ve spojení s tím, že její příbuzní nebo známí věděli, že trpí určitou chorobou, ji učinilo identifikovatelnou pro řadu lidí. V takovém případě by se rentgenový snímek považoval za osobní údaj.

Příklad č. 13: údaje z farmaceutického výzkumu

Nemocnice nebo jednotliví lékaři předávají údaje z lékařských záznamů svých pacientů určité společnosti pro účely lékařského výzkumu. Při tom se nepoužívají jména

pacientů, nýbrž pouze sériová čísla, která se náhodně přiřazují jednotlivým klinickým případům, aby se zajistila konzistence a zabránilo se záměně s informacemi o jiných pacientech. Jména pacientů zůstávají výlučně v držení příslušných lékařů, kteří jsou vázáni lékařským tajemstvím. Údaje neobsahují žádné dodatečné informace, které by v kombinaci s těmito údaji umožňovaly identifikaci pacientů. Kromě toho byla přijata všechna další potřebná opatření, ať již právní, technické nebo organizační povahy, pro prevenci identifikace a identifikovatelnosti subjektů údajů. Za těchto okolností může orgán pro ochranu údajů usoudit, že v rámci zpracování údajů prováděného farmaceutickou společností neexistují žádné prostředky, které by mohly být rozumně použity k identifikaci subjektů údajů.

Jak je uvedeno výše, při posuzování „*všech prostředků, které mohou být rozumně použity*“ pro identifikaci osob, bude k významným faktorům patřit účel, který správce údajů zpracováním sleduje. Vnitrostátní orgány pro ochranu údajů se setkaly s případy, kdy správce údajů tvrdil, že se zpracovávají pouze rozptýlené informace neobsahující odkaz na jméno ani jiné přímé identifikátory, a prosazoval, aby se tyto údaje nepovažovaly za osobní údaje a aby se na ně nevztahovala pravidla ochrany údajů. Na druhé straně ovšem zpracování těchto informací mělo smysl pouze za předpokladu, že umožňovalo identifikaci konkrétních jednotlivců a určitý způsob zacházení s nimi. V takovýchto případech, kdy identifikace jednotlivců vyplývá z účelu zpracování, lze předpokládat, že správce údajů nebo jakákoli jiná zúčastněná osoba má nebo bude mít prostředky, „které mohou být rozumně použity“ k identifikaci subjektu údajů. Tvrzení, že jednotlivci nejsou identifikovatelní v situaci, kdy je účelem zpracování právě jejich identifikace, by obsahovalo jasný vnitřní rozpor. Proto je zde třeba mít za to, že se informace týkají identifikovatelných jednotlivců, a na jejich zpracování by se měla vztahovat pravidla ochrany údajů.

Příklad č. 14: dohled pomocí videokamer

Výše uvedené má zvláštní význam v souvislosti s dohledem pomocí videokamer, kdy správci údajů často tvrdí, že k identifikaci dojde jen u malé části shromážděného materiálu, a že tedy žádné osobní údaje nejsou zpracovávány, dokud identifikace v těchto několika málo případech skutečně neproběhne. Účelem dohledu pomocí videokamer však je právě identifikace osob zachycených na záznamu ve všech případech, kdy to správce pokládá za nezbytné. Celý systém jako takový se proto musí považovat za zpracovávání údajů o identifikovatelných osobách, i když některé natočené osoby v praxi identifikovatelné nejsou.

Příklad č. 15: dynamické IP adresy

Pracovní skupina již uvedla, že IP adresy považuje za údaje týkající se identifikovatelné osoby. Konstatovala totiž, že „*poskytovatelé přístupu k internetu a správci sítí LAN mohou s použitím přiměřených prostředků identifikovat uživatele internetu, kterým přiřadili IP adresy, protože obvykle soustavně „protokolují“ do souboru datum, čas a trvání připojení a dynamickou IP adresu přidělenou uživateli. Totéž platí o poskytovatelích internetových služeb, kteří mají protokol na HTTP serveru. V těchto případech lze nepochybně hovořit o osobních údajích ve smyslu čl. 2 písm. a) směrnice ...)*“[12]

[12] Dokument č. WP 37: Soukromí na internetu – integrovaný přístup EU k ochraně údajů na internetu, přijatý dne 21. listopadu 2000.

Zejména v případech, kdy se zpracování IP adres provádí za účelem identifikace uživatelů počítače (například ze strany majitelů autorských práv, kteří chtějí stíhat uživatele počítačů za porušování práv duševního vlastnictví), správce údajů předjímá, že „prostředky, které mohou být rozumně použity“ k identifikaci těchto osob budou k dispozici, např. prostřednictvím soudů, na něž se obrátí, (jinak by sběr informací neměl smysl), a tyto informace by se proto měly považovat za osobní údaje.

Zvláštním případem by byl nějaký druh IP adres, které za určitých okolností z různých technických a organizačních důvodů skutečně neumožňují identifikaci uživatele. Příkladem mohou být IP adresy přidělované počítači v internetové kavárně, kde se nevyžaduje prokázání totožnosti zákazníků. Zde by se dalo tvrdit, že údaje o používání počítače X shromážděné za určité časové období neumožňují identifikaci uživatele s použitím rozumných prostředků, a tedy nejsou osobními údaji. Je ovšem třeba poznamenat, že poskytovatelé internetových služeb s největší pravděpodobností nebudou vědět, zda daná IP adresa umožňuje, nebo neumožňuje identifikaci, a že údaje spojené s touto adresou budou zpracovávat stejným způsobem jako informace spojené s IP adresami řádně zaregistrovaných uživatelů, kteří jsou identifikovatelní. Pokud tedy poskytovatel internetových služeb není schopen s naprostou jistotou odlišit údaje odpovídající uživatelům, kteří nemohou být identifikováni, bude muset pro jistotu nakládat se všemi informace o IP adresách jako s osobními údaji.

Příklad č. 16: škody, které způsobuje graffiti

Vozy pro přepravu cestujících, které vlastní určitá dopravní společnost, jsou opakovaně poškozovány graffiti. Za účelem stanovení výše škody a pro snazší uplatnění právních nároků vůči tvůrcům graffiti vytvoří tato společnost rejstřík, který obsahuje informace o okolnostech vzniku škody a vyobrazení poškozených věcí i „tagů“ neboli „podpisů“ těchto tvůrců. V okamžiku vložení informací do rejstříku jsou původci škody neznámí a neví se ani, komu patří který „podpis“. Může se stát, že se to nezjistí nikdy. Účelem zpracování je však právě identifikovat jednotlivce, kterých se informace týkají, jakožto původce škody, aby vůči nim bylo možné vznést právní nároky. Takové zpracování má smysl, jestliže správce údajů považuje za rozumně pravděpodobné, že prostředky k identifikaci těchto jednotlivců jednou budou existovat. Informace na vyobrazení by se měly pokládat za informace týkající se „identifikovatelných“ jednotlivců a informace v rejstříku za „osobní údaje“ a na jejich zpracování by se měla vztahovat pravidla ochrany údajů, která takové zpracování za určitých okolností umožňují jakožto legitimní, jsou-li přijata určitá ochranná opatření.

Jestliže identifikace subjektu údajů není součástí účelu zpracování, hrají důležitou úlohu technická opatření, která mají identifikaci zabránit. Zavedení vhodných nejmodernějších technických a organizačních opatření na ochranu údajů před identifikací může rozhodnout o tom, že se osoby nebudou považovat za identifikovatelné s přihlédnutím ke *všem prostředkům, které mohou být rozumně použity správcem nebo jakoukoli jinou osobou k* identifikaci jednotlivců. V tomto případě zavedení takových opatření není *důsledkem* právní povinnosti vyplývající z článku 17 směrnice (který se použije, pouze pokud informace jsou osobními údaji), nýbrž *podmínkou* toho, aby informace za osobní údaje právě považovány nebyly a aby jejich zpracování nespadalo do oblasti působnosti směrnice.

Pseudonymizované údaje

Pseudonymizace je proces skrytí identit, jehož účelem je mít možnost sbírat další údaje týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost. To má zvláštní význam v oblasti výzkumu a statistiky.

Pseudonymizaci lze provést pomocí korespondenčních tabulek identit a k nim příslušejících pseudonymů nebo pomocí obousměrných kryptografických algoritmů pro pseudonymizaci. V takovém případě je možné identity zpětně vysledovat. Identity lze skrýt také způsobem, který jakoukoli zpětnou identifikaci znemožňuje, např. pomocí jednosměrné kryptografie, která obecně generuje anonymizované údaje.

Efektivnost postupu pseudonymizace závisí na řadě faktorů (na tom, v jaké fázi se použije a nakolik je zabezpečen před zpětným vysledováním identit; na velikosti souboru, jehož je jednotlivec součástí; na možnosti spojit jednotlivé operace nebo záznamy se stejnou osobou atd.). Pseudonymy by měly být náhodné a nepředvídatelné. Počet možných pseudonymů by měl být natolik velký, aby stejný pseudonym nikdy nebyl náhodně vybrán dvakrát. Vyžaduje-li se vysoká úroveň zabezpečení, musí se množina možných pseudonymů alespoň rovnat rozpětí hodnot bezpečných kryptografických hash funkcí.[13]

Pseudonymizované údaje, jež umožňují zpětné vysledování, lze pokládat za informace o jednotlivcích, které jsou *nepřímo identifikovatelné.* Použití pseudonymu skutečně znamená, že jednotlivce je možné zpětně dohledat, takže lze zjistit jeho identitu – ovšem pouze za předem stanovených podmínek. V tomto případě se pravidla ochrany údajů sice použijí, ale rizika pro jednotlivce, která jsou spojena se zpracováním takovýchto nepřímo identifikovatelných informací, budou nejčastěji nízká, takže tato pravidla bude možné oprávněně použít pružněji, než kdyby byly zpracovávány informace o přímo identifikovatelných jednotlivcích.

Údaje kódované pomocí klíče

Údaje kódované pomocí klíče jsou klasickým příkladem pseudonymizace. Informace se týkají jednotlivců, kteří jsou označeni kódem, přičemž klíč spojující kódy s běžnými identifikátory těchto jednotlivců (jméno, datum narození, adresa apod.) se uchovává odděleně.

Příklad č. 17: neagregované údaje pro statistické účely

Při posuzování toho, zda prostředky k identifikaci „mohou být rozumně“ použity, je důležité brát v potaz všechny okolnosti. To lze ilustrovat na příkladu osobních informací zpracovávaných vnitrostátním statistickým úřadem, které se v určité fázi uchovávají v neagregované podobě a týkají se konkrétních jednotlivců. Tito jednotlivci však nejsou označeni jménem, nýbrž kódem (např. osoba s kódem X1234 vypije sklenici vína častěji než třikrát za týden). Klíč k těmto kódům (tabulku přiřazující kódy ke jménům osob) statistický úřad uchovává odděleně. Lze mít za to, že tento klíč „může být rozumně použit“ statistickým úřadem, a soubor informací týkajících se jednotlivců proto může být považován za osobní údaje, a úřad by s ním měl nakládat podle pravidel ochrany údajů. Následně je možné si představit, že se seznam s údaji o zvyklostech spotřebitelů ohledně pití vína předá národní organizaci výrobců vína,

[13] Viz pracovní dokument „Technologie zlepšující ochranu soukromí“ pracovní skupiny pro „technologie zlepšující ochranu soukromí“ výboru pro „technické a organizační aspekty ochrany údajů“ německých spolkových a zemských komisařů pro ochranu údajů (říjen 1997); zveřejněný na adrese: http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm.

která chce tyto statistické údaje využít na podporu svého veřejného stanoviska. Má-li se určit, zda tento seznam informací stále představuje osobní údaje, mělo by se posoudit, zda „*s přihlédnutím ke všem prostředkům, které mohou být rozumně použity správcem nebo jakoukoli jinou osobou*“, mohou být jednotliví spotřebitelé vína identifikováni.

Je-li pro každou konkrétní osobu použit jedinečný kód, riziko identifikace nastává, kdykoli lze získat přístup k šifrovacímu klíči. Při rozhodování o tom, zda mohou být s *přihlédnutím ke všem prostředkům, které mohou být rozumně použity správcem nebo jakoukoli jinou osobou*, příslušné osoby identifikovány, *a* tedy zda je tyto informace třeba považovat za „osobní údaje“, je proto nutné vzít v potaz faktory, jako jsou riziko počítačového průniku zvenčí, pravděpodobnost, že někdo z odesílající organizace poruší profesní tajemství a klíč poskytne, a proveditelnost nepřímé identifikace. Pokud informace osobními údaji jsou, použijí se pravidla ochrany údajů. Jiná otázka je, že při uplatnění těchto pravidel by bylo možné zohlednit, zda byla rizika pro jednotlivce snížena, a stanovit pro zpracování přísnější nebo mírnější podmínky s využitím pružnosti, kterou pravidla směrnice umožňují.

Jestliže kódy naopak jedinečné nejsou a stejný číselný kód (např. „123“) je použit pro označení jednotlivců v různých městech a pro údaje z různých let (konkrétní jednotlivec je odlišen pouze v rámci daného roku a v rámci vzorku ze stejného města), mohl by správce nebo třetí osoba konkrétního jednotlivce identifikovat pouze v případě, že by věděl, kterého roku a kterého města se ten který údaj týká. Pokud byly tyto doplňující informace odstraněny a pomocí rozumných prostředků je nelze získat zpět, bylo by možné mít za to, že se informace netýkají identifikovatelných jednotlivců, a pravidla ochrany údajů by se na ně nevztahovala.

Tento druh údajů se běžně používá při klinických zkouškách léčivých přípravků. Právní rámec pro provádění těchto činností stanoví směrnice 2001/20 ze dne 4. dubna 2001 o uplatňování správné klinické praxe při provádění klinických hodnocení[14]. Lékař / výzkumný pracovník („zkoušející“), který lék testuje, shromažďuje informace o klinických výsledcích u jednotlivých pacientů, které označí kódy. Farmaceutické společnosti nebo jiným zúčastněným stranám („zadavatelům“) výzkumný pracovník tyto informace předává pouze v této kódované podobě, protože je zajímají pouze biostatistické informace. Zkoušející ovšem odděleně uchovává klíč, který kódy přiřazuje k běžným informacím umožňujícím oddělenou identifikaci pacientů. Zkoušející je povinen tento klíč uchovávat v zájmu ochrany zdraví pacientů pro případ, že se v souvislosti s lékem projeví nějaká nebezpečí. Jde o to, aby v případě potřeby mohli být jednotliví pacienti identifikováni a náležitě léčeni.

Zde vzniká otázka, zda lze údaje používané pro klinické zkoušky pokládat za údaje týkající se „identifikovatelných“ fyzických osob, čili za údaje, na které se vztahují pravidla ochrany údajů. V souladu s již popsanou analýzou je pro určení, zda je osoba identifikovatelná, třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby. V tomto případě je identifikace jednotlivců (kvůli nasazení vhodné léčby v případě potřeby) jedním z účelů zpracování údajů kódovaných pomocí klíče. Farmaceutická společnost nastavila prostředky pro zpracování údajů, včetně organizačních opatření a svých vztahů s výzkumným pracovníkem, který má v držení klíč, takovým způsobem, že identifikace jednotlivců nejen *může* nastat, ale za určitých okolností nastat *musí*.

[14] Úř. věst. L 121, 1.5.2001, s. 34.

Identifikace pacientů je tak nedílnou součástí účelů a prostředků zpracování. V takovém případě lze učinit závěr, že tyto údaje kódované pomocí klíče představují informace týkající se identifikovatelných fyzických osob pro všechny strany, které se mohou podílet na případné identifikaci, a měla by se na ně vztahovat pravidla uvedená v právních předpisech o ochraně údajů. To ovšem neznamená, že i každý další správce údajů zpracovávající stejný soubor kódovaných údajů bude zpracovávat osobní údaje, pokud je v konkrétním režimu, v němž tito jiní správci působí, zpětná identifikace explicitně vyloučena a v tomto směru byla přijata vhodná technická opatření.

V jiných oblastech výzkumu nebo jiných částech stejného projektu mohla být zpětná identifikace subjektu údajů vyloučena při přípravě protokolů a postupů, a to například z důvodu, že v nich nejsou přítomny žádné léčebné aspekty. Z technických nebo jiných důvodů může přesto existovat způsob, jak zjistit, kterým osobám odpovídají které klinické údaje. Nepředpokládá se však a ani se neočekává, že by tato identifikace za jakýchkoli okolností proběhla, a byla zavedena vhodná technická opatření (např. kryptografická, nevratné zašifrování pomocí hash algoritmu), která identifikaci brání. I když k identifikaci některých subjektů údajů může dojít navzdory všem těmto protokolům a opatřením (vinou nepředvídatelných okolností, jako je náhodná shoda vlastností subjektu údajů, které odhalí jeho identitu), v tomto případě se s přihlédnutím ke *všem prostředkům, které mohou být rozumně použity správcem nebo jakoukoli jinou osobou*, informace zpracovávané původním správcem nemusejí považovat za informace týkající se identifikovaných nebo identifikovatelných jednotlivců. Na jejich zpracování se tak nemusejí vztahovat ustanovení směrnice. Avšak v případě nového správce, který fakticky získal přístup k identifikovatelným informacím, se tyto informace nepochybně budou považovat za „osobní údaje“.

Často kladená otázka (FAQ) 14 bod 7 zásad bezpečného přístavu

Otázka údajů kódovaných pomocí klíče ve farmaceutickém výzkumu je řešena v rámci zásad bezpečného přístavu[15]. FAQ 14 bod 7 zní takto:

FAQ 14 – Léčiva

7. Ot.: Údaje určené pro výzkum jsou u zdroje zásadně kódovány pomocí unikátního klíče vedoucím výzkumným pracovníkem tak, aby nebyla zřejmá totožnost konkrétních subjektů údajů. Farmaceutické společnosti financující takový výzkum klíč neobdrží. Kód k unikátnímu klíči má pouze výzkumný pracovník, který tak může za určitých okolností danou osobu identifikovat (např. je-li potřebný následný lékařský dohled). Představuje předání takto kódovaných údajů z EU do Spojených států předání osobních údajů, které podléhá zásadám „bezpečného přístavu“?

7. Odp.: Ne. V tomto případě nejde o předání osobních údajů, které by podléhalo zásadám „bezpečného přístavu“.

Pracovní skupina soudí, že toto tvrzení v zásadách bezpečného přístavu není neslučitelné s výše uvedenou argumentací ve prospěch toho, aby se takové informace pokládaly za osobní údaje, na které se vztahuje směrnice. Tato FAQ ve skutečnosti není dostatečně přesná, protože neuvádí, komu a za jakých podmínek se údaje předávají. Pracovní skupina rozumí této FAQ tak, že se týká případů, kdy jsou údaje kódované pomocí klíče odesílány příjemci v USA (například farmaceutické

[15] Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000, Úř. věst. L 215/7, 25.8.2000.

společnosti), který obdrží pouze údaje kódované pomocí klíče a nikdy nebude znát totožnost pacientů. Ta je a v případě potřeby léčby bude známa pouze lékaři / výzkumnému pracovníkovi v EU, nikdy však společnosti v USA.

Anonymní údaje

„Anonymní údaje" ve smyslu směrnice lze definovat jako jakékoli informace týkající se fyzické osoby, z nichž tato osoba nemůže být identifikována ani správcem ani jakoukoli jinou osobou s *přihlédnutím ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou* pro identifikaci daného jednotlivce. „Anonymizovanými údaji" se proto rozumí anonymní údaje, které dříve odkazovaly na identifikovatelnou osobu, ale u nichž tuto identifikaci již nelze provést. Na tento pojem odkazuje také 26. bod odůvodnění, když říká, že „*zásady ochrany se nevztahují na údaje, které byly anonymizovány tak, že subjekt údajů již není identifikovatelný*". I zde posouzení otázky, zda údaje umožňují identifikaci jednotlivce a zda informace lze, nebo nelze považovat za anonymní, závisí na okolnostech a analýzu je třeba provádět případ od případu se zvláštním ohledem na míru, v jaké mohou být rozumně použity prostředky pro identifikaci, jak je popsáno ve 26. bodu odůvodnění. Toto má zvláštní význam v případech statistických informací, které sice mohou být prezentovány v podobě agregovaných údajů, ale původní vzorek není dostatečně velký a další informace mohou umožnit identifikaci jednotlivců.

Příklad č. 18: statistická šetření a spojení rozptýlených informací

Kromě obecné povinnosti dodržovat pravidla ochrany údajů mají statistici v zájmu zajištění anonymity statistických šetření také zvláštní povinnost zachovávat profesní tajemství. Tato pravidla jim zakazují zveřejňovat neanonymní údaje. Musejí tedy zveřejňovat agregované statistické údaje, jež v žádném případě nelze přiřadit k identifikované osobě, která je předmětem statistiky. Toto pravidlo je zvláště významné v souvislosti se zveřejňováním výsledků sčítání lidu. V každé situaci by měl být stanoven práh, při jehož nedosažení se má za to, že dotčené osoby lze identifikovat. Jestliže se zdá, že nějaké kritérium vede k identifikaci v dané kategorii osob, pak by bez ohledu na velikost této kategorie (např. když ve městě s 6 000 obyvateli působí jen jeden lékař) mělo být toto „diskriminační" kritérium zcela vypuštěno nebo by měla být doplněna další kritéria, aby došlo k „rozředění" výsledků o dané osobě, a tak bylo možné zachovat statistické tajemství.

Příklad č. 19: zveřejnění snímků z dohledu pomocí videokamer

Majitel prodejny ve svém obchodě nainstaluje systém dohledu pomocí videokamer. Následně v obchodě zveřejní snímky zlodějů, kteří byli díky tomuto systému zadrženi. Po zásahu policie obličeje zlodějů začerní. Avšak i po této úpravě existuje možnost, že osoby na fotografiích poznají jejich přátelé, příbuzní nebo sousedé, například proto, že se stále dají rozeznat jejich postavy, účesy a oblečení.

4. ČTVRTÁ SLOŽKA: (FYZICKÁ) „OSOBA"

Ochrana, kterou poskytují pravidla směrnice, se vztahuje na fyzické osoby, tj. na lidi. V tomto smyslu je právo na ochranu osobních údajů univerzálním právem, které není omezeno na státní příslušníky či obyvatele určité země. To je výslovně uvedeno v 2. bodu odůvodnění směrnice, kde se konstatuje, že „*systémy zpracování údajů slouží*

lidem“ a že „*musí bez ohledu na státní občanství nebo bydliště fyzických osob dodržovat základní svobody a práva těchto osob*“.

Na pojem fyzická osoba odkazuje článek 6 Všeobecné deklarace lidských práv, který zní: „*Každý má právo na to, aby byla všude uznávána jeho právní osobnost*.“ Pojem právní osobnosti (právní subjektivity) lidí, kterou se rozumí způsobilost být subjektem právních vztahů a která začíná narozením a končí smrtí, přesněji vymezují právní předpisy členských států, obvykle v oblasti občanského práva. Osobními údaji jsou proto v zásadě údaje týkající se identifikovaných nebo identifikovatelných *žijících jednotlivců*. Z toho pro účely této analýzy vyplývá řada otázek.

Údaje o zemřelých osobách

Informace, které se týkají zemřelých jednotlivců, by se proto v zásadě neměly pokládat za osobní údaje, na které se vztahují pravidla směrnice, protože zemřelí již nejsou fyzickými osobami podle občanského práva. V některých případech se však údajům o zemřelých přesto může nepřímo dostat určité ochrany.

Zaprvé nemusí být správce údajů schopen zjistit, zda osoba, které se údaje týkají, je stále naživu, nebo již zemřela. Ale i v případě, že to zjistit dokáže, mohou být informace o zemřelých bez rozlišení zpracovávány ve stejném režimu jako informace o žijících osobách. Vzhledem k údajům o žijících jednotlivcích se na správce údajů vztahují povinnosti v oblasti ochrany údajů uložené směrnicí, a v praxi pro něj proto bude pravděpodobně jednodušší zpracovávat i údaje o zemřelých způsobem, který ukládají pravidla ochrany údajů, než oba soubory údajů oddělovat.

Zadruhé mohou informace o zemřelých jednotlivcích odkazovat také na žijící osoby. Například z informace, že zemřelá Gaia trpěla hemofilií, vyplývá, že jí trpí i její syn Titius, protože toto onemocnění souvisí s genem v chromozomu X. Jestliže tedy informace, které jsou údaji o zemřelých, lze současně považovat za informace týkající se také žijících osob a za osobní údaje, na které se vztahuje směrnice, mohou osobní údaje zemřelých nepřímo požívat ochrany podle pravidel ochrany údajů.

Zatřetí mohou být informace o zemřelých osobách předmětem zvláštní ochrany, kterou poskytují jiné soubory pravidel než právní předpisy o ochraně údajů. Tato pravidla vymezují hranice toho, co se někdy označuje jako „*personalitas praeterita*“. Povinnost zdravotníků zachovávat důvěrnost nekončí smrtí pacienta. Vnitrostátní právní předpisy o právu na ochranu osobní pověsti a cti mohou poskytovat ochranu také památce zemřelých.

Začtvrté, jak připomněl ESD[16], nic nebrání členskému státu, aby oblast působnosti vnitrostátních právních předpisů, kterými se provádí směrnice 95/46/ES, rozšířil na oblasti nezahrnuté do působnosti této směrnice za předpokladu, že to není v rozporu s žádným jiným právním předpisem Společenství. Je možné, že se vnitrostátní zákonodárce v některých státech rozhodne rozšířit ustanovení vnitrostátních právních

[16] Rozsudek Evropského soudního dvora ve věci C-101/2001 (Lindqvist) ze dne 6. listopadu 2003, bod 98.

předpisů o ochraně údajů i na některé aspekty zpracování údajů o zemřelých osobách, pokud to bude opodstatněno legitimním zájmem.[17]

Nenarozené děti

Míra, v jaké se pravidla ochrany údajů mohou použít před narozením, závisí na obecném postoji vnitrostátních právních systémů k ochraně nenarozených dětí. Především s ohledem na dědická práva některé členské státy uznávají zásadu, že počaté, ale dosud nenarozené děti se pokládají za narozené, pokud jde o jejich prospěch (a tak mohou dědit či přijímat dary), za podmínky, že se skutečně narodí. V jiných členských státech poskytují konkrétní ochranu zvláštní právní předpisy, a to za stejné podmínky. Aby bylo možné určit, zda vnitrostátní předpisy o ochraně údajů chrání také informace o nenarozených dětech, je třeba posoudit tento obecný přístup vnitrostátního právního systému spolu s účelem pravidel ochrany údajů, kterým je ochrana jednotlivce.

Další otázka souvisí s úvahou, že obecná reakce právního systému vychází z předpokladu, že situace nenarozených dětí je časově omezena na dobu těhotenství, a nebere se v úvahu, že ve skutečnosti může trvat podstatně déle – jako v případě zmrazených embryí. Konkrétní právní reakce mohou být součástí zvláštních předpisů o metodách reprodukce, které se zabývají použitím lékařských nebo genetických informací o embryích.

Právnické osoby

Jelikož v definici osobních údajů se odkazuje na jednotlivce, tj. fyzické osoby, na informace týkající se právnických osob se směrnice v zásadě nevztahuje, a ochrana poskytovaná směrnicí se v jejich případě nepoužije.[18] Ovšem některá pravidla ochrany údajů se přesto mohou v řadě situací nepřímo vztahovat i na informace týkající se podniků nebo právnických osob.

Na právnické osoby se vztahují některá ustanovení směrnice 2002/58/ES o soukromí a elektronických komunikacích. V článku 1 této směrnice se uvádí: „2. *Ustanovení této směrnice upřesňují a doplňují směrnici 95/46/ES pro účely uvedené v odstavci 1. Navíc poskytují ochranu oprávněných zájmů účastníků, kteří jsou právnickými osobami*.“ V souladu s tím články 12 a 13 rozšiřují použití některých ustanovení o účastnických seznamech a nevyžádaných sděleních i na právnické osoby.

Informace o právnických osobách lze považovat za informace „týkající se“ fyzických osob podle kritérií uvedených v tomto dokumentu také na základě jejich věcného obsahu. Tak tomu může být například tehdy, když je název právnické osoby odvozen od jména fyzické osoby. Dalším příkladem může být podnikový e-mail, který obvykle používá určitý zaměstnanec, nebo informace o malém podniku (který je z právního hlediska „věcí“, a nikoli právnickou osobou), které mohou popisovat chování jeho majitele. Ve všech těchto případech, kdy je na základě kritérií „obsahu“, „účelu“ nebo „výsledku“ možné mít za to, že se informace o právnické osobě nebo podniku „týkají“

[17] Zápis ze zasedání Rady Evropské unie konaného dne 8. února 1995, dokument 4730/95: „K čl. 2 písm. a) „*Rada a Komise potvrzují, že stanovení toho, zda a do jaké míry se tato směrnice použije pro zemřelé osoby, přísluší členským státům.*“

[18] 24. bod odůvodnění směrnice: „*vzhledem k tomu, že se tato směrnice nevztahuje na právní předpisy týkající se ochrany právnických osob v souvislosti se zpracováním údajů*“.

fyzické osoby, měly by se považovat za osobní údaje a pravidla ochrany údajů by se měla použít.

Evropský soudní dvůr jasně stanovil, že členským státům nic nebrání, aby oblast působnosti vnitrostátních právních předpisů, kterými se provádí směrnice, rozšířily na oblasti nespadající do její působnosti za předpokladu, že to není v rozporu s žádným jiným právním předpisem Společenství.[19] V souladu s tím některé členské státy, například Itálie, Rakousko nebo Lucembursko, použití některých ustanovení vnitrostátních právních předpisů přijatých na základě směrnice (například ustanovení o bezpečnostních opatřeních) skutečně rozšířily i na zpracování údajů o právnických osobách.

Stejně jako u informací o zemřelých lidech se i zde může stát, že se v důsledku praktických opatření správce údajů budou pravidla ochrany údajů fakticky vztahovat také na údaje o právnických osobách. Jestliže správce údajů bez rozlišení shromažďuje údaje o fyzických a právnických osobách a ukládá je do stejných datových souborů, mechanismy zpracování údajů a kontrolní systém mohou být navrženy tak, aby vyhovovaly pravidlům ochrany údajů. Ve skutečnosti může být pro správce snazší používat pravidla ochrany údajů pro všechny druhy informací v jeho záznamech než snažit se informace třídit podle toho, zda se týkají fyzických, nebo právnických osob.

IV. CO SE STANE, KDYŽ SE NA ÚDAJE DEFINICE NEVZTAHUJE?

Jak je v tomto dokumentu uvedeno na řadě míst, informace se za různých okolností nemusejí považovat za osobní údaje. To platí v případech, kdy nelze mít za to, že se údaje týkají jednotlivce, nebo kdy jednotlivce nelze považovat za identifikovaného ani identifikovatelného. Jestliže se pojem „osobní údaje“ na zpracovávané informace nevztahuje, důsledkem je, že se směrnice v souladu se svým článkem 3 nepoužije. To ovšem neznamená, že mohou být jednotlivci v dané konkrétní situaci zbaveni jakékoli ochrany. V úvahu je třeba vzít níže uvedené aspekty.

Jestliže se směrnice nepoužije, je možné, že se použijí vnitrostátní právní předpisy o ochraně údajů. Jak stanoví její článek 34, směrnice je určena členským státům. Mimo oblast její působnosti členské státy nepodléhají povinnostem, které ukládá, tj. zejména povinnosti přijmout právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí. Jak ovšem jasně stanovil Evropský soudní dvůr, členským státům nic nebrání, aby oblast působnosti vnitrostátních právních předpisů, kterými se směrnice provádí, rozšířily na oblasti nespadající do její působnosti za předpokladu, že to není v rozporu s žádným jiným právním předpisem Společenství. Může se proto snadno stát, že na některé situace nezahrnující zpracování osobních údajů podle definice ve směrnici se přesto vztahují ochranná opatření podle vnitrostátních právních předpisů. To se může týkat například údajů kódovaných pomocí klíče bez ohledu na to, zda jsou, nebo nejsou osobními údaji.

I v případech, kdy se pravidla ochrany údajů nepoužijí, mohou některé činnosti představovat porušení článku 8 Evropské úmluvy o lidských právech, který chrání právo na soukromý a rodinný život, ve světle rozsáhlé judikatury Evropského soudu pro lidská práva. V případech, kdy se pravidla ochrany údajů nepoužijí, ale v sázce

[19] Rozsudek Evropského soudního dvora ve věci C-101/2001 (Lindqvist) ze dne 6. listopadu 2003, bod 98.

mohou být různé oprávněné zájmy, mohou jednotlivcům poskytnout ochranu i jiné soubory pravidel, jako je právo občanskoprávních deliktů, trestní právo nebo právní předpisy proti diskriminaci.

V. ZÁVĚRY

V tomto stanovisku pracovní skupina poskytuje vodítko ke způsobu, jakým by se měl chápat pojem osobní údaje ve směrnici 95/46/ES a souvisejících právních předpisech Společenství a jak by se měl v různých situacích používat.

V rámci obecných úvah bylo konstatováno, že evropský zákonodárce měl v úmyslu zavést široký pojem osobní údaje, jehož rozsah však není neomezený. Stále je třeba mít na paměti, že cílem pravidel obsažených ve směrnici je ochrana základních práv a svobod jednotlivců, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů. Tato pravidla byla proto vytvořena pro použití v situacích, kdy mohou být práva jednotlivců ohrožena, a kdy tudíž potřebují ochranu. Oblast působnosti pravidel ochrany údajů by se neměla nadměrně rozšiřovat, ale současně je třeba se vyvarovat nepatřičnému zužování pojmu osobní údaje. Směrnice vymezuje oblast své působnosti, z níž vylučuje řadu činností, a u činností, které do její oblasti působnosti spadají, umožňuje pružné používání pravidel. Zásadní úlohu při hledání vhodné rovnováhy v jejich používání hrají orgány pro ochranu údajů (viz oddíl II).

Analýza pracovní skupiny vychází ze čtyř hlavních složek, které lze rozlišit v definici „osobních údajů“: „veškeré informace“, „o“ (vztah mezi informacemi a osobou), „identifikovaná nebo identifikovatelná“ a (fyzická) „osoba“. Tyto složky jsou těsně provázány a vzájemně se podporují a společně rozhodují o tom, zda by se určitá informace měla považovat za „osobní údaj“. Na podporu uvedené analýzy byly využity příklady z vnitrostátní praxe evropských orgánů pro ochranu údajů.

- První složka – „veškeré informace“ – vyžaduje široký výklad pojmu osobní údaje – nezávisle na povaze a obsahu informací a technickém formátu, ve kterém jsou prezentovány. To znamená, že za „osobní údaje“ lze považovat jak objektivní, tak subjektivní informace o osobě v libovolném postavení, a to bez ohledu na to, jaký technický nosič je obsahuje. Stanovisko se zabývá také biometrickými údaji a právním rozdílem mezi nimi a vzorky lidských tkání, z nichž se dají získat (viz oddíl III bod 1).

- Druhá složka – „o“ (vztah mezi informacemi a osobou) – byla dosud často přehlížena, ale přitom má klíčový význam pro určení věcného rozsahu dotčeného pojmu, zejména ve vztahu k věcem a novým technologiím. Stanovisko předkládá tři alternativní prvky, tj. obsah, účel nebo výsledek, umožňující určit, zda je informace „o“ jednotlivci (týká se jednotlivce). To se týká také informací, které mohou mít zjevný dopad na způsob, jakým se s jednotlivcem zachází nebo jakým je hodnocen (viz oddíl III bod 2).

- Třetí složka – „identifikovaná nebo identifikovatelná“ – je posouzena se zaměřením na podmínky, za kterých má být jednotlivec považován za „identifikovatelného“, a zvláště na „prostředky, které mohou být rozumně použity“ správcem nebo jakoukoli jinou osobou k jeho identifikaci. V této analýze hrají důležitou úlohu konkrétní souvislosti a okolnosti každého případu. Stanovisko se zabývá také „pseudonymizovanými údaji“ a použitím „údajů kódovaných pomocí klíče“ ve statistických šetřeních nebo farmaceutickém výzkumu (viz oddíl III bod 3).

- Čtvrtá složka – (fyzická) „osoba“ – je analyzována s ohledem na požadavek, že „osobní údaje“ musejí být o „žijících jednotlivcích“. Stanovisko se věnuje rovněž oblastem, které hraničí s údaji o zemřelých osobách, nenarozených dětech a právnických osobách (viz oddíl III bod 4).

Nakonec se ve stanovisku řeší otázka, co se stane, když se definice „osobních údajů“ na údaje nevztahuje. V takových případech mohou být k dispozici různá řešení, včetně vnitrostátních právních předpisů, které při dodržení ostatních právních předpisů Společenství mohou zasahovat i mimo oblast působnosti směrnice (viz oddíl IV).

Pracovní skupina vyzývá všechny zúčastněné strany, aby pečlivě prostudovaly pokyny obsažené v tomto stanovisku a braly je v potaz při výkladu a používání vnitrostátních právních předpisů v souladu se směrnicí 95/46/ES.

Členové pracovní skupiny, kteří jsou většinou představiteli vnitrostátních orgánů dozoru nad ochranou údajů, jsou odhodláni pokyny poskytnuté v tomto stanovisku dále rozvíjet v rámci oblastí svých pravomocí a zajišťovat řádné používání vnitrostátních právních předpisů svých zemí v souladu se směrnicí 95/46/ES.

Pracovní skupina má v úmyslu pokyny obsažené v tomto stanovisku uplatňovat a rozvíjet ve všech vhodných oblastech a pečlivě je zohledňovat ve své další práci, zejména při řešení otázek, jako je správa identit v rámci elektronické veřejné správy a elektronického zdravotnictví, jakož i v souvislosti s identifikací na základě rádiové frekvence (RFID). U druhého z uvedených témat pracovní skupina zamýšlí přispět k další analýze dopadu, jaký pravidla ochrany údajů mohou mít na využití RFID, a případných dodatečných opatření, která mohou být nezbytná k zajištění řádného respektování práv a zájmů na ochranu údajů v této oblasti.

Konečně by pracovní skupina také přivítala jakoukoli zpětnou vazbu od zúčastněných stran a orgánů dozoru ohledně jejich praktických zkušeností s pokyny v tomto stanovisku, včetně případných dalších příkladů vedle těch, které jsou uvedeny v tomto dokumentu. Skupina má v úmyslu se k tomuto tématu ve vhodné době vrátit s cílem dále posílit společné porozumění klíčovému pojmu osobní údaje a na tomto základě zajistit harmonizované používání a lepší provádění směrnice 95/46/ES a souvisejících právních předpisů Společenství.

Za pracovní skupinu

Peter SCHAAR
předseda

IV. Materiály z Úředního věstníku Evropské unie

Příloha Věstníku Úřadu pro ochranu osobních údajů (s. 2719 – 2741)

III

(Akty přijaté na základě Smlouvy o EU)

AKTY PŘIJATÉ NA ZÁKLADĚ HLAVY VI SMLOUVY O EU

ROZHODNUTÍ RADY 2007/533/SV

ze dne 12. června 2007

o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II)

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o Evropské unii, a zejména na čl. 30 odst. 1 písm. a) a b), čl. 31 odst. 1 písm. a) a b) a čl. 34 odst. 2 písm. c) této smlouvy,

s ohledem na návrh Komise,

s ohledem na stanovisko Evropského parlamentu [1],

vzhledem k těmto důvodům:

(1) Schengenský informační systém (dále jen „SIS“) zřízený v souladu s ustanoveními 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 [2] (dále jen „Schengenská úmluva“) a jeho rozšířená verze SIS 1+ představují nezbytný nástroj pro uplatňování ustanovení schengenského *acquis* začleněného do rámce Evropské unie.

(2) Vývoj SIS druhé generace (dále jen „SIS II“) byl svěřen Komisi na základě nařízení Rady (ES) č. 2424/2001 [3] a rozhodnutí Rady 2001/886/SVV ze dne 6. prosince 2001 o vývoji Schengenského informačního systému druhé generace (SIS II) [4]. SIS II nahradí SIS vytvořený na základě Schengenské úmluvy.

(3) Toto rozhodnutí představuje nezbytný právní základ pro řízení SIS II s ohledem na záležitosti spadající do oblasti působnosti Smlouvy o založení Evropské unie (dále jen „Smlouva o EU“). Nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 ze dne 20. prosince 2006 o zřízení, provozu a využívání SIS II [5] představuje nezbytný právní základ pro řízení SIS II s ohledem na záležitosti spadající do oblasti působnosti Smlouvy o založení Evropského společenství (dále jen „Smlouva o ES“).

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

(5) SIS II by měl představovat vyrovnávací opatření přispívající k udržení vysokého stupně bezpečnosti v rámci prostoru svobody, bezpečnosti a práva Evropské unie prostřednictvím podpory operativní spolupráce mezi policejními a justičními orgány v trestních věcech.

[1] Stanovisko ze dne 25. října 2006 (dosud nezveřejněné v Úředním věstníku).

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

[3] Úř. věst. L 328, 13.12.2001, s. 4.

[4] Úř. věst. L 328, 13.12.2001, s. 1.

[5] Úř. věst. L 381, 28.12.2006, s. 4.

(6) Je nezbytné konkrétně vymezit účely SIS II, jeho technickou architekturu a financování a stanovit pravidla týkající se jeho provozu, využívání a odpovědností, kategorií údajů vkládaných do systému, účelů jejich vkládání, kritérií jejich vkládání, orgánů oprávněných k přístupu do systému, propojení záznamů, jakož i další pravidla týkající se zpracování údajů a ochrany osobních údajů.

(7) SIS II by měl zahrnovat centrální systém (dále jen „centrální SIS II“) a vnitrostátní aplikace. Výdaje spojené s provozem centrálního SIS II a komunikační infrastruktury by měly být financovány ze souhrnného rozpočtu Evropské unie.

(8) Je nezbytné vytvořit příručku obsahující podrobná pravidla pro výměnu doplňujících informací týkajících se opatření, které záznam vyžaduje. Výměnu těchto informací by měly zajišťovat vnitrostátní orgány jednotlivých členských států.

(9) Během přechodného období by za provozní řízení centrálního SIS II a částí komunikační infrastruktury měla odpovídat Komise. V zájmu zajištění hladkého přechodu na SIS II však může přenést některé nebo všechny odpovědnosti na dva vnitrostátní veřejnoprávní subjekty. Z dlouhodobého hlediska a v návaznosti na posouzení dopadu obsahující věcnou analýzu alternativ z finančního, provozního a organizačního hlediska, a na legislativní návrhy Komise by měl být zřízen řídící orgán odpovědný za tyto úkoly. Přechodné období by mělo trvat nejdéle pět let ode dne použitelnosti tohoto rozhodnutí.

(10) SIS II by měl obsahovat záznamy o osobách hledaných za účelem zatčení a předání a hledaných za účelem zatčení a vydání. Je vhodné, aby byla kromě záznamů umožněna i výměna doplňujících informací nezbytných pro postupy předávání a vydávání. V SIS II by se měly zpracovávat zejména údaje uvedené v článku 8 rámcového rozhodnutí Rady 2002/584/SVV ze dne 13. června 2002 o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy [1].

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

(12) SIS II by měl obsahovat záznamy o pohřešovaných osobách k zajištění jejich ochrany nebo předcházení nebezpečí hrozícího těmto osobám, záznamy o osobách hledaných za účelem soudního řízení, záznamy o osobách a věcech pořízené pro účely skrytých kontrol nebo zvláštních kontrol a záznamy o věcech hledaných za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení.

(13) Záznamy by v SIS II měly být uchovávány nanejvýš po dobu nezbytnou pro splnění účelů, pro které byly poskytnuty. Obecnou zásadou je, že záznamy o osobách by měly být z SIS II automaticky vymazány po uplynutí tří let. Záznamy o věcech pořízené pro účely skrytých kontrol nebo zvláštních kontrol by měly být ze SIS II automaticky vymazány po uplynutí pěti let. Záznamy o věcech hledaných za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení by měly být z SIS II automaticky vymazány po uplynutí deseti let. Rozhodnutí o uchování záznamů o osobách by měla vycházet z komplexního individuálního posouzení. Členské státy by měly během vymezeného období záznamy o osobách přezkoumat a měly by vést statistiku o počtu záznamů o osobách, u nichž byla doba uchovávání prodloužena.

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

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

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

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

[1] Úř. věst. L 190, 18.7.2002, s. 1.

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

(19) Všechny členské státy ratifikovaly úmluvu Rady Evropy ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat. Úmluva připouští v rámci určitých mezí výjimky a omezení práv a povinností, které úmluva stanovuje. Osobní údaje zpracované v rámci provádění tohoto rozhodnutí by měly být chráněny v souladu se zásadami uvedené úmluvy. Pokud je to nezbytné, je třeba zásady uvedené v úmluvě doplnit nebo objasnit v tomto rozhodnutí.

(20) Při zpracování osobních údajů policejními orgány za použití tohoto rozhodnutí by měly být vzaty v úvahu zásady obsažené v doporučení č. R (87) 15 Výboru ministrů Rady Evropy ze dne 17. září 1987 o používání osobních údajů v policejní oblasti.

(21) Komise předložila Radě návrh rámcového rozhodnutí o ochraně údajů zpracovávaných v rámci policejní a soudní spolupráce v trestních záležitostech, které by mělo být schváleno do konce roku 2006 a uplatňováno na osobní údaje zpracovávané v rámci Schengenského informačního systému druhé generace a související výměnu doplňujících informací podle tohoto rozhodnutí.

(22) 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 [1], a zejména ta jeho ustanovení, která se týkají důvěrné povahy a bezpečnosti zpracovávání, se vztahuje na zpracovávání osobních údajů orgány nebo institucemi Společenství při plnění jejich úkolů jakožto orgánů odpovědných za provozní řízení SIS II v rámci výkonu činností, z nichž všechny nebo část spadá do oblasti působnosti práva Společenství. Část zpracování osobních údajů v SIS II spadá do oblasti působnosti práva Společenství. V zájmu soudržného a stejnorodého uplatňování pravidel ochrany základních práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů je třeba vysvětlit, že pokud Komise zpracovává osobní údaje za použití tohoto rozhodnutí, vztahuje se na ni nařízení (ES) č. 45/2001. Pokud je to nezbytné, měly by se zásady uvedené v nařízení (ES) č. 45/2001 doplnit nebo objasnit v tomto rozhodnutí.

(23) Pokud jde o důvěrnost, měla by se na úředníky nebo ostatní zaměstnance Evropských společenství zaměstnané a pracující v souvislosti se SIS II vztahovat příslušná ustanovení služebního řádu úředníků Evropských společenství a pracovní řád ostatních zaměstnanců Evropských společenství.

(24) Je vhodné, aby zákonnost zpracovávání osobních údajů členskými státy sledovaly vnitrostátní orgány dozoru, zatímco evropský inspektor ochrany údajů jmenovaný podle rozhodnutí Evropského parlamentu a Rady 2004/55/ES ze dne 22. prosince 2003 o jmenování nezávislého kontrolního orgánu podle článku 286 Smlouvy o ES [2] by měl sledovat činnosti orgánů a institucí Společenství související se zpracováváním osobních údajů s ohledem na omezené úkoly orgánů a institucí Společenství ve vztahu k samotným údajům.

(25) Členské státy i Komise by měly vypracovat bezpečnostní plán s cílem usnadnit provádění bezpečnostních povinností a měly by vzájemně spolupracovat s cílem společně řešit bezpečnostní otázky.

(26) Na zpracování údajů SIS II Europolem se vztahují ustanovení Úmluvy o zřízení Evropského policejního úřadu ze dne 26. července 1995 [3] (dále jen „Úmluva o Europolu"), týkající se ochrany údajů, včetně pravomocí Společného kontrolního orgánu zřízeného podle Úmluvy o Europolu sledovat činnosti Europolu a odpovědnost za jakékoliv protiprávní zpracování osobních údajů ze strany Europolu.

(27) Na zpracování údajů SIS II Eurojustem se vztahují ustanovení rozhodnutí 2002/187/SVV ze dne 28. února 2002 o zřízení Evropské jednotky pro justiční spolupráci (Eurojust) za účelem posílení boje proti závažné trestné činnosti [4], týkající se ochrany údajů, včetně pravomocí Společného kontrolního orgánu zřízeného podle uvedeného rozhodnutí sledovat činnosti Eurojustu a odpovědnost za jakékoliv protiprávní zpracování osobních údajů ze strany Eurojustu.

[1] Úř. věst. L 8, 12.1.2001, s. 1.

[2] Úř. věst. L 12, 17.1.2004, s. 47.

[3] Úř. věst. C 316, 27.11.1995, s. 2.

[4] Úř. věst. L 63, 6.3.2002, s. 1.

(28) Za účelem zajištění transparentnosti by měla Komise, nebo řídící orgán, je-li zřízen, každé dva roky vypracovat zprávu o technickém fungování centrálního SIS II a komunikační infrastruktury, včetně jejího zabezpečení, a o výměně doplňujících informací. Každé čtyři roky by měla Komise předložit celkové vyhodnocení.

(29) Ustanoveními tohoto rozhodnutí nelze vyčerpávajícím způsobem upravit některé aspekty SIS II, jako jsou technická pravidla pro vkládání údajů, včetně údajů potřebných pro vložení záznamu, aktualizace, výmaz a vyhledávání, pravidla týkající se slučitelnosti a priority záznamů, označování, odkazy mezi záznamy a výměna doplňujících informací v důsledku jejich technické podstaty, podrobného charakteru a potřeby pravidelné aktualizace. Prováděcí pravomoci, pokud jde o tyto aspekty, by proto měly být svěřeny Komisi. Technická pravidla týkající se vyhledávání v záznamech by měla přihlížet k řádnému fungování vnitrostátních aplikací. Na základě posouzení dopadu předloženého Komisí by mělo být rozhodnuto, v jakém rozsahu může být řídící orgán, jakmile bude zřízen, odpovědný za prováděcí opatření.

(30) Toto rozhodnutí by mělo vymezit postup pro přijímání opatření nezbytných k jeho provádění. Postup pro přijímání prováděcích opatření podle tohoto rozhodnutí a nařízení (ES) č. 1987/2006 by měl být totožný.

(31) Je vhodné stanovit přechodná ustanovení, pokud jde o záznamy pořízené v SIS 1+, které mají být přeneseny do SIS II. Některá ustanovení schengenského *acquis* by měla dále platit po omezené období, dokud členské státy nepřezkoumají slučitelnost těchto záznamů s novým právním rámcem. Přednostně je třeba přezkoumat slučitelnost záznamů o osobách. Navíc by jakákoliv změna, doplnění, oprava nebo aktualizace záznamu přeneseného ze SIS 1+ do SIS II, a jakýkoliv pozitivní nález takového záznamu, měla podnítit okamžité posouzení jeho souladu s ustanoveními tohoto rozhodnutí.

(32) Je nezbytné stanovit zvláštní ustanovení, pokud jde o zbývající část rozpočtu vyčleněného na provoz SIS, která není součástí souhrnného rozpočtu Evropské unie.

(33) Protože cílů navrhované akce, zejména vytvoření a řízení společného informačního systému, nemůže být dosaženo uspokojivě na úrovni členských států, a může jich být proto z důvodu rozsahu a účinků činnosti lépe dosaženo na úrovni Evropské unie, může Rada přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o ES a uvedenou v článku 2 Smlouvy o EU. V souladu se zásadou proporcionality podle článku 5 Smlouvy o ES nepřekročí toto rozhodnutí rámec toho, co je nezbytné pro dosažení těchto cílů.

(34) Toto rozhodnutí ctí základní práva a zachovává zásady uznávané zejména v Listině základních práv Evropské unie.

(35) Spojené království se účastní tohoto rozhodnutí v souladu s článkem 5 Protokolu o začlenění schengenského *acquis* do rámce Evropské unie, připojeného ke Smlouvě o EU a Smlouvě o ES, a v souladu s čl. 8 odst. 2 rozhodnutí Rady 2000/365/ES ze dne 29. května 2000 o žádosti Spojeného království Velké Británie a Severního Irska, aby se na ně vztahovala některá ustanovení schengenského *acquis* [1].

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

(37) Toto rozhodnutí se nedotýká opatření pro částečnou účast Spojeného království a Irska na schengenském *acquis*, jak jsou vymezena pro Spojené království v rozhodnutí 2000/365/ES a pro Irsko v rozhodnutí 2002/192/ES.

(38) Pokud jde o Island a Norsko, rozvíjí toto rozhodnutí 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* [3], která spadají do oblasti uvedené v čl. 1 bodu G rozhodnutí Rady 1999/437/ES [4] o některých opatřeních pro uplatňování dané dohody.

(39) Je třeba přijmout opatření umožňující zástupcům Islandu a Norska zapojení do práce výborů, jež jsou nápomocny Komisi při výkonu jejích prováděcích pravomocí. Takové opatření je uvedeno ve výměně dopisů mezi Radou Evropské unie a Islandskou republikou a Norským královstvím o výborech, které jsou nápomocny Evropské komisi při výkonu jejích prováděcích pravomocí [5], připojené k výše uvedené dohodě.

---

[1] Úř. věst. L 131, 1.6.2000, s. 43.
[2] Úř. věst. L 64, 7.3.2002, s. 20.
[3] Úř. věst. L 176, 10.7.1999, s. 36.
[4] Úř. věst. L 176, 10.7.1999, s. 31.
[5] Úř. věst. L 176, 10.7.1999, s. 53.

(40) Pokud jde o Švýcarsko, rozvíjí toto nařízení ta ustanovení schengenského *acquis* ve smyslu dohody podepsané mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis*, která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí 1999/437/ES ve spojení s čl. 4 odst. 1 rozhodnutí Rady 2004/849/ES [1] a 2004/860/ES [2].

(41) Je třeba přijmout opatření umožňující zástupcům Švýcarska zapojení do práce výborů, jež jsou nápomocny Komisi při výkonu jejích prováděcích pravomocí. Takové opatření je předmětem výměny dopisů mezi Společenstvím a Švýcarskem, připojené k uvedené dohodě.

(42) Toto rozhodnutí představuje akt navazující na schengenské *acquis* nebo s ním jinak související ve smyslu čl. 3 odst. 2 aktu o přistoupení z roku 2003 a čl. 4 odst. 2 aktu o přistoupení z roku 2005.

(43) Toto rozhodnutí by se mělo vztahovat na Spojené království, Irsko a Švýcarsko ke dni určenému v souladu s postupy stanovenými v příslušných nástrojích týkajících se použití schengenského *acquis* na tyto státy,

ROZHODLA TAKTO:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Zřízení a obecný účel SIS II

1. Zřizuje se Schengenský informační systém druhé generace (dále jen „SIS II“).

2. Účelem SIS II je zajistit v souladu s tímto rozhodnutím na územích členských států vysokou úroveň bezpečnosti v rámci prostoru svobody, bezpečnosti a práva Evropské unie, včetně udržování veřejné bezpečnosti a veřejného pořádku a zajišťování bezpečnosti, a uplatňovat ustanovení hlavy IV části třetí Smlouvy o ES, pokud jde o pohyb osob na jejich územích, s využitím informací předávaných prostřednictvím tohoto systému.

Článek 2

Oblast působnosti

1. Toto rozhodnutí zavádí podmínky a postupy pro vkládání a zpracovávání záznamů v SIS II o osobách a věcech a pro výměnu doplňujících informací a dalších údajů za účelem policejní a justiční spolupráce v trestních věcech.

2. Toto rozhodnutí též stanoví pravidla o technické architektuře SIS II, o povinnostech členských států a řídícího orgánu uvedeného v článku 15, o obecném zpracování údajů, o právech dotčených osob a o odpovědnosti za škodu.

Článek 3

Definice

1. Pro účely tohoto rozhodnutí se rozumí:

a) „záznamem“ soubor údajů vložených do SIS II umožňující příslušným orgánům identifikovat osobu nebo věc s ohledem na konkrétní opatření, které má být přijato;

b) „doplňujícími informacemi“ informace, které nejsou uložené v SIS II, ale souvisejí se záznamy SIS II a které se vyměňují:

   i) s cílem umožnit členským státům vzájemné poskytování konzultací či informací při vkládání záznamu,

   ii) po pozitivním nálezu, aby bylo možné přijmout vhodné opatření,

   iii) pokud nelze požadované opatření přijmout,

   iv) pokud se jedná o kvalitu údajů v SIS II,

   v) pokud se jedná o slučitelnost a prioritu záznamů,

   vi) pokud se jedná o práva přístupu;

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

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

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

d) „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo určit;

e) „zpracováním osobních údajů“ (dále jen „zpracování“) jakýkoli úkon nebo soubor úkonů, které jsou prováděny s osobními údaji pomocí automatizovaných postupů či bez nich, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, nahlížení, používání, sdělování prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnávání či kombinování, jakož i blokování, výmaz nebo znehodnocení údajů.

2. Jakýkoliv odkaz na ustanovení rámcového rozhodnutí 2002/584/SVV se považuje rovněž za odkaz na odpovídající ustanovení dohod uzavřených mezi Evropskou unií a třetími státy na základě článků 24 a 38 Smlouvy o EU za účelem předávání osob na základě zatýkacího rozkazu, které stanoví předávání tohoto zatýkacího rozkazu prostřednictvím Schengenského informačního systému.

Článek 4

Technická architektura a způsoby provozování SIS II

1. Druhá generace Schengenského informačního systému (SIS II) sestává z:

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

— technické podpůrné funkce (dále jen „CS-SIS“) obsahující databázi, dále jen „databázi SIS II“,

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

b) vnitrostátního systému (dále jen „N.SIS II“) v každém členském státě, sestávajícího z vnitrostátních datových systémů, které komunikují s centrálním SIS II. Vnitrostátní systém N.SIS II může obsahovat soubor údajů (dále jen „vnitrostátní kopie“) obsahující úplnou nebo částečnou kopii databáze SIS II;

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

2. Údaje SIS II se vkládají, aktualizují, vymazávají a vyhledávají prostřednictvím různých systémů N.SIS II. Vnitrostátní kopie je k dispozici za účelem automatizovaného vyhledávání na území každého členského státu, jenž takovou kopii používá. Vyhledávání v souborech údajů N.SIS II jiných členských států není umožněno.

3. Technická podpůrná funkce CS-SIS, jež vykonává technický dohled a správu, se nachází ve Štrasburku (Francie) a záložní CS-SIS, jež je schopna zajistit všechny funkce hlavního CS-SIS v případě její poruchy, se nachází v Sankt Johann im Pongau (Rakousko).

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

a) on-line aktualizaci vnitrostátních kopií;

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

c) počáteční nastavení a opětovné zavedení vnitrostátních kopií.

Článek 5

Náklady

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

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

3. Náklady na zřízení, provoz a údržbu jednotlivých N.SIS II ponese dotyčný členský stát.

KAPITOLA II

POVINNOSTI ČLENSKÝCH STÁTŮ

Článek 6

Vnitrostátní systémy

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

Článek 7

Úřad N.SIS II a centrála SIRENE

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

Tento orgán je odpovědný za plynulý provoz a zabezpečení N.SIS II, zajišťuje přístup příslušných orgánů k SIS II a přijímá nezbytná opatření pro dodržování ustanovení tohoto rozhodnutí.

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

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

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

3. Členské státy uvědomí řídící orgán o svém úřadu N.SIS II a o své centrále SIRENE. Řídící orgán zveřejní jejich seznam spolu se seznamem uvedeným v čl. 46 odst. 8.

Článek 8

Výměna doplňujících informací

1. Doplňující informace se vyměňují v souladu s ustanoveními příručky SIRENE a prostřednictvím komunikační infrastruktury. Pokud by komunikační infrastruktura nebyla dostupná, členské státy mohou k výměně doplňujících informací použít jiné náležitě zabezpečené technické prostředky.

2. Doplňující informace se použijí pouze pro účely, pro které byly předány.

3. Žádosti jiných členských států o doplňující informace musí být vyřízeny co nejdříve.

4. Aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán, přijmou se postupem podle článku 67podrobná pravidla pro výměnu doplňujících informací v podobě příručky SIRENE.

Článek 9

Technický soulad

1. K zajištění okamžitého a účinného přenosu údajů postupuje každý členský stát při zřizování svého N.SIS II podle protokolů a technických postupů stanovených pro zajištění souladu mezi CS-SIS a N-SIS II. Tyto protokoly a technické postupy se stanoví postupem podle článku 67, aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán.

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

Článek 10

Bezpečnost – členské státy

1. Každý členský stát přijme, ve vztahu ke své N.SIS II, nezbytná opatření, včetně přijetí bezpečnostního plánu, aby:

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

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

c) zabránil neoprávněnému čtení, kopírování, pozměňování či vyjímání nosičů dat (kontrola nosičů dat);

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

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

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

g) zajistil, aby všechny orgány s oprávněním přístupu do SIS II nebo k zařízením pro zpracování údajů vytvořily profily popisující funkce a povinnosti osob, jež jsou oprávněny k údajům přistupovat a údaje zadávat, aktualizovat, mazat a vyhledávat, a aby tyto profily bezodkladně na základě žádosti zpřístupnily vnitrostátním orgánům dozoru uvedeným v článku 60 (profily pracovníků);

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

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

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

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

2. Členské státy přijmou opatření rovnocenná opatřením uvedeným v odstavci 1, pokud jde o bezpečnost v souvislosti s výměnou doplňujících informací.

Článek 11

Důvěrnost – členské státy

Každý členský stát použije v souladu se svými vnitrostátními právními předpisy svá pravidla 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 zaměstnanecký poměr, nebo poté, co dotyčné subjekty ukončí svou činnost.

Článek 12

Vedení evidence na vnitrostátní úrovni

1. Členské státy, které nepoužívají vnitrostátní kopie, jsou povinny zajistit, aby každý přístup k osobním údajům a všechny výměny osobních údajů s CS-SIS byly evidovány v N.SIS II za účelem kontroly, zda je vyhledávání zákonné či nikoli, za účelem sledování zákonnosti zpracovávání údajů, pro vlastní kontrolu, pro zajištění řádného fungování N.SIS II, neporušenosti údajů a jejich zabezpečení.

2. Členské státy používající vnitrostátní kopie zajistí, aby každý vstup do údajů SIS II a každá výměna těchto údajů byly zaznamenány pro účely určené v odst. 1. To neplatí pro postupy uvedené v čl. 4 odst. 4.

3. Evidence obsahuje zejména historii záznamů, datum a čas předání údajů, údaje použité pro provedení vyhledávání, odkaz na předávané údaje a název jak příslušného orgánu, tak osoby odpovědné za zpracování údajů.

4. Evidenci lze použít pouze k účelu uvedenému v odstavcích 1 a 2 a vymaže se nejdříve po uplynutí jednoho roku a nejpozději po třech letech od jejího vytvoření. Evidence obsahující historii záznamů musí být smazána po uplynutí jednoho roku až tří let od výmazu záznamů.

5. Evidenci lze uchovat déle, je-li potřebná pro postupy kontroly, které již započaly.

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

Článek 13

Vlastní kontrola

Členské státy zajistí, aby každý orgán s oprávněním k přístupu k údajům SIS II učinil opatření nezbytná k zajištění dodržování tohoto rozhodnutí a spolupracuje, pokud je to nutné, s vnitrostátním orgánem dozoru.

Článek 14

Odborná příprava zaměstnanců

Dříve, než zaměstnanci orgánů s právem přístupu do SIS II obdrží povolení zpracovávat údaje uložené v SIS II, absolvují odpovídající odbornou přípravu týkající se zabezpečení údajů a pravidel o ochraně údajů a jsou informováni o jakýchkoliv příslušných trestných činech a sankcích.

KAPITOLA III

POVINNOSTI ŘÍDÍCÍHO ORGÁNU

Článek 15

Provozní řízení

1. Po přechodném období řídící orgán financovaný ze souhrnného rozpočtu Evropské unie, odpovídá za provozní řízení centrálního SIS II. Řídící orgán ve spolupráci s členskými státy zajistí na základě analýzy nákladů a přínosů, aby pro centrální SIS II byla vždy využívána nejlepší dostupná technologie.

2. Řídící orgán odpovídá též za následující úkoly spojené s komunikační infrastrukturou:

a) dohled;

b) zabezpečení;

c) koordinace vztahů mezi členskými státy a poskytovatelem.

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

a) úkoly související s plněním rozpočtu;

b) pořizování a obnovu;

c) smluvní záležitosti.

4. Během přechodného období, než se řídící orgán uvedený v odstavci 1 ujme svých povinností, je za provozní řízení centrálního SIS II odpovědná Komise. Komise může v souladu s nařízením Rady (ES, Euratom) č. 1605/2002 ze dne 25. června 2002, kterým se stanoví finanční nařízení o souhrnném rozpočtu Evropských společenství [1], svěřit provádění tohoto řízení, jakož i úkolů souvisejících s plněním rozpočtu, vnitrostátním veřejnoprávním subjektům ve dvou různých zemích.

5. Každý vnitrostátní veřejnoprávní subjekt uvedený v odstavci 4 musí splňovat zejména tato výběrová kritéria:

a) musí prokázat dlouhodobou zkušenost v provozování rozsáhlého informačního systému s funkcemi uvedenými v čl. 4 odst. 4;

b) musí mít značnou odbornou znalost, pokud jde o obsluhu a požadavky na zabezpečení informačního systému srovnatelného s funkcemi uvedenými v čl. 4 odst. 4;

c) musí mít dostatečný počet zkušených pracovníků, kteří mají patřičnou odbornou a jazykovou způsobilost pro práci v prostředí mezinárodní spolupráce, jakou vyžaduje SIS II;

d) musí mít k dispozici bezpečnou a na míru postavenou infrastrukturu zařízení, která je zejména schopná zálohovat a zaručit nepřetržitou funkčnost rozsáhlých IT systémů, a

e) jeho administrativní prostředí mu musí umožňovat řádně plnit jeho úkoly a vyhnout se jakémukoli střetu zájmů.

6. Před jakýmkoli takovým pověřením podle odstavce 4 a poté v pravidelných intervalech oznámí Komise Evropskému parlamentu a Radě podmínky pověření, přesný rozsah pověření a orgány, které jsou plněním úkolů pověřeny.

7. V případě, že Komise provede pověření podle odst. 4 během přechodného období, zajistí, aby toto pověření plně respektovalo meze stanovené institucionálním systémem daným ve Smlouvě o ES. Zejména zajistí, aby toto pověření nepříznivým způsobem neovlivnilo případný účinný kontrolní mechanismus podle práva Evropské unie, ať se jedná o Soudní dvůr, Účetní dvůr nebo evropského inspektora ochrany údajů.

8. Provozní řízení centrálního SIS II sestává ze všech úkolů nezbytných pro zachování funkčnosti centrálního SIS II 24 hodiny denně 7 dní v týdnu v souladu s tímto rozhodnutím, zejména z údržby a technického rozvoje nezbytného pro plynulý chod systému.

[1] Úř. věst. L 248, 16.9.2002, s. 1.

Článek 16

Bezpečnost

1. Řídící orgán ve vztahu k centrálnímu SIS II a Komise ve vztahu ke komunikační infrastruktuře přijmou nezbytná opatření, včetně bezpečnostního plánu, aby:

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

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

c) zabránily neoprávněnému čtení, kopírování, pozměňování či vyjímání nosičů dat (kontrola nosičů dat);

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

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

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

g) vytvořily profily popisující funkce a povinnosti osob, jež jsou oprávněny k údajům nebo k zařízením pro zpracování údajů přistupovat, a aby tyto profily na žádost bezodkladně zpřístupnily evropskému inspektorovi ochrany údajů uvedenému v článku 61 (profily pracovníků);

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

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

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

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

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

Článek 17

Důvěrnost – řídící orgán

1. Aniž je dotčen článek 17 služebního řádu úředníků Evropských společenství, řídící orgán použije odpovídající pravidla služebního tajemství nebo jiné srovnatelné povinnosti zachování důvěrnosti na všechny své zaměstnance, kteří musí pracovat s údaji SIS II s použitím norem srovnatelných s normami stanovenými v článku 11 tohoto rozhodnutí. Tato povinnost trvá i poté, co dotyčné osoby opustí svůj úřad nebo zaměstnanecký poměr, nebo poté, co ukončí svou činnost.

2. Řídící orgán přijme opatření rovnocenná opatřením podle odstavce 1, pokud jde o důvěrnost při výměně doplňujících informací prostřednictvím komunikační infrastruktury.

Článek 18

Vedení evidence na centrální úrovni

1. Řídící orgán zajistí, aby každý přístup k osobním údajům a všechny výměny osobních údajů v rámci CS-SIS byly evidovány pro účely uvedené v čl. 12 odst. 1 a 2.

2. Evidence obsahuje zejména historii záznamů, datum a čas přenosu údajů, údaje použité pro provedení vyhledávání, odkaz na předávané údaje a název příslušného orgánu odpovědného za zpracování údajů.

3. Evidenci lze použít pouze k účelům uvedeným v odstavci 1 a vymaže se nejdříve po uplynutí jednoho roku a nejpozději po třech letech od jejího vytvoření. Evidence obsahující historii záznamů musí být smazána po uplynutí jednoho roku až tří let od výmazu záznamů.

4. Evidenci lze uchovat déle, je-li potřebná pro postupy kontroly, které již započaly.

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

Článek 19

Informační kampaň

Komise, ve spolupráci s vnitrostátními orgány dozoru a s evropským inspektorem ochrany údajů, spustí při zahájení provozu SIS II informační kampaň, která informuje veřejnost o účelech systému, o údajích, které se v něm ukládají, o orgánech, které k němu mají přístup a o právech osob. Po jeho zřízení řídící orgán, ve spolupráci s vnitrostátními orgány dozoru a evropským inspektorem ochrany údajů, tyto kampaně pravidelně opakuje. Členské státy, ve spolupráci se svými vnitrostátními orgány dozoru, navrhnou a provedou nezbytné politiky s cílem obecně informovat své občany o SIS II.

KAPITOLA IV

KATEGORIE ÚDAJŮ A OZNAČOVÁNÍ ZÁZNAMŮ

Článek 20

Kategorie údajů

1. Aniž je dotčen čl. 8 odst. 1 nebo ustanovení tohoto rozhodnutí, jež stanoví uchovávání doplňujících údajů, obsahuje SIS II pouze ty kategorie údajů, které dodává každý z členských států a které jsou potřebné pro účely uvedené v článcích 26, 32, 34, 36 a 38.

2. Kategorie údajů jsou následující:

a) osoby, u kterých byl pořízen záznam;

b) věci uvedené v článcích 36 a 38.

3. O osobách, o kterých byl pořízen záznam, se vloží nanejvýš tyto údaje:

a) příjmení a jméno/jména, jméno při narození a dříve užívaná jména, případně alias, které může být vedeno zvlášť;

b) jakékoli zvláštní objektivní a nezměnitelné tělesné znaky;

c) datum a místo narození;

d) pohlaví;

e) fotografie;

f) otisky prstů;

g) státní příslušnost/příslušnosti;

h) údaj o tom, zda je dotyčná osoba ozbrojena, má sklon k násilí nebo jde o uprchlou osobu;

i) důvod záznamu;

j) orgán pořizující záznam;

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

l) opatření, která je třeba přijmout;

m) odkaz/odkazy podle článku 52 na další záznamy pořízené v SIS II;

n) druh trestného činu.

4. Technická pravidla potřebná pro vložení, aktualizaci, vymazávání a vyhledávání údajů uvedených v odstavcích 2 a 3 se stanoví postupem podle článku 67, aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán.

5. Technická pravidla potřebná pro vyhledávání údajů podle odstavce 3 jsou podobná pro vyhledávání v CS-SIS, ve vnitrostátních kopiích i v kopiích pro technické účely podle čl. 46 odst. 2.

Článek 21

Proporcionalita

Členský stát před pořízením záznamu ověří, zda je daný případ dostatečně přiměřený, relevantní a závažný pro vložení záznamu do SIS II.

Článek 22

Zvláštní pravidla pro fotografie a otisky prstů

Fotografie a otisky prstů uvedené v čl. 20 odst. 3 písm. e) a f) se použijí podle těchto ustanovení:

a) fotografie a otisky prstů se vloží pouze po provedení zvláštní kontroly kvality s cílem zjistit, zda jsou splněny minimální normy kvality údajů. Upřesnění zvláštní kontroly kvality se stanoví postupem podle článku 67, aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán;

b) fotografie a otisky prstů se použijí pouze k potvrzení totožnosti osob, které byly nalezeny na základě alfanumerického vyhledávání v SIS II;

c) jakmile to bude z technického hlediska možné, lze též použít otisky prstů k určení totožnosti osoby na základě jejího biometrického identifikátoru. Před zavedením této funkce do SIS II předloží Komise zprávu o dostupnosti a připravenosti potřebné technologie, kterou konzultuje s Evropským parlamentem.

Článek 23

Požadavek na vložení záznamu

1. Záznamy o osobách nemohou být vloženy bez údajů uvedených v čl. 20 odst. 3 písm. a), d), l) a případně k).

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

Článek 24

Obecná ustanovení týkající se označování záznamů

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

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

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

Článek 25

Označování záznamů za účelem zatčení a předání

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

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

KAPITOLA V

ZÁZNAMY O OSOBÁCH HLEDANÝCH ZA ÚČELEM ZATČENÍ A PŘEDÁNÍ NEBO VYDÁNÍ

Článek 26

Cíle a podmínky pořizování záznamů

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

2. Údaje o osobách hledaných za účelem zatčení a předání se vkládají na základě zatýkacích rozkazů vydaných v souladu s dohodami uzavřenými mezi Evropskou unií a třetími státy na základě článků 24 a 38 Smlouvy o EU za účelem předání osob na základě zatýkacího rozkazu, které stanoví předávání tohoto zatýkacího rozkazu prostřednictvím Schengenského informačního systému.

Článek 27

Další údaje o osobách hledaných za účelem zatčení a předání

1. V případě osoby hledané za účelem zatčení a předání na základě evropského zatýkacího rozkazu vloží pořizující členský stát do SIS II kopii originálu evropského zatýkacího rozkazu.

2. Pořizující členský stát může vložit kopii překladu evropského zatýkacího rozkazu do jednoho nebo několika dalších úředních jazyků orgánů Evropské unie.

Článek 28

Doplňující informace o osobách hledaných za účelem zatčení a předání

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

Článek 29

Doplňující informace o osobách hledaných za účelem zatčení a vydání

1. Členský stát, který vložil do SIS II záznam za účelem vydání, sdělí prostřednictvím výměny doplňujících informací všem členským státům tyto údaje:

a) orgán, který vydal žádost o zatčení;

b) zda je k dispozici zatýkací rozkaz nebo akt se stejným právním účinkem nebo pravomocný rozsudek;

c) podstatu a právní kvalifikaci trestného činu;

d) popis okolností, za kterých byl trestný čin spáchán, včetně doby, místa činu a stupně účasti dotyčné osoby na něm;

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

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

2. Údaje uvedené v odstavci 1 se nesdělí, pokud byly již poskytnuty údaje uvedené v článcích 27 nebo 28 a pokud jsou považovány za dostačující pro výkon záznamu dotčeným členským státem.

Článek 30

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

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

Článek 31

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

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

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

KAPITOLA VI

ZÁZNAMY O POHŘEŠOVANÝCH OSOBÁCH

Článek 32

Cíle a podmínky pořizování záznamů

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

2. Je možné vkládat tyto kategorie pohřešovaných osob:

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

   i) v zájmu své vlastní ochrany,

   ii) za účelem předcházení nebezpečí hrozícího těmto osobám;

b) pohřešované osoby, které nemusí být umístěny pod dočasnou ochranu.

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

4. Odstavce 1, 2 a 3 se použijí zejména na nezletilé osoby.

5. Členské státy zajistí, aby údaje vložené do SIS II uváděly, do které z kategorií zmíněných v odstavci 2 pohřešovaná osoba patří.

Článek 33

Výkon opatření na základě záznamu

1. Je-li nalezena osoba uvedená v článku 32, příslušné orgány sdělí s výhradou odstavce 2 členskému státu pořizujícímu záznam jejich místo pobytu. V případech uvedených v čl. 32 odst. 2 písm. a) mohou umístit osoby pod ochranu a zabránit jim tak v tom, aby pokračovaly v cestě, pokud to dovolují vnitrostátní právní předpisy.

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

KAPITOLA VII

ZÁZNAMY O OSOBÁCH ZA ÚČELEM ZAJIŠTĚNÍ JEJICH SPOLUPRÁCE V SOUDNÍM ŘÍZENÍ

Článek 34

Cíle a podmínky pořizování záznamů

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

a) svědcích;

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

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

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

Článek 35

Výkon opatření na základě záznamu

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

KAPITOLA VIII

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

Článek 36

Cíle a podmínky pořizování záznamů

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

2. Tento záznam může být pořízen pro účely trestního stíhání a předcházení ohrožení veřejné bezpečnosti, pokud:

a) existuje důvodné podezření, že osoba zamýšlí spáchat nebo páchá závažný trestný čin, jako jsou trestné činy uvedené v čl. 2 odst. 2 rámcového rozhodnutí 2002/584/SVV, nebo

b) z celkového posouzení osoby, zejména na základě dosud spáchaných trestných činů, lze předpokládat, že se i v budoucnosti dopustí závažných trestných činů, jako jsou trestné činy uvedené v čl. 2 odst. 2 rámcového rozhodnutí 2002/584/SVV.

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

4. Záznamy o vozidlech, plavidlech, letadlech a kontejnerech mohou být pořízeny, pokud existuje důvodné podezření o jejich spojení se závažnými trestnými činy uvedenými v odstavci 2 nebo závažnými ohroženími uvedenými v odstavci 3.

Článek 37

Provádění opatření na základě záznamu

1. Pro účely skrytých kontrol nebo zvláštních kontrol mohou být při provádění hraniční kontroly a jiných policejních a celních kontrol v členském státě shromažďovány a předávány orgánu pořizujícímu záznam všechny nebo některé z následujících informací:

a) skutečnost, že osoba, o které byl pořízen záznam nebo vozidlo, plavidlo, letadlo nebo kontejner, o němž byl pořízen záznam, byly nalezeny;

b) místo, čas nebo důvod kontroly;

c) trasa a cíl cesty;

d) osoby, které doprovázejí dotyčné osoby nebo cestující ve vozidle, na plavidle nebo v letadle, o kterých lze důvodně předpokládat, že jsou s dotyčnou osobou spojeny;

e) použité vozidlo, plavidlo, letadlo nebo kontejner;

f) převážené věci;

g) okolnosti, za jakých byly osoba nebo vozidlo, plavidlo, letadlo nebo kontejner nalezeny.

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

3. Při shromažďování informací uvedených v odstavci 1 přijmou členské státy opatření, aby nebyla ohrožena utajená povaha kontroly.

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

KAPITOLA IX

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

Článek 38

Cíle a podmínky pořizování záznamů

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

2. Vkládají se tyto kategorie snadno identifikovatelných věcí:

a) vozidla s motorem o obsahu válců nad 50 ccm, plavidla a letadla;

b) přívěsy o pohotovostní hmotnosti přesahující 750 kg, obytné přívěsy, průmyslová zařízení, závěsné motory a kontejnery;

c) střelné zbraně;

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

e) odcizené, neoprávněně užívané, pohřešované nebo neplatné doklady totožnosti, jako jsou pasy, občanské průkazy, řidičské průkazy, povolení k pobytu a cestovní doklady, jež byly vydané;

f) odcizená, neoprávněně užívaná, pohřešovaná nebo neplatná osvědčení o registraci vozidel a státní poznávací značky;

g) bankovky (evidované);

h) odcizené, neoprávněně užívané, pohřešované nebo neplatné cenné papíry a platební nástroje, jako jsou šeky, kreditní karty, dluhopisy, akcie a podíly.

3. Technická pravidla potřebná pro vkládání, aktualizaci, vymazávání a vyhledávání údajů uvedených v odstavci 2 se stanoví postupem podle článku 67, aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán.

Článek 39

Provádění opatření na základě záznamu

1. Pokud se při vyhledávání zjistí záznam o věci, která byla nalezena, spojí se orgán, který zjistil shodu dvou položek údajů, s orgánem, který pořídil záznam s cílem dohodnout vhodná opatření. Za tímto účelem mohou být v souladu s tímto rozhodnutím sdělovány i osobní údaje.

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

3. Opatření, jež má přijmout členský stát, který věc nalezl, musí být v souladu s jeho vnitrostátními právními předpisy.

KAPITOLA X

PRÁVO PŘÍSTUPU K ZÁZNAMŮM A JEJICH UCHOVÁVÁNÍ

Článek 40

Orgány mající právo přístupu k záznamům

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

a) ochranu hranic, v souladu s nařízením Evropského parlamentu a Rady (ES) č. 562/2006 ze dne 15. března 2006, kterým se stanoví kodex Společenství o pravidlech upravujících přeshraniční pohyb osob (Schengenský hraniční kodex) [1];

b) provádění jiných policejních a celních kontrol v dotyčném členském státě, jakož i za jejich koordinaci mezi určenými orgány.

2. Právo na přístup k údajům vloženým do SIS II a právo tyto údaje přímo vyhledávat mohou však při plnění svých úkolů stanovených vnitrostátními právními předpisy vykonávat i vnitrostátní justiční orgány, včetně těch, které odpovídají za zahájení trestního stíhání a za vyšetřování před podáním obžaloby, jakož i jejich koordinační orgány.

[1] Úř. věst. L 105, 13.4.2006, s. 1.

3. Orgány uvedené v tomto článku se zahrnou do seznamu uvedeného v čl. 46 odst. 8.

Článek 41

Přístup Europolu k údajům SIS II

1. Evropský policejní úřad (Europol) má v rámci svého mandátu právo na přístup k údajům vloženým do SIS II a právo tyto údaje přímo vyhledávat v souladu s články 26, 36 a 38.

2. Pokud vyhledávání provedené Europolem odhalí existenci záznamu v SIS II, Europol o tom informuje způsobem vymezeným Úmluvou o Europolu členský stát, který daný záznam pořídil.

3. Použití informací získaných vyhledáváním v SIS II podléhá souhlasu dotyčného členského státu. Pokud členský stát povolí použití takové informace, řídí se nakládání s ní Úmluvou o Europolu. Europol může takovou informaci sdělit třetím státům a třetím subjektům pouze se souhlasem dotyčného členského státu.

4. Europol může od dotyčného členského státu v souladu s ustanoveními Úmluvy o Europolu požadovat další informace.

5. Europol:

a) v souladu s ustanoveními článku 12 zaznamená každý vstup a vyhledávání, které provede;

b) aniž jsou dotčena ustanovení odstavců 3 a 4, nepropojí části SIS II s jakýmkoli počítačovým 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;

c) omezí přístup k údajům vloženým do SIS II na konkrétně oprávněné zaměstnance Europolu;

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

e) umožní Společnému kontrolnímu orgánu zřízenému podle článku 24 Úmluvy o Europolu, aby kontroloval činnost Europolu při výkonu jeho práva na přístup k údajům vloženým do SIS II a práva tyto údaje vyhledávat.

Článek 42

Přístup Eurojustu k údajům SIS II

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

2. Pokud vyhledávání provedené národním členem Eurojustu odhalí existenci záznamu v SIS II, informuje o tom členský stát, který daný záznam pořídil. Jakákoli informace získaná takovým vyhledáváním může být třetím státům a třetím subjektům sdělena pouze se souhlasem členského státu, který daný záznam pořídil.

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

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

5. Části SIS II se nepropojí s jakýmkoli počítačovým systémem pro sběr a zpracování údajů provozovaným Eurojustem nebo na jeho pracovištích, ani se do takového systému nepřenesou údaje v SIS II obsažené, k nimž mají vnitrostátní členové nebo jejich asistenti přístup, ani se žádné části SIS II nestáhnou.

6. Přístup k údajům vloženým do SIS II se omezuje na národní členy a jejich asistenty a nelze jej rozšířit na zaměstnance Eurojustu.

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

Článek 43

Rozsah přístupu

Uživatelé, včetně Europolu, národní členové Eurojustu a jejich asistenti mají přístup pouze k údajům, které jsou nezbytné k plnění jejich úkolů.

Článek 44

Doba uchovávání záznamů o osobách

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

2. Do tří let od vložení takového záznamu do SIS II přezkoumá členský stát, který záznam pořídil, nutnost jej zachovat. V případě záznamů o osobách podle článku 36 činí tato lhůta jeden rok.

3. Každý členský stát ve vhodných případech stanoví kratší doby pro přezkum v souladu se svými vnitrostátními právními předpisy.

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

5. Záznamy se automaticky vymazávají po uplynutí doby pro přezkum uvedené v odstavci 2 s výjimkou případu, kdy členský stát, který záznam pořídil, informoval CS-SIS o prodloužení záznamu podle odstavce 4. CS-SIS automaticky čtyři měsíce předem uvědomí členské státy o plánovaném výmazu údajů ze systému.

6. Členské státy vedou statistiku o počtu záznamů, u nichž byla doba uchovávání prodloužena v souladu s odstavcem 4.

Článek 45

Doba uchovávání záznamů o věcech

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

2. Záznamy o věcech vložené v souladu s článkem 36 se uchovávají nejvýše po dobu pěti let.

3. Záznamy o věcech vložené v souladu s článkem 38 se uchovávají nejvýše po dobu deseti let.

4. Doby uchovávání uvedené v odstavcích 2 a 3 se mohou prodloužit, pokud se to ukáže jako nezbytné pro účely, pro které byl záznam pořízen. V tomto případě se odstavce 2 a 3 použijí na toto delší uchovávání.

KAPITOLA XI

OBECNÁ PRAVIDLA PRO ZPRACOVÁNÍ ÚDAJŮ

Článek 46

Zpracování údajů v SIS II

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

2. Kopie údajů se mohou pořizovat pouze pro technické účely, pokud jsou potřebné k přímému vyhledávání orgány uvedenými v článku 40. Na tyto kopie se použijí ustanovení tohoto rozhodnutí. Záznamy pořízené jinými členskými státy nesmějí být kopírovány z jejich N.SIS II do jiných vnitrostátních souborů údajů.

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

Členské státy vedou aktualizovaný seznam těchto kopií, zpřístupní tento seznam vnitrostátním orgánům dozoru a zajistí, aby v souvislosti s těmito kopiemi byla uplatňována ustanovení tohoto rozhodnutí, zejména ustanovení uvedená v článku 10.

4. Přístup k údajům SIS II se povoluje pouze v mezích pravomoci vnitrostátního orgánu uvedeného v článku 40 a pouze osobám vybaveným náležitým oprávněním.

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

6. Údaje nesmějí být využívány k administrativním účelům.

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

8. Každý členský stát sdělí řídícímu orgánu seznam příslušných orgánů, které jsou podle tohoto rozhodnutí oprávněny přímo vyhledávat údaje uložené v SIS II, a jeho případné změny. V tomto seznamu je u každého orgánu uvedeno, v jakých údajích může vyhledávat a za jakými účely. Řídící orgán zajistí každoroční zveřejnění seznamu v *Úředním věstníku Evropské unie*.

9. Nestanoví-li právní předpisy Evropské unie zvláštní ustanovení, použijí se pro údaje vložené do N.SIS II právní předpisy každého členského státu.

Článek 47

Údaje a vnitrostátní soubory SIS II

1. Článkem 46 odst. 2 není dotčeno právo členského státu uchovávat ve svém vnitrostátním souboru údaje SIS II, ve spojitosti s nimiž bylo učiněno opatření na jeho území. Takové údaje se uchovávají ve vnitrostátních souborech nanejvýš po dobu tří let s výjimkou případů, kdy konkrétní ustanovení vnitrostátního práva upravují delší období uchovávání.

2. Článkem 46 odst. 2 není dotčeno právo členského státu uchovávat ve svých vnitrostátních souborech údaje obsažené v konkrétním záznamu, který vložil dotyčný členský stát do SIS II.

Článek 48

Informování v případě nepoužití záznamu

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

Článek 49

Kvalita údajů zpracovávaných v SIS II

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

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

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

4. Nemohou-li se členské státy dohodnout ve lhůtě dvou měsíců, předloží členský stát, který nepořídil záznam, věc evropskému inspektorovi ochrany údajů, který spolu s dotyčnými vnitrostátními orgány dozoru vystupuje jako prostředník.

5. Členské státy si vymění doplňující informace v případě, že si dotyčná osoba stěžuje, že není osobou, k níž se má záznam vztahovat. Prokáže-li kontrola, že se skutečně jedná o dvě odlišné osoby, bude osoba, která si stěžuje, informována o ustanoveních uvedených v článku 51.

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

Článek 50

Rozlišování osob s podobnými znaky

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

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

b) v případě, že kontrola prokáže, že osoba, jež je předmětem nového záznamu, a osoba, o níž již existuje záznam v SIS II, je ve skutečnosti jedna a ta samá, centrála SIRENE použije postup vkládání vícenásobných záznamů uvedený v čl. 49 odst. 6. Prokáže-li kontrola, že se ve skutečnosti jedná o dvě různé osoby, centrála SIRENE schválí požadavek na vložení dalšího záznamu a to tak, že doplní potřebné prvky, které zabrání jakýmkoli chybným určením totožnosti.

Článek 51

Další údaje pro účely řešení zneužití totožnosti

1. Může-li dojít k záměně mezi osobou, která má být ve skutečnosti předmětem záznamu, a osobou, jejíž totožnost byla zneužita, doplní členský stát, který záznam vložil, s výslovným souhlasem osoby, jejíž totožnost byla zneužita, záznam o údaje týkající se této osoby, aby se předešlo nežádoucím důsledkům chybného určení totožnosti.

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

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

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

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

a) příjmení a jméno/jména, rodné příjmení a dříve užívaná jména, případně alias, která mohou být vedena zvlášť;

b) veškeré zvláštní objektivní a tělesné nezměnitelné znaky;

c) místo a datum narození;

d) pohlaví;

e) fotografie;

f) otisky prstů;

g) státní příslušnost/příslušnosti;

h) číslo/čísla průkazu/průkazů totožnosti a datum vydání.

4. Technická pravidla potřebná pro vkládání, aktualizaci a vymazávání údajů uvedených v odstavci 3 se stanoví postupem podle článku 67, aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán.

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

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

Článek 52

Odkazy mezi záznamy

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

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

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

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

5. Členský stát může vytvořit odkazy v souladu se svými vnitrostátními právními předpisy, pokud jsou dodržovány zásady uvedené v tomto článku.

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

7. Technická pravidla pro odkazování mezi záznamy se přijmou postupem podle článku 67, aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán.

Článek 53

Účel a doba uchovávání doplňujících informací

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

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

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

Článek 54

Předávání osobních údajů třetím stranám

Údaje zpracovávané v SIS II za použití tohoto rozhodnutí se neposkytují ani nezpřístupňují žádné třetí zemi nebo mezinárodní organizaci.

Článek 55

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

1. Odchylně od článku 54 lze s členy Interpolu vyměňovat číslo cestovního pasu, země vystavení a druh dokumentu odcizených, neoprávněně užívaných, ztracených nebo neplatných cestovních pasů vložených do SIS II prostřednictvím propojení SIS II a databáze Interpolu o odcizených nebo pohřešovaných cestovních dokladech, s výhradou uzavření dohody mezi Interpolem a Evropskou unií. Dohodou se stanoví, že předávání údajů vložených členským státem podléhá souhlasu uvedeného členského státu.

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

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

KAPITOLA XII

OCHRANA ÚDAJŮ

Článek 56

Zpracování citlivých kategorií údajů

Zakazuje se zpracování kategorií údajů uvedených v první větě článku 6 Úmluvy Rady Evropy ze dne 28. ledna 1981 o ochraně osob s ohledem na automatizované zpracování osobních údajů.

Článek 57

Použití úmluvy Rady Evropy o ochraně údajů

Osobní údaje zpracovávané za použití tohoto rozhodnutí se chrání v souladu s Úmluvou Rady Evropy ze dne 28. ledna 1981 o ochraně osob s ohledem na automatizované zpracování osobních údajů a jejími následnými změnami.

Článek 58

Přístupové právo, oprava nepřesných údajů a výmaz protiprávně uchovávaných údajů

1. Právo osob na přístup k údajům vloženým o nich do SIS II v souladu s tímto rozhodnutím se vykonává v souladu s právními předpisy členského státu, u kterého toto právo uplatňují.

2. Pokud to stanoví vnitrostátní právní předpisy, rozhoduje o tom, zda a jakým způsobem se tyto informace poskytují, vnitrostátní orgán dozoru.

3. Členský stát, který záznam nepořídil, může poskytnout informace o těchto údajích pouze tehdy, pokud předem poskytl členskému státu, který záznam pořídil, příležitost zaujmout postoj. Toto se provádí prostřednictvím výměny doplňujících informací.

4. Informace nebude subjektu údajů sdělena, pokud je to nevyhnutelné pro výkon zákonného úkolu v souvislosti se záznamem nebo z důvodu ochrany práv a svobod třetích stran.

5. Každý má právo na opravu věcně nepřesných údajů nebo výmaz protiprávně uchovávaných údajů, které se jej týkají.

6. Dotyčná osoba je informována co nejdříve a v každém případě nejpozději do 60 dnů ode dne, kdy tato osoba požádala o přístup nebo dříve, stanoví-li tak vnitrostátní právní předpisy.

7. Tato osoba je o činnostech v návaznosti na výkon jejích práv na opravu a výmaz informována co nejdříve a v každém případě nejpozději do tří měsíců ode dne, kdy požádala o opravu nebo výmaz nebo dříve, stanoví-li tak vnitrostátní právní předpisy.

Článek 59

Opravné prostředky

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

2. Aniž jsou dotčena ustanovení článku 64, zavazují se členské státy navzájem vymáhat konečná rozhodnutí přijatá soudy nebo orgány uvedenými v odstavci 1.

3. Do 23. srpna 2009 Komise posoudí pravidla týkající se opravných prostředků uvedená v tomto článku.

Článek 60

Dohled nad N.SIS II

1. Každý členský stát zajistí, aby nezávislý orgán (dále jen „vnitrostátní orgán dozoru“) sledoval nezávisle zákonnost zpracování osobních údajů SIS II na svém území a jejich předávání mimo své území, včetně výměny a dalšího zpracování doplňujících informací.

2. Vnitrostátní orgány dozoru zajistí, aby alespoň každým čtvrtým rokem byl v souladu s mezinárodními auditorskými standardy proveden audit činností zpracování údajů v N.SIS II.

3. Členské státy zajistí, aby jejich vnitrostátní orgán dozoru měl dostatečné zdroje pro plnění úkolů, které mu byly tímto rozhodnutím svěřeny.

Článek 61

Dohled nad řídícím orgánem

1. Evropský inspektor ochrany údajů kontroluje, zda jsou činnosti řídícího orgánu související se zpracováváním osobních údajů prováděny v souladu s tímto rozhodnutím. Odpovídajícím způsobem se použijí povinnosti a pravomoci uvedené v článku 46 a 47 nařízení (ES) č. 45/2001.

2. Evropský inspektor ochrany údajů zajistí, aby alespoň každým čtvrtým rokem byl v souladu s mezinárodními auditorskými standardy proveden audit činností řídícího orgánu souvisejících se zpracováváním osobních údajů. Zpráva vzešlá z auditu se zašle Evropskému parlamentu, Radě, řídícímu orgánu, Komisi a vnitrostátním orgánům dozoru. Řídícímu orgánu se poskytne příležitost zprávu připomínkovat před jejím přijetím.

Článek 62

Spolupráce mezi vnitrostátními orgány dozoru a evropským inspektorem ochrany údajů

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

2. Vyměňují si příslušné informace, každý z nich jednaje v rámci svých příslušných pravomocí, pomáhají si navzájem při provádění auditů a kontrol, přezkoumávají obtíže týkající se výkladu nebo použití tohoto rozhodnutí, zabývají se problémy při výkonu nezávislého dohledu nebo při výkonu práv subjektu údajů, vypracovávají harmonizované návrhy společných řešení případných problémů a podle potřeby zvyšují povědomí o právech na ochranu údajů.

3. Vnitrostátní orgány dozoru a evropský inspektor ochrany údajů se za tímto účelem setkají alespoň dvakrát do roka. Náklady na tato setkání a jejich obsluhu ponese evropský inspektor ochrany údajů. Na prvním setkání se přijme jednací řád. Další pracovní metody se vypracují společně podle potřeby. Společná zpráva o činnostech se zasílá Evropskému parlamentu, Radě, Komisi a řídícímu orgánu každé dva roky.

Článek 63

Ochrana údajů během přechodného období

V případě, že Komise podle čl. 15 odst. 4 pověří jiný orgán nebo orgány plněním svých povinností během přechodného období, zajistí, aby měl evropský inspektor ochrany údajů právo a možnost plně vykonávat své úkoly, včetně možnosti provádět kontroly na místě nebo vykonávat jiné pravomoci, které na něj byly přeneseny podle článku 47 nařízení (ES) č. 45/2001.

KAPITOLA XIII

ODPOVĚDNOST A SANKCE

Článek 64

Odpovědnost

1. Každý členský stát odpovídá v souladu se svými vnitrostátními právními předpisy za škodu způsobenou kterékoli osobě při využívání N.SIS II. To platí i v případě škody způsobené členským státem, který záznam pořídil, tím, že tento členský stát vložil věcně nepřesné údaje nebo údaje protiprávně uchovával.

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

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

Článek 65

Sankce

Členské státy zajistí, aby jakékoli zneužití údajů vložených do SIS II nebo jakákoliv výměna doplňujících informací, která je v rozporu s tímto rozhodnutím, podléhaly účinným, přiměřeným a odrazujícím sankcím v souladu s vnitrostátními právními předpisy.

KAPITOLA XIV

ZÁVĚREČNÁ USTANOVENÍ

Článek 66

Sledování a statistika

1. Řídící orgán zajistí zavedení postupů pro sledování fungování SIS II z hlediska výstupů, účinnosti vynaložených prostředků, zabezpečení a kvality služeb.

2. Pro účely technické údržby, vypracovávání zpráv a statistik má řídící orgán přístup k nezbytným informacím souvisejícím s operacemi zpracování prováděnými v centrálním SIS II.

3. Každým rokem zveřejní řídící orgán statistické údaje, z kterých vyplývá počet evidovaných vstupů připadajících na jednu kategorii záznamů, počet pozitivních nálezů připadajících na jednu kategorii záznamů a počet přístupů do SIS II, a to pro každý tento počet celkem a pro každý členský stát jednotlivě.

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

5. Tři roky po spuštění provozu SIS II a poté vždy po čtyřech letech vypracuje Komise celkové vyhodnocení centrálního SIS II a dvoustranné i mnohostranné výměny doplňujících informací mezi členskými státy. Toto celkové vyhodnocení musí zahrnovat přezkoumání dosažených výsledků v porovnání s vytyčenými cíli, posouzení trvající platnosti důvodu pro vznik systému, uplatňování tohoto rozhodnutí v souvislosti s centrálním SIS II, zabezpečení centrálního SIS II i všech dopadů jeho budoucího provozování. Komise předá hodnotící zprávy Evropskému parlamentu a Radě.

6. Členské státy poskytnou řídícímu orgánu a Komisi informace nezbytné pro vypracování zpráv uvedených v odstavcích 3, 4 a 5.

7. Řídící orgán poskytne Komisi informace nezbytné pro vypracování celkových vyhodnocení uvedených v odstavci 5.

Článek 67

Regulativní výbor

1. Odkazuje-li se na tento článek, je Komisi nápomocen regulativní výbor, jehož členy jsou zástupci členských států a jehož předsedou je zástupce Komise. Zástupce Komise předloží výboru návrh opatření, která mají být přijata. Podle naléhavosti dotčené záležitosti sdělí výbor své stanovisko k předloženému návrhu do termínu stanoveného předsedou. V případě rozhodnutí, která má Rada přijmout na návrh Komise, musí být stanovisko přijato většinou stanovenou v čl. 205 odst. 2 Smlouvy o ES. Hlasy zástupců členských států zasedajících ve výboru budou váženy způsobem uvedeným v daném článku. Předseda nehlasuje.

2. Výbor přijme na návrh předsedy svůj jednací řád podle standardních jednacích řádů zveřejněných v Úředním věstníku Evropské unie.

3. Komise zamýšlená opatření přijme, pokud jsou v souladu se stanoviskem výboru. Pokud zamýšlená opatření nejsou v souladu se stanoviskem výboru nebo pokud výbor žádné stanovisko nevydá, Komise předloží Radě bezodkladně návrh týkající se opatření, která mají být přijata.

4. Rada je oprávněna o tomto návrhu rozhodnout kvalifikovanou většinou do dvou měsíců ode dne, kdy jí byl předložen. Pokud Rada v této lhůtě kvalifikovanou většinou sdělí, že s návrhem nesouhlasí, Komise daný návrh znovu přezkoumá. Je pak oprávněna předložit Radě upravený návrh, původní návrh nebo legislativní návrh. Pokud po uplynutí uvedené lhůty Rada návrh prováděcího právního aktu ani nepřijme, ani neuvede, že s tímto návrhem prováděcích opatření nesouhlasí, Komise tento návrh prováděcího právního aktu přijme.

5. Výbor uvedený v odstavci 1 vykonává svou funkci ode dne 23. srpna 2007.

Článek 68

Změna ustanovení schengenského *acquis*

1. Pro účely záležitostí spadajících do oblasti působnosti Smlouvy o EU nahrazuje toto rozhodnutí ode dne uvedeného v čl. 71 odst. 2 ustanovení článků 64 a 92 až 119 Schengenské úmluvy s výjimkou jejího článku 102a.

2. Pro účely záležitostí spadajících do oblasti působnosti Smlouvy o EU toto rozhodnutí rovněž zrušuje ode dne uvedeného v čl. 71 odst. 2 níže uvedená ustanovení schengenského *acquis* provádějící uvedené články [1]:

a) rozhodnutí výkonného výboru ze dne 14. prosince 1993 o finančním nařízení o nákladech na zřízení a provoz Schengenského informačního systému (C.SIS) (SCH/Com-ex (93) 16);

b) rozhodnutí výkonného výboru ze dne 7. října 1997 o vývoji SIS (SCH/Com-ex (97) 24);

c) rozhodnutí výkonného výboru ze dne 15. prosince 1997, kterým se mění finanční nařízení o C.SIS (SCH/Com-ex (97) 35);

d) rozhodnutí výkonného výboru ze dne 21. dubna 1998 o C.SIS s 15/18 přípojkami (SCH/Com-ex (98) 11);

e) rozhodnutí výkonného výboru ze dne 25. dubna 1997 o udělení zakázky na předběžnou studii SIS II (SCH/Com-ex (97) 2 rev. 2);

f) rozhodnutí výkonného výboru ze dne 28. dubna 1999 o výdajích na zřízení C.SIS (SCH/Com-ex (99) 4);

g) rozhodnutí výkonného výboru ze dne 28. dubna 1999 o aktualizaci příručky SIRENE (SCH/Com-ex (99) 5);

h) prohlášení výkonného výboru ze dne 18. dubna 1996, kterým se vymezuje pojem cizí státní příslušník (SCH/Com-ex (96) decl. 5);

i) prohlášení výkonného výboru ze dne 28. dubna 1999 o struktuře SIS (SCH/Com-ex (99) decl. 2 rev.);

j) rozhodnutí výkonného výboru ze dne 7. října 1997 o příspěvcích Norska a Islandu na náklady na zřízení a provoz C.SIS (SCH/Com-ex (97) 18).

3. Pro účely záležitostí spadajících do oblasti působnosti Smlouvy o EU se odkazy na nahrazené články Schengenské úmluvy a na příslušná ustanovení schengenského *acquis*, kterými se uvedené články provádějí, považují za odkazy na toto rozhodnutí.

Článek 69

Ustanovení o zrušení

Ke dni uvedenému v čl. 71 odst. 2 se zrušují rozhodnutí 2004/201/SVV, rozhodnutí 2005/211/SVV, rozhodnutí 2005/719/SVV, rozhodnutí 2005/727/SVV, rozhodnutí 2006/228/SVV, rozhodnutí 2006/229/SVV, a rozhodnutí 2006/631/SVV.

[1] Úř. věst. L 239, 22.9.2000, s. 439.

Článek 70

Přechodné období a rozpočet

1. Záznamy ze SIS 1+ je možné přenášet do SIS II. Členské státy zajistí, aby byl obsah záznamů, které jsou přeneseny ze SIS 1+ do SIS II, co nejdříve a nejpozději do tří let ode dne uvedeného v čl. 71 odst. 2 uveden v soulad s ustanoveními tohoto rozhodnutí, přičemž přednost mají záznamy o osobách. Členské státy mohou během tohoto přechodného období i nadále používat pro obsah záznamů, které jsou přeneseny ze SIS 1+ do SIS II, ustanovení článků 94, 95 a 97 až 100 Schengenské úmluvy, a to s výhradou těchto zásad:

a) v případě změny, doplnění nebo opravy nebo aktualizace obsahu záznamu přeneseného z SIS 1+ do SIS II členské státy zajistí, aby záznam ode dne této změny, doplnění, opravy nebo aktualizace vyhovoval ustanovením tohoto rozhodnutí;

b) v případě pozitivního nálezu záznamu přeneseného z SIS 1+ do SIS II členské státy posoudí soulad uvedeného záznamu s ustanoveními tohoto rozhodnutí bezodkladně, ale bez zpoždění opatření, která mají být přijata na základě uvedeného záznamu.

2. K datu stanovenému v souladu s čl. 71 odst. 2 se zbývající část rozpočtu schváleného v souladu s článkem 119 Schengenské úmluvy členským státům vrátí. Částky, které mají být vráceny, se vypočítají na základě příspěvků členských států, jak jsou stanoveny rozhodnutím výkonného výboru ze dne 14. prosince 1993 o finančním nařízení o nákladech na zřízení a provoz Schengenského informačního systému.

3. Po dobu přechodného období podle čl. 15 odst. 4 se odkazy na řídící orgán v tomto rozhodnutí považují za odkazy na Komisi.

Článek 71

Vstup v platnost, použitelnost a migrace

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

2. Vztahuje se na členské státy, které se účastní SIS 1+ ode dne, který stanoví Rada jednomyslným usnesením svých členů zastupujících vlády členských států, které se účastní SIS 1+.

3. Datum uvedené v odstavci 2 se určí:

a) po přijetí nezbytných prováděcích opatření;

b) po tom, co všechny členské státy, které se plně účastní SIS 1+ Komisi oznámí, že přijaly nezbytná technická a právní opatření pro zpracovávání údajů SIS II a výměnu dodatečných informací;

c) po tom, co Komise oznámí úspěšné dokončení souhrnného testu SIS II, který provede Komise společně s členskými státy a po tom, co přípravné orgány Rady ověří navrhovaný výsledek testu. Toto ověření potvrdí, že úroveň funkční způsobilosti SIS II je přinejmenším rovnocenná úrovni funkční způsobilosti, které bylo dosaženo u SIS 1+;

d) po tom, co Komise provede veškerá nezbytná technická opatření umožňující připojení centrálního SIS II k N.SIS II dotyčných členských států.

4. Komise sdělí Evropskému parlamentu výsledky testů provedených podle odst. 3 písm. c).

5. Každé rozhodnutí Rady přijaté v souladu s odstavcem 2 se zveřejní v *Úředním věstníku Evropské unie*.

V Lucemburku dne 12. června 2007.

Za Radu
předseda
W. SCHÄUBLE

Věstník Úřadu pro ochranu osobních údajů

Vydavatel: Úřad pro ochranu osobních údajů
Adresa redakce: Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7
Redakce: Miluše Nejedlá, tel.: 234 665 232, fax: 234 665 505
e-mail: posta@uoou.cz
internetová adresa: www.uoou.cz

Administrace: Písemné objednávky předplatného, změny adres a počtu odebíraných výtisků – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422, www.sevt.cz, e-mail: sevt@sevt.cz. – **Předpokládané roční předplatné** se stanovuje za dodávku kompletního ročníku a je od předplatitelů vybíráno formou záloh ve výši oznámené ve Věstníku a pro tento rok činí 450 Kč – Vychází podle potřeby – **Tiskne**: sprint servis, Lovosická 31, Praha 9.

Distribuce: Předplatné, jednotlivé částky na objednávku i za hotové – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422; drobný prodej v prodejnách SEVT, a. s. – Praha 5, Elišky Peškové 14, tel./fax: 257 320 049, – Praha 4, Jihlavská 405, tel.: 261 260 414 – Brno, Česká 14, tel.: 542 213 962 – Ostrava, roh ul. Nádražní a Denisovy, tel.: 596 120 690 – České Budějovice, Česká 3, tel.: 387 319 045 a ve vybraných knihkupectvích. Distribuční podmínky předplatného: Jednotlivé částky jsou expedovány předplatitelům neprodleně po dodání z tiskárny. Objednávky nového předplatného jsou vyřizovány do 15 dnů a pravidelné dodávky jsou zahajovány od nejbližší částky po ověření úhrady předplatného, nebo jeho zálohy. Částky vyšlé v době od zaevidování předplatného do jeho úhrady jsou doposílány jednorázově. Změny adres a počtu odebíraných výtisků jsou prováděny do 15 dnů. Lhůta pro uplatnění reklamací je stanovena na 15 dnů od data rozeslání, po této lhůtě jsou reklamace vyřizovány jako běžné objednávky za úhradu. V písemném styku vždy uvádějte IČ (právnická osoba) a kmenové číslo předplatitele. Podávání novinových zásilek povoleno ŘPP Praha.

ISSN 1213-3442