VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2014

Částka 67 **25. srpna 2014**

OBSAH

ÚVOD

Vážení čtenáři,

v souvislosti se změnou způsobu publikace Věstníku Úřadu pro ochranu osobních údajů Vám sdělujeme, že Věstník je od částky 67 publikován pouze v elektronické podobě. Navazuje na předcházející částky a je zdarma přístupný na internetové adrese Úřadu www.uoou.cz v rubrice Publikace. Věstník byl od 12. 4. 2000 do 31. 1. 2013 (částky 1 – 66) publikován v tištěné podobě a text byl umísťován do odpovídajících rubrik na webových stránkách Úřadu. Částky 1 – 66 jsou k dispozici na webových stránkách v rubrice Archiv Věstníků Úřadu pro ochranu osobních údajů.

Šedesátá sedmá částka Věstníku Úřadu pro ochranu osobních údajů obsahuje přehled zrušených registrací za období od 21. 10. 2013 do 15. 8. 2014.

Rubrika Stanoviska Úřadu přináší dvě stanovisko Úřadu. Prvním dokumentem je stanovisko č. 1/2014 „Chytré měření a ochrana osobních údajů“, které se zabývá otázkou zavádění inteligentních sítí a chytrého měření především do domácností. Mezi informacemi získanými inteligentním měřením spotřeby energie domácností bude velká množina těch, na které je nutno pohlížet jako na osobní údaje. Vzhledem k tomu, že tyto informace budou jako celek za určitým účelem shromažďovány, předávány, využívány a dále zpracovávány, je podle názoru Úřadu nezbytné na provozování inteligentních sítí obsahujících inteligentní měření spotřeby s přihlédnutím k dalším technickým parametrům a nastavení těchto systémů obvykle pohlížet jako na zpracování osobních údajů a přizpůsobit je zákonným požadavkům vyjádřeným především v zákoně o ochraně osobních údajů.

Druhým dokumentem této rubriky je stanovisko č. 2/2014 „Dynamický biometrický podpis“. Podpis v jakékoliv podobě je osobním údajem a ve smluvních vztazích dochází k jeho zpracování. Ve stanovisku je definováno, že jediným právním titulem, na základě kterého je takové zpracování obecně realizovatelné, je výslovný a informovaných souhlas každého subjektu údajů podle § 9 písm. a) zákona č. 101/2000 Sb., který musí být správce schopen prokázat po celou dobu zpracování. Zvýšenou pozornost je nutné věnovat zejména plnění informační a oznamovací povinnosti a zabezpečení biometrických údajů.

V rubrice Sdělení Úřadu je publikován dokument Pracovní skupiny pro ochranu dat podle článku 29 směrnice 95/46/ES (WP29), kterým je Stanovisko č. 6/2013 k veřejně přístupným údajům a opakovanému použití informací veřejného sektoru. Cílem tohoto stanoviska je pomoci zajistit jednotné chápaní platného právního rámce a poskytnout jednotné pokyny a příklady osvědčených postupů, pokud jde o způsob provedení (pozměněné) směrnice o informacích veřejného sektoru s ohledem na zpracovávání osobních údajů. Pracovní skupina podle článku 29 konstatuje, že opakované použití informací veřejného sektoru může zajistit přínosy vedoucí k větší transparentnosti a inovativnímu opakovanému použití informací veřejného sektoru. Výsledná větší dostupnost informací však není bez rizika. V zájmu zajištění ochrany soukromí a osobních údajů jednotlivců je třeba uplatňovat vyvážený přístup. Právní předpisy o ochraně údajů musejí pomoci řídit proces výběru osobních údajů, které lze, či nelze zpřístupnit pro opakované použití, a formulovat opatření, která je nutno přijmout na ochranu osobních údajů. Jedná se o překlad pořízený Evropskou komisí.

I. REGISTRACE

Přehled zrušených registrací od 21. 10. 2013 do 15. 8. 2014

Číslo registrace	Subjekt	Datum zrušení
00000022/002	AERO Vodochody a.s.	3.4.2014
00000022/001	AERO Vodochody a.s.	3.4.2014
00000882/001	BOŽENA SEDLÁKOVÁ - BOSPOR	19.11.2013
00000882/002	BOŽENA SEDLÁKOVÁ - BOSPOR	19.11.2013
00001471/027	Městská část Praha 12	9.4.2014
00001471/020	Městská část Praha 12	16.4.2014
00001471/018	Městská část Praha 12	16.4.2014
00006435/003	Město Tábor	6.6.2014
00006647/001	Univerzita Pardubice	16.4.2014
00006647/006	Univerzita Pardubice	16.4.2014
00007356/001	MĚSTSKÉ KULTURNÍ STŘEDISKO	28.2.2014
00007592/002	KVADOS Mobile Solutions s.r.o.	30.4.2014
00007592/001	KVADOS Mobile Solutions s.r.o.	30.4.2014
00011375/002	Nokia Czech Republic, s.r.o.	16.4.2014
00011375/001	Nokia Czech Republic, s.r.o.	16.4.2014
00011375/004	Nokia Czech Republic, s.r.o.	16.4.2014
00011375/003	Nokia Czech Republic, s.r.o.	16.4.2014
00011799/021	PPD Czech Republic, s.r.o.	15.7.2014
00017511/001	LESÁK LUBOŠ	5.11.2013
00019068/002	Město Veselí nad Moravou	3.12.2013
00019116/018	Správa železniční dopravní cesty, státní organizace	17.4.2014
00019116/059	Správa železniční dopravní cesty, státní organizace	3.6.2014
00024301/003	OREA HOTELS s.r.o.	3.12.2013
00025055/001	Liberecká IS, a.s.	8.11.2013
00026451/014	SCHENKER spol.s r.o.	5.6.2014
00026451/003	SCHENKER spol.s r.o.	2.11.2013
00026451/009	SCHENKER spol.s r.o.	29.5.2014
00027279/005	Severočeské doly a.s.	12.7.2014
00029538/001	ZFP akademie, a.s.	21.12.2013
00032175/001	BKS Capital Partners a.s.	26.7.2014
00033126/002	SD - KOMES, a.s.	1.2.2014
00033126/001	SD - KOMES, a.s.	1.2.2014
00033403/001	Biogen Idec (Czech Republic) s.r.o.	19.7.2014
00033481/032	Family drogerie s.r.o.	23.11.2013
00033481/001	Family drogerie s.r.o.	25.1.2014
00033908/006	AGROPODNIK DOMAŽLICE a. s.	9.4.2014
00034384/002	Ivo Pačinek	13.6.2014
00034564/004	TOP TANK s.r.o.	12.6.2014
00035169/002	AXA Bank Europe, organizační složka	22.12.2013

00037047/002	KERAMOST, akciová společnost	8.11.2013
00037234/002	GYMNÁZIUM, STŘEDNÍ ODBORNÁ ŠKOLA A VYŠŠÍ ODBORNÁ ŠKOLA LEDEČ NAD SÁZAVOU	15.3.2014
00037268/001	Bacardi - Martini Czech s.r.o., v likvidaci	31.10.2013
00038384/001	ZUZANA PETROVIČOVÁ	22.4.2014
00039146/001	LENKA KAISEROVÁ	7.1.2014
00039296/002	DAPI, s.r.o.	30.4.2014
00039693/001	Společenství vlastníků bl. 506 č.p. 1306, 1307, 1308, 1309 ulice Jana Kubelíka	6.3.2014
00039705/002	W.H.R. Petrol s.r.o.	11.7.2014
00039705/003	W.H.R. Petrol s.r.o.	11.7.2014
00039705/005	W.H.R. Petrol s.r.o.	11.7.2014
00039705/004	W.H.R. Petrol s.r.o.	11.7.2014
00039705/007	W.H.R. Petrol s.r.o.	11.7.2014
00039705/001	W.H.R. Petrol s.r.o.	11.7.2014
00040671/001	Docter Optics s.r.o.	7.6.2014
00041627/001	NEOPALLADIUM, s.r.o.	15.7.2014
00041710/001	FILIP ŠLEGER	24.5.2014
00042179/001	Ústav fotoniky a elektroniky AV ČR, v. v. i.	14.3.2014
00043507/001	JP INFOSALES, s.r.o., v likvidaci	5.4.2014
00044755/001	MARTINA HRŮZOVÁ	25.4.2014
00044976/001	RENÁTA ŠNAJBERKOVÁ	2.11.2013
00045043/001	ATREA s.r.o.	13.5.2014
00045654/002	Air Telecom a.s.	23.11.2013
00045858/001	Marek Remecký	7.1.2014
00046001/006	ALL IN AGENCY, spol. s r.o.	27.3.2014
00046001/005	ALL IN AGENCY, spol. s r.o.	27.3.2014
00046001/004	ALL IN AGENCY, spol. s r.o.	27.3.2014
00046001/003	ALL IN AGENCY, spol. s r.o.	27.3.2014
00046001/002	ALL IN AGENCY, spol. s r.o.	27.3.2014
00046001/001	ALL IN AGENCY, spol. s r.o.	27.3.2014
00046046/001	Jiří Straka	21.2.2014
00046414/001	JP RESTAURANT s.r.o.	15.11.2013
00046853/003	Monika Šafárová	13.7.2014
00047767/001	Jiří Aujezdský, DiS.	24.12.2013
00049098/001	SEKYRKA ANTONÍN	16.4.2014
00049105/001	Alice Kattirsová	4.4.2014
00049522/022	ČESKÁ LÉKÁRNA HOLDING, a.s.	20.5.2014
00049522/041	ČESKÁ LÉKÁRNA HOLDING, a.s.	3.5.2014
00050631/001	Mgr. Lucia Brinzanik	16.7.2014
00051435/001	Tomáš Junek	26.4.2014

II. STANOVISKA ÚŘADU

Stanovisko č. 1/2014

leden 2014[1]

Chytré měření a ochrana osobních údajů

Směrnice Evropského parlamentu a Rady 2009/72/ES ze dne 13. července 2009 o společných pravidlech pro vnitřní trh s elektřinou a o zrušení směrnice 2003/54/ES se mimo jiné zabývá i zaváděním inteligentních sítí a inteligentních měřicích systémů na trhu s elektrickou energií, tzv. princip smart metering. Tento technologický trend umožňuje interaktivní dvoustrannou komunikaci mezi dodavatelem energie a jejím odběratelem, která obsahuje i informace o spotřebitelském chování, jež mohou mít dopad na soukromí spotřebitele, odběratele energií, a dalších členů jeho domácnosti. Uvedená směrnice členským státům rovněž uložila, aby zpracovaly vyhodnocení ekonomických dopadů zavádění inteligentních sítí. Ač studie vypracovaná Ministerstvem průmyslu a obchodu[2] v prostředí České republiky neshledává zavádění těchto systémů jako ekonomicky výhodné, trend v nasazování inteligentních měřicích systémů je zjevný, což dokazují i související žádosti o konzultace Úřadu pro ochranu osobních údajů (dále jen „Úřad“) od společností, které se jimi zabývají nebo hodlají zabývat.

Příslušné evropské předpisy ani další evropské[3] či vnitrostátní dokumenty se otázkou ochrany soukromí, která se zaváděním inteligentních sítí a chytrého měření především pro domácnosti bezprostředně souvisí, příliš nezabývají. Z tohoto důvodu považuje Úřad za vhodné se k inteligentním měřicím systémům vyjádřit i z pohledu své kompetence, ochrany osobních údajů zúčastněných fyzických osob.[4]

Inteligentní sítě a chytré měření

Inteligentní sítě jsou klasické energetické sítě doplněné o další prvky, především interaktivní obousměrnou komunikací mezi dodavatelem a spotřebitelem, inteligentní měření spotřeby a případně dalšími monitorovacími či komunikačními systémy, které dodavatelům umožňují efektivnější distribuci energie a uživatelům její efektivnější spotřebu. Základní rozdíl oproti běžným sítím spočívá v tom, že inteligentní sítě pomocí prvků inteligentního měření umožňují či směřují k prakticky nepřetržitému a v čase průběžnému sledování odběru energií konkrétním spotřebitelem, respektive jeho domácností. Právě zkrácení frekvence odečtu odebrané energie konkrétních uživatelů z měření prováděného jednou za několik měsíců, jak tomu obvykle probíhá u klasických sítí, až prakticky k on-line sledování, představuje největší riziko pro soukromí spotřebitelů. Prostřednictvím systémů inteligentního měření totiž lze poměrně přesně sledovat chování konkrétních osob a vytvářet jejich spotřebitelský profil, například pomocí informací o tom, jaký spotřebič a v jaký čas daný uživatel zapnul a kdy jej vypnul, sledovat jeho další životní zvyklosti atd.

Jedná se o zpracování osobních údajů

Osobní údaj je definován v § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, jako jakákoliv informace týkající se

[1] Podle stavu právních předpisů k 15. lednu 2014.
[2] Dostupná na http://www.mpo.cz/dokument106754.html.
[3] K problematice se vyjadřuje také stanovisko pracovní skupiny WP29 č. 12/2011 k inteligentnímu měření.
[4] O možném zavedení inteligentních měřících systémů či inteligentních sítích se uvažuje i v jiných oblastech, srov. především směrnici Evropského parlamentu a Rady 2009/73/ES ze dne 13. července 2009 o společných pravidlech pro vnitřní trh se zemním plynem a o zrušení směrnice 2003/55/ES. Dále uvedené principy ochrany dat je nutno uplatňovat ve všech oblastech dodávek energií, kde bude chytré měření nasazeno.

určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo, či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

Lze namítnout, že inteligentní měřicí systémy neshromažďují informace o konkrétním spotřebiteli, ale o domácnosti a celkové spotřebě všech jejích členů, a proto se o osobní údaje ve smyslu uvedené definice nejedná. S tímto názorem však Úřad nesouhlasí především z následujících důvodů:

Informace o spotřebě v rámci jedné domácnosti budou alespoň pro některé příjemce údajů vždy spjaty s konkrétními osobami, které v dané domácnosti žijí. Bude se jednat především o osobu odběratele, jímž je obvykle jeden z členů domácnosti, který k informaci o aktuální spotřebě v daném dni může přiřadit informace týkající se ostatních členů domácnosti. Jinak řečeno je nebo může mu být známo, kdo byl v daný okamžik v domácnosti přítomen, kdo v čase, kdy se prudce zvýšila spotřeba energie, přišel či měl přijít domů, či naopak, že domácnost měla být dle tvrzení jejích ostatních členů prázdná, ačkoliv informace o spotřebě vypovídají o opaku. Další informace k osobám žijících v konkrétní domácnosti však mohou mít i další osoby, např. majitel bytového domu či obdobný subjekt (společenství vlastníků jednotek), dodavatel energie či společnost podílející se na měření spotřeby a jejím vyúčtovávání.

Nelze opominout ani fenomén nárůstu počtu tzv. jednočlenných domácností, kterých je v České republice dle informací Českého statistického úřadu k roku 2010 již více než jeden milion.[5] V případě informací o spotřebě odběratelů žijících právě v jednočlenných domácnostech se bude o osobní údaje jednat v zásadě vždy.

Výše uvedené lze shrnout tak, že mezi informacemi získanými inteligentním měřením spotřeby domácností bude velká množina těch, na které je nutno pohlížet jako na osobní údaje. Vzhledem k tomu, že tyto informace jako celek budou zpracovávány ve smyslu § 4 písm. e) zákona č. 101/2000 Sb., tedy cíleně a za určitým účelem shromažďovány, předávány, využívány atd., je podle názoru Úřadu nezbytné na provozování inteligentních sítí obsahujících inteligentní měření spotřeby s přihlédnutím k dalším technickým parametrům a nastavení těchto systémů obvykle pohlížet jako na zpracování osobních údajů a přizpůsobit jej zákonným požadavkům vyjádřeným především v zákoně č. 101/2000 Sb.

Role dotčených subjektů

Zákon č. 101/2000 Sb. rozlišuje odpovědné osoby podílející se na zpracování osobních údajů na správce a zpracovatele. Správcem údajů je ta osoba, která především určuje účel a prostředky zpracování osobních údajů, zpracování provádí a odpovídá za něj. Správce může část samotného zpracování či realizaci zpracování jako celku přenést na další subjekt, zpracovatele, který provádí zpracování za správce s vlastní odpovědností. V takovém případě, pokud zmocnění pro zpracovatele nevyplývá ze zvláštního zákona, musí správce se zpracovatelem uzavřít smlouvu, jejíž nezbytné náležitosti upravuje § 6 zákona č. 101/2000 Sb.

Vzhledem k počtu a odlišnému postavení subjektů, které se na realizaci obchodních vztahů na trhu s energiemi podílejí, zejména jde o výrobce a distributory energií, společnosti zabývající se účtováním spotřeby, majitele bytových domů či jednotlivých bytů atd., nelze obecně určit, kdo z nich bude v každém jednotlivém obchodním modelu v postavení správce a zpracovatele osobních údajů. Pro určení správce, hlavní odpovědné osoby, bude klíčové především kritérium prvotního rozhodnutí o zahájení zpracování údajů a stanovení jeho účelu, kdy správcem bude právě ta osoba, která o zpracování osobních údajů prostřednictvím inteligentních sítí za určitým účelem rozhodne. V pozici zpracovatele mohou vystupovat další subjekty, které budou mít na základě pověření od správce k předávaným informacím přístup a budou se na jejich zpracování, byť i v minimální míře, podílet. Pokud však některý z dalších zúčastněných subjektů bude chtít zpracovávat předmětné údaje i za dalším odlišným účelem, bude již v procesu zpracování samostatným správcem.

[5] Blíže viz zpráva Českého statistického úřadu dostupná na adrese http://www.czso.cz/csu/csu.nsf/ainformace/78E200316A95.

Účel zpracování osobních údajů

Jednou z klíčových povinností při zpracování osobních údajů je stanovit jeho účel, který musí být legitimní a legální. Z účelu zpracování je pak pro správce a zpracovatele odvozena řada dalších povinností.

Energetický trh je v České republice plně liberalizován, pohybujeme se proto v soukromoprávní oblasti. Ústavní maxima zní, že soukromé subjekty mohou dělat to, co jim zákon nezakazuje. Jako legální proto lze označit každý účel zpracování osobních údajů, který není zákonem výslovně zakázán a ani nesměřuje k porušení zákona, například k diskriminaci některých skupin spotřebitelů.

Legitimitu úmyslu zpracovávat osobní údaje, tedy zasahovat do soukromí fyzických osob, je vždy nutno hodnotit individuálně, podle deklarovaného účelu a dalších souvisejících okolností, a to i s přihlédnutím k otázce nezbytnosti a přiměřenosti zamýšleného zásahu do soukromí. Toto pravidlo je v zákoně č. 101/2000 Sb. vyjádřeno především v § 10, podle kterého jsou odpovědné subjekty při každém zpracování osobních údajů povinny dbát na to, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.[6]

Při nasazení systému inteligentního měření spotřeby je tak vždy nezbytné jasně deklarovat nejen sám účel tohoto systému jako celku, ale v návaznosti na tento krok je třeba posoudit, zda je pro dosažení očekávaného účelu nezbytné zpracovávat osobní údaje, případně v jakém rozsahu. Pokud pro realizaci deklarovaného cíle nebude objektivně nezbytné zpracovávat osobní údaje, bude jej možno dosáhnout i bez nich, například zpracováním anonymizovaných údajů, pak se zpracování osobních údajů prováděné za tímto účelem jeví jako nelegitimní. Takové zpracování není nezbytné a navíc deklarovaný účel může zakrývat účel jiný, ke kterému mají být údaje spotřebitelů bez jejich vědomí získávány, přičemž tento postup je nutno označit nejen za nelegitimní, ale přímo za nelegální, neboť by byl v rozporu s povinností shromažďovat osobní údaje pouze otevřeně a nikoliv pod záminkou jiného účelu nebo činnosti.[7]

Právní titul pro zpracování osobních údajů

Výčet právních titulů právem předvídaných situací, kdy lze osobní údaje zpracovávat, je uveden v § 5 odst. 2 zákona č. 101/2000 Sb. Pro zpracování osobních údajů prostřednictvím inteligentních sítí se podle názoru Úřadu nabízejí dva možné právní tituly: souhlas subjektu údajů a zpracování nezbytné k plnění smlouvy, jejíž je subjekt údajů smluvní stranou.

Souhlas se zpracováním osobních údajů je jednostranným právním úkonem, dikcí nového občanského zákoníku právním jednáním. Proto, aby byl platný, musí splňovat veškeré náležitosti podle předpisů občanského práva a podle požadavků zákona č. 101/2000 Sb. Musí být svobodný, vážný, srozumitelný, určitý a informovaný. Pokud by poskytnutý souhlas nenaplňoval byť jednu z těchto náležitostí, nebyl by například svobodný, pokud by spotřebitel zpracování osobních údajů prostředky inteligentního měření spotřeby nemohl bez dalších negativních následků odmítnout, potom by byl souhlas neplatný a celé zpracování osobních údajů by bylo od počátku nelegální.[8]

Druhý z uvedených právních titulů, tedy zpracování nezbytné pro realizaci nebo uzavření smlouvy se subjektem údajů, bude připadat v úvahu především tehdy, pokud subjekt údajů projeví zájem o nabízený produkt, jehož nezbytnou součástí bude právě zpracování jeho osobních údajů v rámci inteligentní sítě. Typicky se může jednat o situaci, kdy výrobce nebo dodavatel energie spotřebitelům nabídne smlouvu na dodávku energie obsahující i zpracování a předávání informací o průběžné spotřebě domácnosti odběratele a dalších souvisejících dat. Pokud odběratel projeví o tento produkt zájem a smlouvu uzavře, druhá smluvní strana je pro naplnění svého závazku na základě tohoto právního titulu oprávněna osobní údaje v nezbytném rozsahu zpracovávat bez souhlasu ve smyslu § 5 odst. 2 písm. b) zákona č. 101/2000 Sb., protože jinak by nemohla dostát svému smluvnímu závazku.

---

[6] Blíže k otázce legitimity účelu a principu minimalizace zásahu do soukromí srov. Kučerová, A., Nováková, L., Foldová, V., Nonnemann, F., Pospíšil, D. Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012.

[7] Viz § 5 odst. 1 písm. g) zákona č. 101/2000 Sb.

[8] Blíže k náležitostem souhlasu se zpracováním osobních údajů viz stanovisko Úřadu č. 2/2008.

Další povinnosti při zpracování osobních údajů

Jak je výše uvedeno, provozování inteligentních sítí v souvislosti s distribucí a měřením spotřeby energie v domácnostech bude bezpochyby spjato se zpracováním osobních údajů. Každý subjekt, který se na zpracování bude podílet, musí plnit všechny povinnosti, které mu ze zákona č. 101/2000 Sb. vyplývají. V kontextu předmětu tohoto stanoviska pak Úřad považuje za vhodné dále zdůraznit především následující:

- Jako klíčová se jeví především informační povinnost upravená v § 11 zákona č. 101/2000 Sb. a její včasné a kompletní plnění. Podle tohoto ustanovení zákona je správce povinen subjekt údajů při shromažďování údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány, kdo a jakým způsobem tak bude činit, komu mohou být údaje zpřístupněny a dále o právu subjektu údajů na informace o jeho zpracovávaných osobních údajích a o právu na námitku proti zpracování, které jsou upraveny v § 12 a 21 zákona č. 101/2000 Sb. Pouze tehdy, obdrží-li subjekt údajů o zamýšleném zpracování pravdivou informaci v zákonem vyžadovaném rozsahu, může platně projevit svoji vůli, tedy vyjádřit se zpracováním řádný souhlas nebo uzavřít příslušnou smlouvu.
- Zpracovávat osobní údaje v souladu s účelem zpracování, shromažďovat je pouze v nezbytném rozsahu, uchovávat je pouze po nezbytnou dobu a nesdružovat je s osobními údaji zpracovávanými za jinými účely (§ 5 odst. 1 písm. d), e), f a h) zákona č. 101/2000 Sb.).
- Zabezpečit zpracování osobních údajů tak, aby nemohlo dojít k nahodilému nebo neoprávněnému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům či k jejich jinému zneužití. Blíže tuto povinnost upravuje § 13 zákona č. 101/2000 a je ji nutno vztáhnout na všechny komponenty inteligentní sítě, které pracují s informacemi charakteru osobních údajů, tzn. i na samotné měřicí zařízení, přenosovou soustavu atd.
- Před samotným započetím zpracování, které bude založeno na souhlasu dotčených osob, oznámit Úřadu úmysl zpracovávat osobní údaje v rámci inteligentních sítí. Rozsah informací, které je budoucí správce povinen poskytnout, a některé další procesní náležitosti jsou upraveny v § 16 a násl. zákona č. 101/2000 Sb. Informace o takovýchto zpracování osobních údajů jsou následně obsaženy v registru oznámených zpracování, který je veřejně přístupný na internetových stránkách Úřadu.

Využití osobních údajů pro adresný marketing

Úřad si je vědom toho, že informace o spotřebitelských zvyklostech odběratelů energií a případných dalších členů jejich domácnosti mohou mít značnou marketingovou hodnotu. Využití osobních údajů pro nabízení obchodu a služeb upravuje § 5 odst. 5 a násl. zákona č. 101/2000 Sb. tak, že bez souhlasu subjektu údajů lze využít pouze údaje v rozsahu jméno, příjmení a adresa. V případě, když budou adresné marketingové nabídky zasílány prostřednictvím elektronických komunikací, se potom uplatní zvláštní úprava zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů. Podle § 7 odst. 3 tohoto zákona může dodavatel využít pro nabízení obchodu či služeb elektronický kontaktní údaj svého zákazníka, který od něj získal v souvislosti s prodejem výrobku nebo služby, bez jeho souhlasu pouze tehdy, pokud se odesílané obchodní sdělení týká jeho vlastních obdobných výrobků nebo služeb, především tedy dodávek energií. Pro realizaci takovéhoto způsobu marketingu je tak přípustné využití i základní informace o tom, jaké zboží či služby již byly danému odběrateli poskytnuty. S ohledem na předmět tohoto stanoviska to budou například informace o tarifu, který byl s určitým odběratelem dohodnut, pokud cílem zaslaného obchodního sdělení bude informace o dalších cenových možnostech atd.

Jakékoliv další informace týkající se určitého spotřebitele včetně informací o jeho spotřebitelských či životních zvyklostech, o jím používaných spotřebičích a jejich charakteristikách, např. spotřebě energií a výkonu, lze za účelem přímého marketingu zpracovávat zásadně jen s předchozím souhlasem subjektu údajů, přičemž i tento pochopitelně musí mít výše uvedené náležitosti. Jinými slovy, pokud subjekt podílející se na zpracování osobních údajů spotřebitelů v rámci provozu inteligentních sítí hodlá získané informace mimo základní identifikační údaje

využívat k adresnému nabízení obchodu či služeb, musí o tomto účelu spotřebitele předem vyrozumět, poskytnout mu o takovémto zpracování řádnou informaci v rozsahu vyžadovaném § 11 zákona č. 101/2000 Sb., získat k tomu jeho platný souhlas a i takovéto zpracování oznámit Úřadu. V opačném případě bude takové zpracování nezákonné.

Závěr

Úřadu nepřísluší hodnotit technické a hospodářské aspekty inteligentních sítí a souvisejících technických zařízení. Zdůrazňuje však, že vždy, kdy bude sledována spotřeba energií fyzických osob prostřednictvím inteligentního měření, bude docházet k zásahu do jejich soukromí a ke zpracování jejich osobních údajů. V návaznosti na nastavení celého systému se může jednat o více, či méně invazivní jednání. Nicméně v každém případě je nezbytné, aby ten, kdo inteligentní sítě a prvky inteligentního systému měření zavádí a provozuje, si byl vědom skutečnosti, že zpracovávané informace mají charakter osobních údajů a že se z tohoto důvodu musí řídit i právními předpisy upravujícími právě ochranu osobních údajů.

Stanovisko č. 2/2014

červenec 2014[1]

Dynamický biometrický podpis z pohledu zákona o ochraně osobních údajů

Úvod

Úřad pro ochranu osobních údajů (dále jen "Úřad") se v rámci své konzultační činnosti setkává s problematikou tzv. dynamického biometrického podpisu, často označovaným také jako digitální nebo elektronický podpis umožňující automatické rozpoznávání biometrických prvků. Jedná se o nahrazení tradičního podepisování se na papír za podepisování se na speciální zařízení (tablet nebo tzv. signpad) pro snímání podpisu, prostřednictvím kterého dochází jak k zachycení grafické podoby vlastnoručního podpisu na obrazovce tohoto zařízení, tak i k zachycení tzv. dynamických parametrů pohybu ruky jako je tlak, rychlost, sklon, křivky, posloupnost tahů apod. Následně je tento podpis, resp. jeho grafická podoba, společně s dynamickými parametry pohybu ruky převeden do elektronické podoby, většinou zašifrovaně, a takto je připojen k podepisovanému dokumentu. Tento nový způsob podepisování začínají již v praxi využívat při jednání se zákazníky například někteří telefonní operátoři, banky či pojišťovny anebo také poskytovatelé poštovních služeb.

Využití technologie biometrického podpisu může sice přinést značnou úsporu nákladů především v oblasti uchovávání smluvní dokumentace, úsporu času spočívající ve zrychlení obchodních a smluvních procesů, vyšší míru jistoty při ověřování pravosti podpisů a zvýšení celkové efektivity činnosti. Jsou s ním však také spojena rizika týkající se mimo jiné ochrany osobních údajů podepisovaných osob. Lze předpokládat, že k zavedení této technologie budou přistupovat i další subjekty, a proto Úřad považuje za nezbytné se souvisejícími otázkami ochrany osobních údajů zabývat.

Aplikace zákona o ochraně osobních údajů

Pravidla zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ve znění pozdějších předpisů, ve smyslu ustanovení § 3 vymezujícího působnost tohoto zákona je nutné aplikovat, pokud dané jednání naplňuje definiční znaky zpracování a předmětem takového jednání je informace spadající do kategorie osobních údajů, přičemž současně není dán důvod pro vyloučení takového jednání z působnosti tohoto zákona.

Osobním údajem podle § 4 písm. a) zákona č. 101/2000 Sb. je jakákoliv informace týkající se určeného nebo určitelného subjektu údajů, přičemž subjekt údajů se považuje za určený nebo určitelný, pokud jej lze na základě poskytnutých informací přímo či nepřímo identifikovat. Podpis lze považovat za jakousi jedinečnou osobní značku člověka, kterou nejen v závazkových vztazích projevuje svoji vůli, tj. vyjadřuje svůj souhlas s danou smlouvou. Jak na základě vlastnoručního podpisu na papír, tak i dynamického biometrického podpisu s použitím dalších údajů, kterými správce údajů ve smluvních vztazích obvykle disponuje, je podepsaná osoba bezesporu identifikovatelná. V obou případech proto podpis naplňuje znaky osobního údaje dle citovaného ustanovení zákona.

Existence osobního údaje však sama o sobě ještě nezakládá působnost zákona č. 101/2000 Sb., a proto je nutné, aby s takovým údajem byla za určitým účelem prováděna jakákoliv operace nebo soustava operací odpovídajících pojmu zpracování podle § 4 písm. e) zákona č. 101/2000 Sb. Těmito operacemi s osobními údaji se rozumí zejména jejich shromažďování, ukládání na datové nosiče, uchovávání, zpřístupňování, zveřejňování, třídění apod.[2] V kontextu ochrany osobních údajů je u uvedených operací důraz kladen na účelovost jejich provádění. Pro naplnění

[1] Podle stavu právních předpisů k 1. červenci 2014.

definice zpracování osobních údajů je rozhodující, aby předmětné jednání spočívající v nakládání s osobními údaji představovalo cílené využívání osobních údajů.

Při shromažďování osobních údajů klientů v rámci smluvní dokumentace, která obsahuje i podpisy, a při dalších operacích prováděných s těmito údaji, tedy uchovávání, využívání pro ověřování podpisů při běžných transakcích nebo v případě sporu o platnost podpisu atd., dochází ke zpracování osobních údajů, a to všech předmětných informací včetně podpisu.

Samotné podepsání se ještě sice není zpracováním osobních údajů, ale při užívaní technologie biometrického podepisování, na rozdíl od klasického podpisu na papír, je automaticky speciálním zařízením (tablet, signpad) již při podepsání nejdříve snímaná a poté zaznamenána grafická podoba podpisu, přičemž jsou současně vygenerovány a uloženy dynamické parametry pohybu ruky podepisující se osoby. Tímto způsobem dochází cíleně ke sběru údajů, jejich shromažďování, ukládání na datové nosiče, uchovávaní [tzn. jejich zpracování ve smyslu § 4 písm. e) zákona č. 101/2000 Sb.], a to vše za účelem, aby údaje mohly být v případě potřeby dále použity. Údaje jsou většinou současně převedeny do elektronického formátu v určitém např. číselném vyjádření, přičemž zůstává zachována i grafická podoba vlastnoručního podpisu.

Pokud jsou naplněny všechny předpoklady pro aplikaci zákona č. 101/2000 Sb., zbývá ještě určit subjekt, který bude za zpracování osobních údajů odpovídat, tedy správce osobních údajů podle § 4 písm. j) zákona č. 101/2000 Sb. Ve smyslu tohoto ustanovení bude správcem ten subjekt, který určuje účel zpracování, a nezmocní-li nebo nepověří-li zpracováním zpracovatele, také zpracování provádí a odpovídá za něj. V praxi bude tímto správcem například banka nebo telefonní operátor, který technologii biometrického podpisu zavede do své činnosti a bude ji při styku s klienty využívat, neboť evidentně právě tento subjekt určuje jak účel, tak i prostředky daného zpracování. Jako správce osobních údajů pak musí plnit všechny povinnosti stanovené zákonem č. 101/2000 Sb.

Dynamický biometrický podpis jako citlivý údaj

Zvláštní kategorií osobních údajů tvoří citlivé údaje. Ustanovení § 4 písm. b) zákona č. 101/2000 Sb. citlivý údaj definuje jako informaci týkající se identifikované či identifikovatelné fyzické osoby, která současně spadá do některé ze zde taxativně uvedených zvláštních kategorií osobních údajů, mj. se jedná také o biometrické údaje umožňující přímou identifikaci nebo autentizaci konkrétního člověka.[3] V případě, že následně dochází ke zpracování citlivých údajů, je nutné aplikovat přísnější režim, protože právě takové zpracování může způsobit mnohem závažnější zásah do soukromí subjektu údajů, než je tomu v případě zpracování „obyčejných“ osobních údajů.

Písmo a stejně tak i podpis, zachyceny v jakékoliv podobě, lze považovat za jedinečný znak každého jednotlivce. Podrobnou analýzou vlastnoručního podpisu lze zpracovávat nejrůznější informace o pohybu ruky v době pořízení podpisu, jako například sklon písma, tlak ruky, rychlost psaní, velikost písma apod., z nichž pak znalec dokáže tuto osobu s větší, či menší mírou pravděpodobnosti identifikovat nebo autentizovat. Tyto informace, resp. dynamické rysy odpovídají definici biometrického, a tedy i citlivého údaje ve smyslu zákona 101/2000 Sb. Klasický podpis zachycený na papír, a stejně tak i dynamický biometrický podpis obsahují odpovídající sumu informací (sklon písma, tlak a rychlost psaní atd.), a jsou tedy nositeli biometrických údajů.

Při posuzování další aplikace zákona č. 101/2000 Sb. je nezbytné vycházet z toho, co je o zpracování údajů výše uvedeno. Samotné pořizování a uchovávání podpisu bez jeho využití jako citlivého údaje proto nelze bez dalšího považovat za zpracování citlivých údajů. K takovému zpracování dochází až tehdy, pokud je podpis např. podroben písmoznalecké analýze za účelem ověření jeho pravosti v případě sporu. O zpracování citlivých údajů obsažených v podpisu se jedná, pokud tyto údaje jsou správcem aktivně využívány. Takový názor lze analogicky dovodit

[2] Blíže k pojmu zpracování osobních údajů viz stanovisko Úřadu č. 4/2013 K pojetí zpracování osobních údajů.
[3] Viz § 4 písm. b) zákona č. 101/2000 Sb.

i ze stanoviska WP29 č. 5/2009[4], ve kterém je uvedeno, že samotná fotografie fyzické osoby zveřejněná na internetu, která je bezpochyby také nositelem biometrických a dalších citlivých údajů, není citlivým údajem, pokud taková fotografie není jasně užita k dalším účelům, např. k odhalení v ní obsažených citlivých údajů. Bez dalšího tedy nelze ani na klasický podpis na papír nahlížet jako na citlivý údaj ve smyslu zákona č. 101/2000 Sb.

V případě dynamického biometrického podpisu však ke zpracování citlivých údajů dochází automaticky. Dynamické prvky jsou speciální technologií cíleně vygenerovány a zachyceny jako přidaná hodnota k samotnému grafickému znázornění podpisu, takže grafické znázornění a biometrické údaje existují vedle sebe a v této podobě jsou s nimi prováděny i následné operace. Zpracování citlivých údajů se při použití technologie biometrického podepisování lze vyhnout pouze v případě, kdy zařízení zaznamená pouze grafickou podobu podpisu, tedy pokud nedojde ke zpracování biometrických údajů. V případech kdy budou správci prostřednictvím technologie vytvářet podpisové vzory a databáze těchto vzorů, je z podstaty věci zřejmé, že musí docházet i ke zpracování citlivých údajů, a je proto nezbytné, aby takové zpracování vždy probíhalo v přísnějším režimu § 9 zákona č. 101/2000 Sb.

Povinnosti při zpracování údajů podle zákona č. 101/2000 Sb.

Zákon č. 101/2000Sb. stanoví každému správci řadu povinností, přičemž většina z nich se aplikuje stejně na zpracování „obyčejných“ osobních údajů i citlivých údajů. Základní povinnosti správce jsou uvedeny v § 5 odst. 1 zákona č. 101/2000 Sb. Ještě před započetím daného zpracování je nutné ve smyslu § 5 odst. 1 písm. a) a b) zákona č. 101/2000 Sb. nejdříve stanovit základní parametry zpracování, tedy účel, k němuž mají být údaje zpracovány a pak způsob a prostředky tohoto zpracování. Právě splnění těchto povinností předurčuje charakter daného zpracování. V průběhu zpracování je správce povinen dodržet všechny další podmínky stanovené v odst. 1, přičemž je zejména nutné dbát na dodržení § 5 odst. 1 písm. d) zákona č.101/2000 Sb., tedy vždy zpracovávat pouze údaje odpovídající stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu.

Nezbytnou podmínkou každého zpracování je existence zákonem uznaného právního titulu pro zpracování údajů. Zpracování osobních údajů může v souladu s § 5 odst. 2 zákona č. 101/2000 Sb. probíhat buď na základě souhlasu subjektu údajů, nebo na základě některého z dalších právních titulů uvedených pod písm. a) až g) tohoto ustanovení. Pokud je podpis zpracováván pouze jako „obyčejný“ osobní údaj, lze aplikovat především právní titul podle § 5 odst. 2 písm. b) zákona č. 101/2000 Sb., který se uplatní právě v případě zpracování nezbytného pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů.

V případě dynamického biometrického podpisu je však vzhledem k citlivému charakteru zpracovaných údajů nutné postupovat v přísnějším režimu § 9 zákona č. 101/2000 Sb. Ze zde uvedeného výčtu možných právních titulů pro zpracování citlivých údajů pak v případě dynamického biometrického podpisu přichází v úvahu pouze souhlas dotčené osoby. Oproti souhlasu se zpracováním „obyčejných“ osobních údajů je zde navíc stanovená kvalifikovaná forma souhlasu, spočívající v jeho výslovnosti. Správce, který bude prostřednictvím technologie biometrického podepisování zpracovávat citlivé údaje fyzické osoby, tedy musí disponovat jejím jednoznačným a výslovným souhlasem.

Podle názoru Úřadu na cílené zpracování citlivých údajů prostřednictvím dynamického biometrického podpisu v zásadě žádný jiný právní titul podle § 9 zákona č. 101/2000 Sb. aplikovat nelze.

Při zpracování citlivých údajů na základě výslovného souhlasu podle § 9 písm. a) zákona č. 101/2000 Sb. musí správce vůči subjektu údajů ještě před udělením tohoto souhlasu splnit

[4] Dokument Pracovní skupiny pro ochranu dat podle článku 29 (WP 29) směrnice 95/46/ES je dostupný na http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

informační povinnost v tomto ustanovení uvedenou, která se fakticky shoduje s informační povinností podle § 11 zákona č. 101/2000 Sb. Subjekt údajů musí být informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Obsahem plnění informační povinnosti u dynamického biometrického podepisování musí být i informace o tom, že prostřednictvím technologie pro automatické rozpoznávání biometrických prvků jsou jako neoddělitelná součást grafické podoby podpisu zaznamenávány i další informace, a jaké, tedy dynamické parametry pohybu ruky podepisující se osoby, které splňují definici citlivého údaje podle § 4 písm. b) zákona č. 101/2000 Sb. Tuto povinnost lze v praxi plnit například prostřednictvím smluvních podmínek. Správce musí subjekt údajů také poučit o právu na přístup k informacím o zpracování podle § 12 zákona č. 101/2000 Sb. a povinnostech správce související s ochranou práv subjektu údajů podle § 21 zákona č. 101/2000 Sb. K poskytnutí těchto informací musí dojít nejpozději současně s udělením výslovného souhlasu, přičemž správce tento souhlas musí být schopen prokázat po celou dobu zpracování. Pokud subjekt údajů odmítne správci udělit souhlas ke zpracování citlivých údajů, musí mu správce umožnit podepsat se klasickým způsobem přímo na papírový dokument.

Vzhledem k povaze zpracování údajů v případě dynamického biometrického podpisu, je nutné upozornit na povinnosti týkající se zabezpečení osobních údajů podle § 13 zákona č. 101/2000 Sb. Toto ustanovení správci ukládá, aby zajistil, že k údajům nebude moci mít žádná třetí osoba neoprávněný nebo nahodilý přístup a že nedojde k jejich změně, zničení, ztrátě, neoprávněnému přenosu nebo jinému neoprávněnému zpracování. Odpovědnost za plnění této povinnosti je zákonem konstruována jako objektivní, tzn. v případě, kdy osobní údaje například budou přístupné neoprávněné osobě, budou v průběhu přenosu ztraceny, změněny apod., bude jednání správce porušením § 13 zákona č. 101/2000 Sb., a tedy správním deliktem, za který nebude odpovídat pouze v případě, že prokáže, že vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránil (viz § 46 odst. 1 zákona č. 101/2000 Sb.). Vzhledem k citlivému charakteru zpracování biometrických údajů je nutné právě u tohoto zpracování klást na zabezpečení údajů zvláštní důraz. V praxi to znamená zejména užívání kvalitní a ověřené technologie pro pořizování dynamického biometrického podpisu, náležité šifrování surových biometrických údajů, zajištění bezpečnosti přenosu údajů a jejich dalšího uchovávání, zajištění nevratné likvidace atd.

Je také nutné zmínit oznamovací povinnost vůči Úřadu podle § 16 zákona č. 101/2000 Sb. Tuto povinnost správce nemusí plnit pouze v případě, že se na něj vztahuje některá výjimka z oznamovací povinnosti podle § 18 tohoto zákona. Zpracování klasického podpisu jako osobního údaje sice Úřadu není potřeba oznamovat, avšak v souvislosti s výše uvedenými pravidly pro posuzování zpracování údajů prostřednictvím technologie biometrického podepisování lze konstatovat, že v případě zpracování biometrických údajů se již jedná o kvalitativně odlišné, a tedy nové zpracování. Na takové zpracování nelze uplatnit žádnou z výjimek z oznamovací povinnosti dle § 18 odst. 1 zákona č. 101/2000 Sb., a správce tak bude povinen ještě předtím, než zpracování zahájí, tuto skutečnost Úřadu oznámit.

Vzhledem k povaze dynamického biometrického podpisu jako neměnného, resp. obtížně změnitelného údaje, je třeba upozornit na značná rizika spojená s jeho odcizením resp. s přístupem neoprávněné osoby k těmto údajům. Proto je třeba, aby před poskytnutím biometrických údajů o podpisu a udělením souhlasu s jejich zpracováním, každý důkladně posoudil důvěryhodnost správce, kterému tyto osobní údaje poskytuje.

Závěr

Podpis v jakékoliv podobě je osobním údajem a ve smluvních vztazích dochází k jeho zpracování. Klasický a stejně tak i dynamický biometrický podpis obsahují biometrické údaje, při využívaní technologie dynamického biometrického podepisování však dochází k jejich automatickému zpracování, které může probíhat pouze v režimu § 9 zákona č. 101/2000 Sb. Jediným právním titulem, na základě kterého je takové zpracování obecně realizovatelné, je výslovný a informovaný souhlas každého subjektu údajů podle § 9 písm. a) zákona č. 101/2000 Sb., který musí být správce schopen prokázat po celou dobu zpracování. O zpracování citlivých údajů tedy musí být

subjekt údajů řádně informován a správce musí plnit všechny další povinnosti, které se vztahují jak na zpracování osobních, tak i citlivých údajů podle zákona č. 101/2000 Sb. Zvýšenou pozornost je nutné věnovat zejména plnění informační a oznamovací povinnosti a zabezpečení biometrických údajů. Vzhledem k současnému vývoji a novým trendům je potřeba uvést, že výše uvedená pravidla ochrany osobních údajů budou obdobně platit i pro další technologie zpracovávající biometrické údaje umožňující identifikaci či autentizaci subjektů údajů.

III. SDĚLENÍ ÚŘADU

Informace o ztrátě služebního průkazu

V červnu 2014 došlo ke ztrátě služebního průkazu inspektora Úřadu pro ochranu osobních údajů č. 052, který byl vydán dne 16. prosince 2011.

Průkaz je (dle nařízení vlády č.277/2011 Sb.) oboustranná papírová karta se zaoblenými rohy o rozměrech 6,8 x 9,9 cm, která je zatavena do průhledné laminační fólie o rozměrech 7,4 x 10,5 cm a je na lícové i rubové straně opatřen ochrannými prvky, kterými jsou rastrový šedožlutý podtisk s irisovým přechodem barev, vodoznak, vlákna viditelná za denního světla a vlákna viditelná v ultrafialovém světle. Průkaz má na přední straně vytištěn státní znak a fotografii inspektora.

V případě nálezu služebního průkazu se obraťte na Úřad pro ochranu osobních údajů. Zneužití služebního průkazu se trestá.

PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

1021/00/CS
WP207

Stanovisko č. 6/2013 k veřejně přístupným údajům a opakovanému použití informací veřejného sektoru

Přijaté dne 5. června 2013

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán ve věci ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Její sekretariát je na Ředitelství C (Základní práva a občanství Unie) Evropské komise, Generální ředitelství pro spravedlnost, B-1049 Brusel, Belgie, kancelář MO-59 02/013.

Internetové stránky: http://ec.europa.eu/justice/data-protection/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,

s ohledem na článek 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice,

s ohledem na svůj jednací řád,

PŘIJALA TOTO STANOVISKO:

I. Úvod

1.1. Revize směrnice o informacích veřejného sektoru

Dne 26. června 2013 přijala Evropská unie směrnici Evropského parlamentu a Rady 2013/37/EU (dále jen „novela směrnice“), kterou se mění směrnice 2003/98/ES o opakovaném použití informací veřejného sektoru (dále jen „směrnice o informacích veřejného sektoru“)[1].

Cílem směrnice o informacích veřejného sektoru je usnadnit opakované použití informací veřejného sektoru, a to harmonizací podmínek opakovaného použití v celé Evropské unii a odstraněním zbytečných překážek pro opakované použití těchto informací na vnitřním trhu.

Původní znění směrnice o informacích veřejného sektoru z roku 2003 harmonizovalo podmínky opakovaného použití, nevyžadovalo však, aby subjekty veřejného sektoru zpřístupňovaly údaje pro opakované použití. Odpověď na otázku, zda údaje zpřístupnit pro opakované použití, byla v podstatě libovolná: rozhodnutí bylo ponecháno na členských státech a dotčených subjektech veřejného sektoru. V důsledku toho se mnoho subjektů veřejného sektoru v celé Evropě jednoduše rozhodlo, že opakované použití svých informací nepovolí.

V tomto kontextu je jedním z hlavních politických cílů novely směrnice zavedení zásady, že veškeré veřejné informace (tj. veškeré informace, které má v držení veřejný sektor a které jsou veřejně přístupné podle vnitrostátního práva) jsou opakovaně použitelné pro komerční a nekomerční účely. V určitých případech platí výjimky z oblasti působnosti pozměněné směrnice o informacích veřejného sektoru, mimo jiné z důvodu ochrany údajů[2].

Pozměněná směrnice o informacích veřejného sektoru tudíž nyní subjektům veřejného sektoru ukládá povinnost povolit opakované použití všech informací veřejného sektoru, které mají v držení. Jak však bude prokázáno níže, směrnice neukládá subjektům veřejného sektoru povinnost zveřejňovat osobní údaje. Vyžaduje pouze opakované použití informací, jsou-li tyto již veřejně přístupné podle vnitrostátního práva, a i tehdy pouze v případě, nejsou-li opakovaným použitím dotčena ustanovení platných právních předpisů o ochraně údajů.

Další příslušná nová ustanovení novely směrnice rozšiřují oblast působnosti směrnice o informacích veřejného sektoru na knihovny (včetně univerzitních), archivy a muzea.

Na základě výše uvedených skutečností může pozměněná směrnice o informacích veřejného sektoru významně zvýšit dostupnost informací, které mají v držení subjekty veřejného sektoru.

1 Úř. věst. L 175, 27.6.2013, s. 1.

2 Pokud jde o oblast působnosti pozměněné směrnice o informacích veřejného sektoru a ustanovení týkající se ochrany údajů, viz oddíl V.

1.2. Opakované použití informací veřejného sektoru a osobní údaje

Iniciativy týkající se opakovaného použití informací veřejného sektoru obvykle zahrnují i) zpřístupnění celých databází ii) ve standardizovaném elektronickém formátu iii) jakémukoli žadateli bez prověření iv) bezplatně (nebo s omezenými poplatky) a v) pro komerční nebo nekomerční účely bez jakýchkoli podmínek (nebo za neomezujících podmínek, případně prostřednictvím licence)[3].

To může zajistit přínosy vedoucí k větší transparentnosti a inovativnímu opakovanému použití informací veřejného sektoru. Výsledná větší dostupnost informací však není bez rizika.

Aby se tato rizika omezila na minimum, musí v případě, že se to týká osobních údajů, právní předpisy o ochraně údajů pomoci řídit proces výběru osobních údajů, které mohou či nemohou být zpřístupněny pro opakované použití, a opatření, která je nutno přijmout k ochraně osobních údajů. Ve všech případech, kdy je v sázce ochrana soukromí a osobních údajů, je třeba uplatňovat vyvážený přístup. Pravidla ochrany osobních údajů by na straně jedné neměla představovat neoprávněnou překážku rozvoje trhu pro opakované použití. Na straně druhé musí být respektováno právo na ochranu osobních údajů a právo na soukromí. Je důležité zdůraznit, že jako koncepce se zpřístupňování údajů zaměřuje na transparentnost a odpovědnost subjektů veřejného sektoru a na hospodářský růst, nikoli na transparentnost jednotlivých občanů.

Při uplatňování směrnice o informacích veřejného sektoru a právních předpisů o ochraně údajů na opakované použití osobních údajů musí subjekt veřejného sektoru pravděpodobně přijmout jedno ze tří různých rozhodnutí:

1. rozhodnutí o nezpřístupnění osobních údajů pro opakované použití za podmínek stanovených ve směrnici o informacích veřejného sektoru
2. rozhodnutí o přeměně osobních údajů na anonymizovanou podobu (obvykle agregované statistické údaje)[4] a zpřístupnění pouze těchto anonymizovaných údajů pro opakované použití
3. rozhodnutí o zpřístupnění osobních údajů pro opakované použití (v případě potřeby s výhradou zvláštních podmínek a náležitých ochranných opatření).

II. Cíl stanoviska

2.1. Jednotné pokyny a osvědčené postupy

Cílem tohoto stanoviska je pomoci zajistit společné chápaní platného právního rámce a poskytnout jednotné pokyny a příklady osvědčených postupů, pokud jde o způsob provedení (pozměněné) směrnice o informacích veřejného sektoru s ohledem na zpracovávání osobních údajů.

Toto stanovisko se nepokouší harmonizovat vnitrostátní přístupy, co se týká úrovně transparentnosti, vnitrostátních právních předpisů o přístupu k dokumentům a dostupnosti informací podle těchto vnitrostátních právních předpisů. Vnitrostátní právní předpisy k provedení směrnice o informacích veřejného sektoru a výklad směrnice 95/46/ES[5] s ohledem na opakované použití těchto informací se však v jednotlivých členských státech někdy natolik liší, že to jde nad rámec

[3] Podotýká se, že podle čl. 8 odst. 1 směrnice o informacích veřejného sektoru v platném znění nesmějí licenční „podmínky zbytečně omezovat možnosti opakovaného použití a nesmějí být použity pro omezování hospodářské soutěže“.

[4] Co se týká opakovaného použití souborů agregovaných a anonymizovaných údajů odvozených z osobních údajů, viz oddíl VI.

[5] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, 23.11.1995, s. 31).

toho, co může být nezbytné vzhledem k rozmanitosti vnitrostátních režimů přístupu a rozdílné úrovni transparentnosti.

Politická doporučení k soukromí, která v září 2012 vydala tematická síť LAPSI, jednoznačně dokládají zbytečné rozdíly ve způsobu provedení směrnice o informacích veřejného sektoru v jednotlivých členských státech, pokud jde o ochranu osobních údajů[6]. Samotná směrnice o informacích veřejného sektoru upozorňuje, že zákonodárné rozdíly a nejistoty by mohly být ještě významnější s dalším rozvojem informační společnosti, která již značně rozšířila využívání informací překračující hranice států[7].

Nejednotný přístup může oslabit postavení dotčených fyzických osob. Může rovněž představovat zbytečnou regulační zátěž pro podniky a jiné organizace působící na přeshraničním základě, a tudíž být překážkou rozvoje společného evropského trhu pro opakované použití. Subjekty údajů musí být na straně jedné ujištěny, že jejich údaje budou důsledně chráněny bez ohledu na jejich předání do jiného členského státu za účelem opakovaného použití. Na straně druhé je třeba zamezit rovněž zbytečné složitosti a roztříštěnosti s cílem umožnit volný tok osobních údajů v celé Evropě, což je další hlavní cíl směrnice 95/46/ES.

2.2. Potřeba aktualizace stanoviska č. 7/2003

Novela směrnice následuje deset let od přijetí směrnice o informacích soukromého sektoru v roce 2003. V té době přijala pracovní skupina podle článku 29 stanovisko k otázkám ochrany údajů v souvislosti s informacemi veřejného sektoru („stanovisko č. 7/2003“)[8]. Ačkoli hlavní zásady uvedené ve stanovisku č. 7/2003 zůstávají platné, technologický a jiný vývoj v oblasti informací veřejného sektoru a ochrany údajů, včetně navrhovaných legislativních změn v obou oblastech, odůvodňuje stávající snahu o aktualizaci a doplnění stanoviska z roku 2003.

Stanovisko může nyní mimoto zohlednit i jiné nedávné a probíhající snahy o poskytnutí dalších pokynů, zejména:

- stanovisko evropského inspektora ochrany údajů (EIOÚ) ze dne 18. dubna 2012 k balíčku opatření Komise týkajících se veřejně přístupných údajů[9],
- stanovisko pracovní skupiny podle článku 29 č. 3/2013 k omezení účelu[10],
- probíhající práci v technologické podskupině pracovní skupiny podle článku 29 pro techniky anonymizace[11],
- práci v oblasti anonymizace a posuzování rizik v některých členských státech[12] a

---

[6] LAPSI je evropská tematická síť pro právní aspekty informací veřejného sektoru (Legal Aspects of Public Sector Information), kterou financuje Evropská komise, viz http://www.lapsi-project.eu/. Politické doporučení je k dispozici na adrese http://www.lapsi-project.eu/lapsifiles/lapsi_privacy_policy.pdf

[7] Viz 7. bod odůvodnění.

[8] Viz stanovisko pracovní skupiny podle článku 29 č. 7/2003 k opakovanému použití informací veřejného sektoru a ochraně osobních údajů – nastolení rovnováhy – přijaté dne 12. prosince 2003 (WP 83). Viz rovněž dvě předchozí související stanoviska pracovní skupiny podle článku 29: stanovisko č. 3/1999 k informacím veřejného sektoru a ochraně osobních údajů přijaté dne 3. května 1999 (WP 20) a stanovisko č. 5/2001 týkající se zvláštní zprávy evropského veřejného ochránce práv přijaté dne 17. května 2001.

[9] Stanovisko evropského inspektora ochrany údajů ze dne 18. dubna 2012 k balíčku opatření Evropské komise týkajících se veřejně přístupných údajů, včetně návrhu směrnice, kterou se mění směrnice 2003/98/ES o opakovaném použití informací veřejného sektoru, sdělení o veřejně přístupných údajích a rozhodnutí Komise 2011/833/EU o opakovaném použití dokumentů Komise. K dispozici na adrese: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-04-18_Open_data_EN.pdf

[10] Stanovisko pracovní skupiny podle článku 29 č. 3/2013 k omezení účelu přijaté dne 2. dubna 2013 (WP 203).

[11] Stanovisko k tomuto tématu má být podle očekávání přijato v druhém pololetí roku 2013.

- stávající judikaturu a praxi v některých členských státech, pokud jde o dosažení rovnováhy mezi opakovaným použitím a ochranou osobních údajů[13].

III. Zaměření a struktura stanoviska

Stanovisko č. 7/2003 se zaměřilo na zásadu omezení účelu[14], zabývalo se však rovněž jinými otázkami, jako jsou zákonné důvody zveřejnění a opakované použití informací veřejného sektoru, zvláštní ochrana citlivých údajů, předávání do třetích zemí, kvalita údajů a práva subjektů údajů. Tyto připomínky jsou dosud platné. Vzhledem k předchozí práci toto stanovisko pouze aktualizuje a doplňuje závěry uvedené ve stanovisku č. 7/2003, je-li to nezbytné vzhledem k novému legislativnímu a technologickému vývoji.

Oddíl IV pomáhá objasnit, že povinností týkající se opakovaného použití podle pozměněné směrnice o informacích veřejného sektoru nejsou dotčeny požadavky na ochranu údajů, a zdůrazňuje význam „ochrany údajů již od návrhu“ a „standardního nastavení ochrany údajů“ a „posouzení dopadu na ochranu údajů“ s cílem pomoci zajistit, aby byly otázky ochrany údajů vyřešeny před zpřístupněním osobních údajů k opakovanému použití.

Oddíl V poskytuje prostřednictvím názorných příkladů vodítko k tomu, jaký druh osobních údajů může spadat do oblasti působnosti směrnice o informacích veřejného sektoru.

Oddíl VI se zaměřuje na situace, které jsou v současnosti v iniciativách týkajících se opakovaného použití informací veřejného sektoru nejběžnější: případy, kdy jsou agregované statistické údaje odvozené z osobních údajů zpřístupněny v agregované a anonymizované podobě. K příkladům patří agregované statistické údaje o kriminalitě, vládních výdajích nebo o tom, jak si vedou školáci v různých zeměpisných oblastech nebo v různých vzdělávacích institucích. Jelikož se jedná o nejčastější scénář opakovaného použití informací veřejného sektoru, které obsahují osobní údaje, bude mu věnována značná část stanoviska. Hlavní otázkou ochrany údajů je zde zajištění účinné agregace a anonymizace a minimalizace rizika, že ze souborů agregovaných údajů mohou být opětovně identifikovány osobní údaje.

Oddíl VII pojednává méně podrobně o případech, kdy jsou zveřejněny osobní údaje, které mohou být tudíž potenciálně dostupné pro opakované použití. Ačkoli to v současnosti nepředstavuje obvyklý scénář iniciativ týkajících se opakovaného použití informací veřejného sektoru, je důležité vzít v úvahu, že subjekty soukromého sektoru zpřístupňují osobní údaje stále více, často na internetu. Zde často hovoříme o přímo identifikovatelných osobních údajích, jako jsou například informace o vlastníkovi určité nemovitosti uvedené v katastru nemovitostí, prohlášení o zájmech nebo platy některých státních zaměstnanců či výdaje poslanců. Vyvstává rovněž otázka, do jaké míry, pro jaké účely, za jakých podmínek a s výhradou jakých ochranných opatření mohou být tyto údaje zpřístupněny pro opakované použití. Je důležité rovněž objasnit, zda se na tyto údaje vztahují ustanovení směrnice o informacích veřejného sektoru.

V této souvislosti je důležité zdůraznit, že veškeré informace týkající se identifikované nebo identifikovatelné fyzické osoby bez ohledu na to, zda jsou veřejně přístupné, či nikoli, představují osobní údaje. Na přístup k osobním údajům, které byly zpřístupněny veřejnosti (např. zveřejněním na internetu), a jejich opakované použití se proto i nadále vztahují platné právní předpisy o ochraně údajů.

---

[12] Viz například kodex anonymizace „Anonymisation: Managing data protection risk code of practice“ (Anonymizace: kodex řízení rizik pro ochranu údajů), který v listopadu 2012 vydal úřad komisaře pro informace ve Spojeném království, a pokyny k analýze rizik, které v červnu 2012 vydal francouzský orgán pro ochranu údajů.

[13] Viz například politické doporučení sítě LAPSI ze září 2012 (s. 4–14).

[14] Viz čl. 6 odst. 1 písm. b) směrnice 95/46/ES.

V oddílech VIII a IX budou stručně projednány některé další zvláštní scénáře, jako jsou údaje z výzkumu a historické archivy, jež nyní spadají do oblasti působnosti směrnice o informacích veřejného sektoru.

Oddíl X se zabývá otázkou vydávání licencí na opakované použití informací veřejného sektoru a potřebou začlenit případně do těchto licencí ustanovení o ochraně údajů.

Oddíl XI obsahuje soubor závěrů a doporučení.

IV. Ne všechny „veřejně přístupné“ osobní údaje by měly být zpřístupněny pro opakované použití

4.1. Povinností týkající se opakovaného použití podle směrnice o informacích veřejného sektoru nejsou dotčeny požadavky na ochranu údajů

Při přijetí v roce 2003 neukládala směrnice o informacích veřejného sektoru subjektům veřejného sektoru povinnost povolit opakované použití těchto informací. Rozhodnutí o povolení či nepovolení opakovaného použití bylo ponecháno na členských státech nebo na dotčeném subjektu veřejného sektoru (s výhradou vnitrostátního regulačního rámce týkajícího se transparentnosti a přístupu). Stanovisko č. 7/2003 bylo přijato na základě neexistence této povinnosti. V oddíle 2 písm. cc) stanoviska č. 7/2003 se uvádí: „Je důležité zdůraznit, že se směrnice o opakovaném použití nelze dovolávat jako právní povinnosti, kterou je nutno splnit, jelikož tato směrnice neukládá povinnost zveřejňovat osobní údaje“.

Po novele směrnice je analýza o něco složitější, konečný závěr je však týž.

V čl. 3 odst. 1 pozměněné směrnice o informacích veřejného sektoru se uvádí, že „s výhradou odstavce 2 členské státy zajistí, aby byly dokumenty, na které se vztahuje tato směrnice v souladu s článkem 1, opakovaně použitelné pro komerční nebo nekomerční účely v souladu s podmínkami podle kapitol III a IV“. Nelze-li opakované použití zamítnout z důvodů stanovených v článku 1 (důvody odvozené z vnitrostátních režimů přístupu a výslovně rovněž ochrana osobních údajů), musí být toto použití povoleno.

Ve 21. bodě odůvodnění směrnice o informacích veřejného sektoru se současně uvádí, že by tato „směrnice měla být provedena a uplatňována v plném souladu se zásadami ochrany osobních údajů“. V čl. 1 odst. 4 je mimoto stanoveno, že směrnice „ponechává nedotčenu a nijak neovlivňuje úroveň ochrany fyzických osob v souvislosti se zpracováním osobních údajů“.

Tato ustanovení společně znamenají, že „zásada opakovaného použití“ není automatická, je-li v sázce právo na ochranu osobních údajů, a že nepřevažuje nad platnými ustanoveními právních předpisů o ochraně údajů. Pokud existující dokumenty, které mají v držení subjekty soukromého sektoru, obsahují osobní údaje, jejich opakované použití spadá do oblasti působnosti směrnice 95/46/ES, a vztahují se na ně tudíž i nadále příslušné právní předpisy o ochraně údajů.

V případech, v nichž opakované použití zahrnuje osobní údaje, se subjekt veřejného sektoru nemůže systematicky dovolávat nutnosti dodržovat směrnici o informacích veřejného sektoru jako zákonného důvodu pro zpřístupnění údajů k opakovanému použití[15].

4.2. Význam posouzení dopadu na ochranu údajů před zpřístupněním údajů pro opakované použití

[15] Pracovní skupina podle článku 29 chce rovněž objasnit, že ani z hlediska dalšího uživatele nepředstavuje směrnice o informacích veřejného sektoru sama o sobě zákonný důvod pro zpracování. (Pokud jde o zákonné důvody, viz stanovisko č. 7/2003 a bod 7.5 níže.)

Vzhledem k možným rizikům spojeným s opakovaným použitím informací veřejného sektoru, a zejména vzhledem ke skutečnosti, že jakmile byly osobní údaje zpřístupněny pro opakované použití, bude velmi obtížné kontrolovat účinně použití těchto údajů, zdůrazňuje pracovní skupina podle článku 29 nutnost dodržovat zásady „ochrany údajů již od návrhu a standardního nastavení ochrany údajů“ a zajistit, aby byly otázky ochrany údajů řešeny v počáteční fázi. Pracovní skupina podle článku 29 zejména důrazně doporučuje, aby subjekt veřejného sektoru provedl před zpřístupněním osobních údajů pro opakované použití důkladné posouzení dopadu na ochranu údajů. Členské státy by měly uvážit učinění tohoto posouzení dopadu závazným podle vnitrostátních právních předpisů, nebo jeho prosazování jako osvědčeného postupu. I v případě, není-li to ve vnitrostátních právních předpisech výslovně stanoveno, měly by subjekty veřejného sektoru provést před zveřejněním informací a přijetím rozhodnutí o jejich zpřístupnění pro opakované použití důkladné posouzení s cílem zjistit, zda mohou být osobní údaje zpřístupněny k opakovanému použití, a je-li tomu tak, za jakých podmínek a s výhradou jakých konkrétních opatření k ochraně údajů je opakované použití přípustné.

Posouzení by mělo mimo jiné stanovit právní základ pro zveřejnění (a potenciální právní základ pro opakované použití), posoudit zásady týkající se omezení účelu, proporcionality a minimalizace údajů a uvážit zvláštní ochranu, která se vyžaduje u citlivých údajů. Při tomto posuzování je třeba pečlivě uvážit možný dopad na subjekty údajů.

Toto posouzení by mělo pomoci při rozhodování, zda mohou být osobní údaje zpřístupněny pro opakované použití a s výhradou jakých ochranných opatření[16]. Je třeba zdůraznit, že navrhované nařízení o ochraně údajů[17] podporuje a v některých případech vyžaduje posouzení dopadu na ochranu údajů jako hlavní nástroj, který má pomoci zajistit odpovědnost správců údajů[18].

Je-li to možné, měla by být analýza před rozhodnutím o opakovaném použití založena na informované diskusi a zastoupení různých zúčastněných stran, včetně správce údajů, který chce údaje zveřejnit, avšak rovněž subjektů požadujících údaje, jež tudíž mohou poskytnout rámec pro diskusi, a rovněž zástupců fyzických osob, o jejichž osobní údaje se jedná (např. organizací na ochranu spotřebitele, organizací pro práva pacientů, odborových svazů učitelů). Není-li výsledek jasný, mohou pokyny poskytnout příslušný orgán pro ochranu údajů a vnitrostátní orgány odpovědné za svobodný přístup k informacím.

Členské státy by měly uvážit rovněž zřízení znalostních sítí / center excelence a poskytování podpory těmto subjektům, a tím umožnit sdílení osvědčených postupů souvisejících s anonymizací a veřejně přístupnými údaji. To může být obzvláště důležité pro menší subjekty veřejného sektoru,

[16] Vede-li posouzení k rozhodnutí, že osobní údaje jako takové nebudou zpřístupněny pro opakované použití, nýbrž místo toho budou poskytnuty soubory anonymizovaných údajů odvozených z osobních údajů, je třeba posoudit riziko opětovného identifikování. Viz oddíl VI o anonymizaci a posouzení rizika opětovného identifikování.

[17] Dne 25. ledna 2012 přijala Komise balíček opatření k reformě evropského rámce pro ochranu údajů. Tento balíček opatření zahrnuje i) „sdělení“ (COM(2012) 9 final), ii) „navrhované nařízení o ochraně údajů“ (COM(2012) 11 final), a iii) „navrhovanou směrnici o ochraně údajů“ (COM(2012) 10 final).

[18] Pokud jde o další vodítko k provádění posouzení dopadu na ochranu údajů, viz například internetové stránky projektu PIAF (Privacy Impact Assessment Framework – rámec posuzování dopadů na soukromí pro práva na ochranu údajů a soukromí) na adrese http://www.piafproject.eu/Index.html. PIAF je projekt spolufinancovaný Evropskou komisí, který má EU a její členské státy podnítit k postupnému přijetí politiky posuzování dopadu na soukromí jako prostředku k řešení potřeb a výzev souvisejících se soukromím a zpracováváním osobních údajů. Pokyny existují rovněž v některých členských státech. Viz například příručka k posuzování dopadu na soukromí, kterou vydal komisař pro informace ve Spojeném království, k dispozici na adrese http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment; pokyny k analýze rizik vydané francouzským orgánem pro ochranu údajů, jež byly zmíněny již v poznámce pod čarou č. 12, a pokyny slovinského komisaře pro informace, zejména k „posuzování dopadu na soukromí v projektech elektronické veřejné správy“, k dispozici na adrese https://webmail.europarl.europa.eu/exchweb/bin/redir.asp?URL=https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/PIASmernice__ENG_Lektorirano_10._6._2011.pdf

které nemusí mít potřebné odborné znalosti pro provádění anonymizace, posouzení dopadu na ochranu údajů a posouzení a ověření rizika opětovného identifikování[19].

Posouzení dopadu se důrazně doporučuje rovněž před zavedením nových právních předpisů, které vyžadují zveřejňování osobních údajů.

V. Oblast působnosti směrnice o informacích veřejného sektoru: výjimky z důvodu ochrany osobních údajů

Tento oddíl obsahuje pokyny k oblasti působnosti směrnice o informacích veřejného sektoru, a zejména k výjimkám z důvodu ochrany údajů.

5.1. Použitelnost obecného rámce pro ochranu údajů na opakované použití informací veřejného sektoru

Ve 21. bodě odůvodnění směrnice o informacích veřejného sektoru je uvedeno, že by tato „směrnice měla být provedena a uplatňována v plném souladu se zásadami ochrany osobních údajů". V čl. 1 odst. 4 je stanoveno, že směrnice o informacích veřejného sektoru „ponechává nedotčenu a nijak neovlivňuje úroveň ochrany fyzických osob v souvislosti se zpracováním osobních údajů".

5.2. Výjimky z důvodu ochrany osobních údajů

Směrnice o informacích veřejného sektoru stanoví, že se „tato směrnice se nepoužije na: … dokumenty, které nejsou přístupné podle režimů přístupu v členských státech …"[20].

Směrnice o informacích veřejného sektoru v platném znění stanoví rovněž výjimky z důvodu ochrany údajů. Ustanovení čl. 1 odst. 2 písm. cc) se zabývá těmito třemi situacemi, přičemž všechny tři jsou vyloučeny z oblasti působnosti směrnice:

- dokumenty, k nimž je vyloučen přístup na základě režimů přístupu z důvodu ochrany osobních údajů;
- dokumenty, k nimž je omezen přístup na základě režimů přístupu z důvodu ochrany osobních údajů, a
- „podle těchto režimů přístupné části dokumentů, které obsahují osobní údaje, jejichž opakované použití bylo právně vymezeno jako jednání v rozporu s právními předpisy na ochranu osob v souvislosti se zpracováním osobních údajů".

5.3. Obecné připomínky

Pracovní skupina podle článku 29 zdůrazňuje, že bez ohledu na „zásadu opakovaného použití" stanovenou v novele směrnice není opakované použití ke komerčním či nekomerčním účelům za podmínek stanovených ve směrnici o informacích veřejného sektoru vždy vhodné v případech, kdy informace veřejného sektoru, jež mají být použity opakovaně, obsahují osobní údaje. Rozhodnutí o opakovaném použití osobních údajů za podmínek stanovených ve směrnici o informacích veřejného sektoru bude nutno přijímat v každém jednotlivém případě a je rovněž nutné zavést další právní, technická nebo organizační opatření na ochranu dotčených osob.

---

[19] Ve Spojeném království provozuje například konsorcium vedené Univerzitou v Manchesteru společně s Univerzitou v Southamptonu, Národním statistickým úřadem a novým státním Institutem pro veřejně přístupné údaje (Open Data Institute (ODI)) síť pro anonymizaci – UK Anonymisation Network (UKAN) – s cílem umožnit sdílení osvědčených postupů souvisejících s anonymizací ve veřejném i soukromém sektoru. Síť zahrnuje internetové stránky na adrese https://webmail.europarl.europa.eu/exchweb/bin/redir.asp?URL=http://www.ukanon.net, případové studie, poradnu a semináře.

[20] Viz směrnice o informacích veřejného sektoru, čl. 1 odst. 2 písm. c).

Opakované použití veřejně přístupných osobních údajů je a mělo by být omezeno

- obecnými ustanoveními platných právních předpisů o ochraně údajů,
- (případně) dalšími zvláštními právními omezeními a
- technickými a organizačními ochrannými opatřeními, která byla zavedena na ochranu osobních údajů.

5.4. Dokumenty, k nimž je vyloučen přístup

Toto ustanovení vylučuje z oblasti působnosti směrnice o informacích veřejného sektoru veškeré dokumenty, k nimž je přístup vyloučen na základě režimů přístupu dotčeného členského státu z důvodu ochrany osobních údajů.

Na rozdíl od právních předpisů o ochraně údajů, které jsou do značné míry harmonizovány na základě směrnice 95/46/ES, se právní předpisy o přístupu k informacím mezi jednotlivými členskými státy EU značně liší. Režimy přístupu obvykle vyžadují ověření vyváženosti, při němž se porovnávají zájmy chráněné pravidly týkajícími se soukromí a ochrany údajů s přínosy otevřenosti a transparentnosti. Vzhledem k rozdílům se může výsledek ověření vyváženosti v jednotlivých členských státech EU lišit. Daňové orgány v některých členských státech mohou například zveřejňovat určité části přiznání k dani z příjmů daňových poplatníků (s výhradou právních, technických a organizačních opatření k omezení rizika zneužití na minimum), zatímco jiný členský stát by to pokládal za informace, na něž se vztahuje výjimka a které by měly být obecně považovány za soukromé.

Vnitrostátní právní předpisy musí být v souladu s článkem 8 Evropské úmluvy o lidských právech (dále jen „EÚLP“) a články 7 a 8 Listiny základních práv Evropské unie (dále jen „Listina EU“). To znamená, že jak Evropský soudní dvůr uvedl v rozsudcích ve věci *Österreichischer Rundfunk* a *Schecke*[21], je třeba ověřit, zda je zveřejnění nezbytné a přiměřené legitimnímu cíli sledovanému zákonem.

Je-li přístup k osobním údajům obsaženým v určitém dokumentu vyloučen na základě právních předpisů příslušného členského státu (včetně případů, kdy vnitrostátní právní předpisy o transparentnosti a otevřenosti neumožňují obecnou dostupnost dotyčných osobních údajů), budou tyto údaje každopádně vyloučeny rovněž z oblasti působnosti směrnice o informacích veřejného sektoru.

V zájmu zajištění právní jistoty a transparentnosti vůči subjektům údajů je osvědčeným postupem přijmout pokud možno aktivní přístup a stanovit předem osobní údaje, které mohou být zpřístupněny veřejnosti. Subjekty údajů pak mohou být v době shromažďování údajů informovány, zda určitá část osobních údajů, které poskytují nebo které budou dále zpracovávány během správního řízení, bude veřejně dostupná v důsledku právních předpisů o svobodném přístupu k informacím.

5.5. Dokumenty, k nimž je omezen přístup

Toto ustanovení vylučuje z oblasti působnosti směrnice o informacích veřejného sektoru všechny dokumenty, k nimž je omezen přístup na základě režimů přístupu dotčeného členského státu z důvodu ochrany osobních údajů. Režimy přístupu v jednotlivých členských státech se mohou lišit, pokud jde o to, k jakým údajům může být omezen přístup a jaký druh omezení může existovat. Níže jsou uvedeny některé příklady:

[21] Viz rozsudek ESD ze dne 20. května 2003, Rundfunk, spojené věci C-465/00, C-138/01 a C-139/01, a rozsudek ESD ze dne 9. listopadu 2010, Volker und Markus Schecke, spojené věci C-92/09 a C-93/09.

- sbírky národních archivů, které obsahují osobní údaje, jež jsou přístupné pouze s výhradou zvláštních podmínek přístupu a dodatečných ochranných opatření (viz oddíl IX),
- soubory údajů z výzkumu, které obsahují osobní údaje, jež jsou přístupné pouze s výhradou zvláštních podmínek přístupu a dodatečných ochranných opatření (viz oddíl VIII),
- určité informace ve veřejných registrech, soudních spisech či jiných správních dokumentech, které obsahují osobní údaje, jež mohou být zpřístupněny pouze jednotlivcům nebo organizacím, které prokážou oprávněný zájem nebo pouze s výhradou jiných zvláštních podmínek přístupu a dodatečných ochranných opatření.

5.6. Přístupné části dokumentů, jejichž opakované použití je v rozporu s právními předpisy

Toto ustanovení vylučuje z oblasti působnosti směrnice o informacích veřejného sektoru

- podle vnitrostátních režimů přístupu přístupné
- části dokumentů,
- které obsahují osobní údaje, jejichž „opakované použití bylo právně vymezeno jako jednání v rozporu s právními předpisy na ochranu osob v souvislosti se zpracováním osobních údajů“.

Toto ustanovení potvrzuje, že i v případech, kdy určité dokumenty obsahující osobní údaje jsou zcela přístupné, může být jejich opakované použití omezeno z důvodu ochrany údajů.

Pracovní skupina podle článku 29 zdůrazňuje, že by toto ustanovení ve směrnici o informacích veřejného sektoru mělo být vykládáno v souladu s čl. 1 odst. 4 uvedené směrnice, v němž se uvádí, že tato směrnice „ponechává nedotčenu a nijak neovlivňuje úroveň ochrany fyzických osob v souvislosti se zpracováním osobních údajů“.

Pracovní skupina podle článku 29 by jako osvědčený postup uvítala přijetí zvláštních ustanovení ve vnitrostátních právních předpisech, která jednoznačně popisují, i) jaké údaje jsou veřejně přístupné, ii) za jakým účelem a která iii) případně upřesňují, do jaké míry a za jakých podmínek je přípustné jejich opakované použití. Pokud však nejsou takováto zvláštní ustanovení zavedena, neznamená to, že veřejně přístupné osobní údaje lze vždy opakovaně použít podle směrnice o informacích veřejného sektoru.

V těchto případech právní předpisy o ochraně údajů (uplatňované společně s jinými příslušnými právními předpisy, jako jsou právní předpisy o přístupu k dokumentům) stanoví, zda mohou být v daném případě osobní údaje zpřístupněny pro opakované použití, a pokud ano, s výhradou jakých dodatečných ochranných opatření. Je-li výsledek tohoto posouzení kladný, je opakované použití povoleno s výhradou zvláštních opatření na ochranu údajů a veškerých dalších podmínek stanovených ve směrnici o informacích veřejného sektoru (nejsou-li dotčeny právní předpisy o ochraně údajů). Je-li výsledek posouzení negativní, nebude opakované použití spadat do oblasti působnosti směrnice o informacích veřejného sektoru.

Následující příklady mohou pomoci objasnit, kdy se může použít tato výjimka z oblasti působnosti směrnice o informacích veřejného sektoru. V prvním příkladě jsou omezení vztahující se na opakované použití jednoznačně stanovena v právních předpisech.

- Daňové zákony v určitém členském státě mohou stanovit, že přiznání k dani z příjmů všech rezidentů dané země jsou na žádost veřejně přístupná v prostorách daňových orgánů za účelem kontroly ze strany jakéhokoli jiného rezidenta, aniž by bylo nutné prokázat oprávněný zájem. Zákon rovněž jednoznačně stanoví, že údaje nemohou být dále zpracovávány, například zveřejněny na internetu, spojovány s jinými údaji nebo dále upravovány. Nevládní organizace požádá o přístup a právo použít opakovaně databázi

přiznání k dani za účelem zveřejnění na svých internetových stránkách. V tomto případě nespadají daňové údaje do oblasti působnosti směrnice o informacích veřejného sektoru a subjekt veřejného sektoru nemá povinnost soubor údajů zpřístupnit za účelem opakovaného použití podle směrnice o informacích veřejného sektoru.

V mnoha jiných případech však budou pravděpodobně právní omezení s ohledem na opakované použití vyjádřena méně jednoznačně a méně kategoricky. Různé státní registry, obchodní rejstříky a evidence obyvatel a jiné databáze umožňují veřejnosti nahlížet do osobních údajů, v rostoucí míře v digitální podobě prostřednictvím internetu. Dostupnost často podléhá zvláštním ochranným opatřením, včetně technických omezení funkcí vyhledávání a hromadného stahování. Uživatelé mohou být rovněž požádáni o vyjádření souhlasu s podmínkami přístupu.

- Daňové zákony v určitém členském státě mohou stanovit, že jména rezidentů, kteří mají delší dobu daňové nedoplatky přesahující určitou prahovou hodnotu, jsou po stanovenou dobu zveřejněna na zvláštních internetových stránkách s výhradou dodatečných technických ochranných opatření, včetně omezení hromadného stahování a funkcí vyhledávání. Toto zveřejnění má vybízet k včasnému uhrazení daně z příjmů a u osob, které tak neučiní, sloužit jako dodatečný trest (ve vztahu k pověsti). Konsorcium bank požádá o přístup za účelem opakovaného použití k vložení údajů do systému úvěrových zpráv.
- Zvláštní právní předpisy ve zdravotnictví v určitém členském státě mohou s výhradou ochranných opatření pacientům umožňovat, aby na zvláštních internetových stránkách ověřili, zda byl určitému lékaři či jinému odborníkovi zakázán výkon praxe. Platí technická ochranná opatření, včetně omezení hromadného stahování a funkcí vyhledávání. Organizace pro práva pacientů požádá o přístup za účelem opakovaného použití k vytvoření vícejazyčných a uživatelsky přívětivějších internetových stránek umožňujících přístup k těmto údajům.
- Zvláštní právní předpisy v určitém členském státě mohou vyžadovat zveřejnění jmen dárců politických stran, jejichž dary překročily určitou prahovou hodnotu. Informace, které mohou odhalit politické názory dárců, jsou zveřejněny na zvláštních internetových stránkách. Platí technická ochranná opatření, včetně omezení hromadného stahování a funkcí vyhledávání. Aktivistická skupina požádá o přístup k hromadným údajům za účelem opakovaného použití podle směrnice o informacích veřejného sektoru k vytvoření nových internetových stránek s dodatečnými prvky a lepšími funkcemi vyhledávání.
- Jméno a adresa vlastníka nemovitosti jsou zveřejněny v katastru nemovitostí určitého členského státu, prohledávání veřejně přístupné databáze je však omezeno, aby bylo možné vyhledání pouze konkrétní nemovitosti, a nikoli jednotlivce. Omezeno je rovněž hromadné stahování. Obchodní společnost požádá o přístup k hromadným údajům za účelem jejich opakovaného použití k vytvoření uživatelsky přívětivějších uživatelských internetových stránek za konkurenčnější cenu.
- Obchodní rejstříky v určitém členském státě umožňují veřejnosti přístup k široké škále osobních údajů, včetně jmen, adres a podpisových vzorů ředitelů a informací ohledně vlastnictví určitých typů společností. Existují určitá omezení funkcí vyhledávání a limity pro počet položek, které lze stáhnout. Informace jsou dostupné na zvláštních internetových stránkách a jsou zpoplatněny. Obchodní společnost požádá o přístup k hromadným údajům za účelem jejich opakovaného použití k vytvoření internetových stránek, které spojují informace z několika různých registrů, a nabízení lepších informací za konkurenčnější cenu.

Ve všech případech musí dotyčný subjekt veřejného sektoru provést pečlivé posouzení dopadu na ochranu údajů, aby rozhodl, zda mohou být údaje zpřístupněny pro opakované použití podle směrnice o informacích veřejného sektoru, a pokud ano, zda právní předpisy o ochraně údajů vyžadují nějaké zvláštní podmínky a ochranná opatření. „Zásada opakovaného použití“ není automatická a nemůže převážit nad ustanoveními právních předpisů o ochraně údajů.

Toto pečlivé posouzení je o to důležitější, že podle směrnice o informacích veřejného sektoru nemusí subjekt veřejného sektoru v zásadě uvážit, kdo je konkrétním dalším uživatelem žádajícím o přístup. Podle článku 10 (Nediskriminace) jsou „podmínky opakovaného použití dokumentů nediskriminační pro srovnatelné kategorie opakovaného použití“. Podle článku 11 (Zákaz výhradních dohod) je „opakované použití dokumentů přístupné všem potenciálním účastníkům trhu Smlouvy nebo jiné dohody mezi subjekty veřejného sektoru, které mají dokumenty v držení, a třetími stranami neposkytují výhradní práva.“

Při rozhodování o povolení či nepovolení opakovaného použití proto musí subjekty veřejného sektoru posoudit slučitelnost povolení opakovaného použití na základě veřejné licence nikoli pouze žadateli, nýbrž komukoli, kdo o údaje požádá. To vyžaduje vysokou míru jistoty, že žádný z potenciálních dalších uživatelů nebude moci poskytnuté osobní údaje zneužít.

Směrnice o informacích veřejného sektoru nevylučuje, že podmínky mohou povolit zpracování pouze ke zvláštním účelům. Otázkou, na níž musí subjekt veřejného sektoru odpovědět, je pak to, zda je opakované použití „jakýmkoli potenciálním účastníkem trhu“ pro tyto účely slučitelné s účely stanovenými subjektem veřejného sektoru. Relevantní je potenciální opakované použití informací o placení daní ze strany finančních institucí například pro účely úvěrových zpráv, jelikož tyto instituce jsou potenciálním dalším uživatelem na základě kritéria „jakákoli osoba“. K vyřešení otázek ochrany údajů, a zejména k zajištění toho, že je dodržena zásada omezení účelu, musí mít subjekt veřejného sektoru (nebo zákonodárce) možnost účely opakovaného použití případně omezit.

VI. Opakované použití souborů agregovaných a anonymizovaných údajů odvozených z osobních údajů

6.1. Jaké jsou výhody agregace a anonymizace při opakovaném použití informací veřejného sektoru?

Až doposud usilovaly iniciativy týkající se opakovaného použití informací veřejného sektoru, které subjekty veřejného sektoru zahájily prostřednictvím „portálů veřejně přístupných údajů“ či jiných platforem, obvykle o zpřístupnění agregovaných a anonymizovaných údajů pro opakované použití místo osobních údajů jako takových. Tento přístup je skutečně bezpečnější a je třeba jej prosazovat.

Právní předpisy o ochraně údajů obvykle neumožňují, aby subjekty veřejného sektoru zveřejnily osobní údaje shromážděné pro jiný, zpravidla administrativní, účel[22]. V těchto případech není tudíž jejich opakované použití v rámci iniciativ týkajících se opakovaného použití informací veřejného sektoru možné. Pro opakované použití jsou a měly by být zpřístupněny – v zásadě – obvykle statistické údaje odvozené z osobních údajů místo osobních údajů. To je nejúčinnější řešení k minimalizaci rizika neúmyslného zveřejnění osobních údajů. Tyto soubory anonymizovaných a agregovaných údajů by neměly umožnit opětovné identifikování jednotlivců, a neměly by tudíž obsahovat osobní údaje.

Rozhodnutí, na jaké úrovni může být agregace vhodná a jaké zvláštní techniky anonymizace použít, je složitý úkol. Není-li agregace a anonymizace provedena účinně, hrozí, že jednotlivci mohou být z těchto souborů údajů zpětně identifikováni. Důležitou úlohu proto musí hrát právní předpisy o ochraně údajů, které napomáhají při stanovení limitu pro „bezpečné“ zveřejnění anonymizovaných a agregovaných údajů v rámci iniciativy týkající se informací veřejného sektoru.

Směrnice 95/46/ES stanoví vysokou úroveň limitu pro anonymizaci

Při použití v tomto dokumentu se výraz „anonymizace“ vztahuje na údaje, které již nelze považovat za osobní údaje podle čl. 2 písm. a) směrnice 95/46/ES. V čl. 2 písm. a) jsou „osobní údaje“ vymezeny jako „veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů)“. Identifikovatelnou osobou je „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“[23].

Důležitý je rovněž 26. bod odůvodnění směrnice 95/46/ES, který stanoví, 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“.

Je třeba zdůraznit, že to stanoví vysoký limit, jak bude projednáno dále v tomto stanovisku. Nelze-li údaje anonymizovat, aby splňovaly tento limit, platí i nadále právní předpisy o ochraně údajů. To mimo jiné znamená, že není-li dosaženo limitu, musí být zveřejnění informací (a případné další použití) „slučitelné“ s původními účely sběru údajů podle čl. 6 odst. 1 písm. b) směrnice 95/46/ES. Musí existovat rovněž odpovídající právní základ pro zpracování podle čl. 7 písm. a) až f) směrnice 95/46/ES (například souhlas, nezbytnost kvůli dodržení právních předpisů). Naopak v případě,

[22] Právní předpisy o svobodném přístupu k informacím mohou případně vyžadovat zveřejnění osobních údajů a zájem týkající se transparentnosti a dostupnosti informací může v některých případech převážit nad obavami ohledně ochrany údajů a soukromí. Jedná se o vyvíjející se oblast, která může v budoucnu přinést změny.

[23] Ve svém prohlášení ze dne 27. února 2013 ke „stávající diskusi o balíčku opatření pro reformu ochrany údajů“ pracovní skupina podle článku 29 zdůraznila, že „fyzickou osobu lze považovat za identifikovatelnou, pokud ji lze ve skupině osob odlišit od ostatních, a tudíž s ní zacházet odlišně. To znamená, že pojem identifikovatelnost zahrnuje vyčlenění“. Prohlášení rovněž objasňuje, že by se „za osobní údaje měly považovat identifikační čísla, lokalizační údaje, IP adresy, elektronické identifikátory nebo jiné specifické prvky vztahující se na jednotlivce“.

byly-li údaje anonymizovány ve smyslu čl. 2 písm. a) a 26. bodu odůvodnění směrnice 95/46/ES, pravidla pro ochranu údajů se již nepoužijí a další uživatelé mohou údaje použít bez omezení.

Opět je třeba zdůraznit, že se pojem „anonymizované údaje“, jak je použit v tomto stanovisku, vztahuje na údaje, které již nelze pokládat za osobní údaje. Anonymizované údaje je třeba odlišovat zejména od údajů, s nimiž bylo pomocí různých technik manipulováno za účelem zmírnění rizika opětovného identifikování dotyčných jednotlivců, nebylo však dosaženo limitu vyžadovaného v čl. 2 písm. a) a ve 26. bodě odůvodnění směrnice 95/46/ES[24]. V mnoha případech jsou tyto techniky vhodné pouze k omezenému zveřejnění pro opakované použití prověřenými třetími stranami, nikoli však pro úplné zpřístupnění veřejnosti a opakované použití na základě veřejné licence.

Je rovněž důležité zdůraznit, že jakmile jsou údaje zpřístupněny veřejnosti pro opakované použití, nebude existovat žádná kontrola nad tím, kdo může k údajům získat přístup. Velmi významně se zvýší pravděpodobnost, že „jakákoli jiná osoba“ bude mít prostředky k opětovnému identifikování subjektů údajů a že je použije. Bez ohledu na výklad 26. bodu odůvodnění v jiných souvislostech si proto pracovní skupina podle článku 29 přeje, aby bylo naprosto jasné, že pokud jde o zpřístupnění údajů pro opakované použití podle směrnice o informacích veřejného sektoru, je třeba se všemožně vynasnažit, aby bylo zajištěno, že soubory údajů, které mají být zveřejněny, neobsahují údaje, jež lze opětovně identifikovat prostředky, které mohou být rozumně použity jakoukoli jinou osobou, včetně potenciálních dalších uživatelů, avšak rovněž jiných stran, jež mohou mít zájem na získání údajů, včetně prosazování práva.

Další pokyny k anonymizaci a pojmu osobní údaje

Pokud jde o další pokyny k anonymizaci a pojmu osobní údaje, viz stanovisko pracovní skupiny podle článku 29 č. 4/2007 k pojmu osobní údaje, které bylo přijato dne 20. června 2007 (WP 136). Ve druhém pololetí roku 2013 může pracovní skupina podle článku 29 vydat další pokyny k technikám anonymizace rovněž ve zvláštním dokumentu.

6.2. Jaké jsou problémy a meze anonymizace při opakovaném použití informací veřejného sektoru?

Dosažení anonymizace je stále obtížnější vzhledem k rozvoji moderní počítačové techniky a všudypřítomné dostupnosti informací. Opětovné identifikování jednotlivců představuje stále běžnější a existující hrozbu[25]. V praxi existuje velmi významná šedá zóna, kde se správce údajů, který údaje zveřejňuje, může domnívat, že údaje jsou anonymizovány, třetí strana však může být přesto schopna identifikovat z těchto údajů přinejmenším některé jednotlivce, například pomocí jiných veřejně dostupných informací nebo dalších údajů, které má k dispozici.

Jedním z důležitých rizikových faktorů je rostoucí množství on-line a off-line údajů, a to jak veřejně dostupných, tak i soustředěných v rukou podnikových organizací, které lze poté použít k vytváření profilů jednotlivců pro účely behaviorální reklamy a stále větší škálu jiných účelů. Při porovnání s „hromadnými údaji“, které již mají tyto organizace k dispozici, by informace veřejného sektoru

[24] V prohlášení ze dne 27. února 2013 je zdůrazněno, že „je-li možné jednotlivce zpětně vysledovat nebo jej (nepřímo) identifikovat pomocí jiných prostředků, platí i nadále pravidla ochrany údajů“.

[25] Viz například zpráva s názvem „Transparent Government, Not transparent Citizens“, kterou pro úřad vlády Spojeného království v roce 2011 vypracoval Kieron O'Hara z Univerzity v Southamptonu a v níž autor upozorňuje na možnost identifikace jednotlivců z anonymizovaných údajů mimo jiné pomocí „mozaiky dat“ a uvádí, že k vyřešení problému deanonymizace neexistují dokonalá technická řešení. K dispozici na adrese: http://www.cabinetoffice.gov.uk/sites/default/files/resources/transparency-and-privacy-review-annex-b.pdf. Viz rovněž dokument „Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization“ vyhotovený Paulem Ohmem z Právnické fakulty Univerzity v Coloradu, 57 UCLA Law Review 1701 (2010), k dispozici na adrese http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

odvozené z osobních údajů a zpřístupněné pro opakované použití mohly zvýšit pravděpodobnost toho, že jednotlivci mohou být identifikováni nebo že lze dále obohacovat jejich profily, často bez jejich vědomí.

6.3. Kdo by měl provádět agregaci a anonymizaci a kdy?

K agregaci a anonymizaci by mělo dojít co nejdříve a měl by je provést správce údajů nebo pověřená třetí strana, která jedná jménem správce nebo několika správců (a která má rovněž potřebné specializované dovednosti). Anonymizaci nelze ponechat na dalším uživateli, například jako licenční podmínku. Dále je důležité zajistit, aby u případné třetí organizace, která provádí agregaci a anonymizaci, neexistoval střet zájmů a aby byla tato organizace jednoznačně odpovědná za to, že osobní údaje budou použity pouze k provedení anonymizace a že za tímto účelem jsou zavedena veškerá nezbytná ochranná opatření. Třetí strana by měla být rovněž schopna zaručit, že osobní údaje, z nichž jsou odvozeny soubory agregovaných a anonymizovaných údajů, jsou vymazány, jakmile již nejsou k tomuto účelu zapotřebí.

6.4. Posouzení rizika opětovného identifikování

Pokud nelze údaje anonymizovat ve smyslu čl. 2 písm. a) a 26. bodu odůvodnění směrnice 95/46/ES, platí i nadále právní předpisy o ochraně údajů.

Správci by měli posoudit, zda lze jednotlivce přiměřeně identifikovat ze souboru „anonymizovaných“ údajů, které mají být zpřístupněny pro opakované použití, a z jiných informací. Jinými slovy, zda organizace nebo jednotlivec může identifikovat jakoukoli osobu z údajů, které jsou zveřejněny – buď samotných, nebo ve spojení s dalšími dostupnými informacemi.

Jak je objasněno v bodě 6.1, cílem tohoto stanoviska není poskytnout zevrubné a definitivní pokyny k posuzování rizika opětovného identifikování. Jeho cílem není ani stanovit konečnou definici „anonymizace“ nebo „anonymizovaných údajů“. Znovu se však zdůrazňuje, že čtenář může nalézt další pokyny v existujících dokumentech (včetně těch, které jsou uvedeny v bodě 6.1), a že probíhá rovněž práce v technologické podskupině pracovní skupiny podle článku 29 pro techniky anonymizace, jak je uvedeno v bodě 6.1 a bodě 2.2.

Aniž by pracovní skupina podle článku 29 usilovala o úplnost, chce vyzdvihnout některé faktory/pojmy, které je užitečné uvážit při posuzování rizika opětovného identifikování, zejména včetně tohoto:

- jaké jiné údaje jsou k dispozici, buď široké veřejnosti, či jiným osobám nebo organizacím, a zda by údaje, které mají být zveřejněny, mohly být propojeny s jinými soubory údajů,
- pravděpodobnost pokusu o opětovné identifikování (některé druhy údajů budou pro potenciální útočníky přitažlivější než jiné) a
- pravděpodobnost toho, že opětovné identifikování bude v případě pokusu úspěšné, s ohledem na účinnost navrhovaných technik anonymizace[26].

Jaké „jiné“ informace jsou k dispozici?

Při určování, zda by jednotlivec mohl být identifikován nepřímo, je třeba uvážit, zda je identifikace možná s použitím dotyčných údajů (v našem případě souboru „anonymizovaných“ údajů), nebo těchto údajů a *jiných informací*, které má organizace či jednotlivec pokoušející se o opětovné identifikování k dispozici nebo které možná/pravděpodobně získá.

[26] Pokud jde o techniky anonymizace, viz připravované stanovisko pracovní skupiny podle článku 29 k tomuto tématu.

„Jinými informacemi“ potřebnými pro opětovné identifikování by mohly být informace, které mají k dispozici určité podniky nebo jiné organizace, včetně donucovacích orgánů či jiných subjektů veřejného sektoru, určití jednotlivci nebo kdokoli, jelikož byly například zveřejněny na internetu. Zjevným příkladem je případ, kdy veřejně přístupné údaje (např. seznam voličů, telefonní seznam nebo jiné údaje, které lze snadno získat vyhledáním na internetu) mohou být propojeny s (nedostatečně) „anonymizovanými“ údaji, což umožní identifikaci jednotlivce (např. pomocí jeho data narození a PSČ).

Riziko opětovného identifikování se může zvýšit, pokud jednotlivec nebo skupina jednotlivců již toho hodně ví o jiném jednotlivci, například rodinném příslušníkovi, kolegovi, kontaktu na sociální síti, lékaři, učiteli, představiteli donucovacích orgánů či jiném odborníkovi.

Nezáleží však na tom, zda může jednotlivec s předchozími znalostmi identifikovat dotyčný subjekt údajů, nýbrž na tom, zda se z informací, které získal prostřednictvím opětovného identifikování, doví něco nového. Význam tohoto rozdílu objasní dva níže uvedené příklady.

První příklad: statistické údaje o spalničkách. V jednom případě mohou anonymizované statistické údaje odhalit, že se v městě A v roce 2012 nakazilo X lidí spalničkami. Není uvedeno žádné další rozčlenění ani informace. Lékař, který ke statistice přispěl tím, že příslušným zdravotnickým orgánům poskytl údaje o svých pacientech, má ve své ordinaci o těchto pacientech úplnější záznamy, na něž se vztahuje lékařské tajemství. Lékař by mohl ze souboru statistických údajů snadno opětovně identifikovat řadu pacientů. Obdobně by mohla matka, která ví, že její dítě v daném roce onemocnělo spalničkami, v souboru údajů snadno opětovně identifikovat své dítě. Matka ani lékař se však ze souboru anonymizovaných údajů, které byly zpřístupněny veřejnosti, nedozví nic, co by již nevěděli předtím.

Druhý příklad: zneužívání drog a alkoholu, sexuální zneužívání a školní výsledky. Uvedený příklad lze porovnat s následujícím příkladem. Je proveden výzkum souvislostí mezi zneužíváním drog a alkoholu u rodičů, sexuálním zneužíváním dětí a školními výsledky. Údajně „anonymizované“ údaje z výzkumu jsou zveřejněny s dobrými úmysly, avšak bez pečlivého posouzení rizika opětovného identifikování.

Statistika mimo jiné odhalí, že ve škole A, na níž je zapsáno celkem 500 žáků, v roce 2012 žilo 20 % žáků (100 žáků) v domácnosti, v níž je nejméně jeden rodič alkoholikem nebo drogově závislým. Z těchto žáků bylo v 8 % případů (8 žáků) dítě sexuálně zneužíváno. Zpráva rovněž upřesňuje, že žádní jiní žáci ve škole A nebyli sexuálně zneužíváni.

Údaje rovněž ukazují, že v 96 % případů (96 žáků) měly děti, jejichž rodiče byli alkoholici nebo drogově závislí, značné problémy s učením („neprospívající žáci“ podle příslušné akademické normy), v této konkrétní škole však mělo značné problémy s učením pouze 50 % sexuálně zneužívaných dětí (4 žáci).

Ve škole je všeobecně známo, že žák AA, chytrý a pracovitý chlapec, pochází z problematické rodiny a že jeho matka je alkoholička. Některými svými spolužáky je často šikanován. Tito spolužáci nyní ze statistických údajů zveřejněných ve školním časopise zjistí, že AA musí patřit k 50 % sexuálně zneužívaných dětí, které nemají s učením problémy („dobří žáci“). Ze souboru nedostatečně anonymizovaných údajů se tudíž dozví nové (a v tomto případě velmi citlivé) informace.

Riziko spojování informací za účelem získání osobních údajů se zvyšuje s tím, jak se vyvíjejí techniky propojování dat a roste výpočetní kapacita a s tím, jak se potenciálně „porovnatelné“ údaje stávají veřejně dostupnými. Výpočetní kapacita se každý rok zdvojnásobí a uchovávání údajů (rovněž kvůli dostupnosti služeb cloud computingu) se pravděpodobně stane komoditou. Riziko

opětovného identifikování prostřednictvím propojení dat je proto nepředvídatelné, jelikož nikdy nelze s jistotou posoudit, jaké údaje již jsou dostupné nebo jaké údaje mohou být zveřejněny v budoucnu.

Navzdory veškeré nejistotě lze riziko opětovného identifikování obvykle přinejmenším do jisté míry snížit dodržením zásady minimalizace údajů, tj. zajištěním, aby byly zveřejněny pouze údaje, které jsou nezbytné pro určitý konkrétní účel.

Pravděpodobnost úspěšného pokusu o opětovné identifikování: kritérium „motivovaného útočníka"

Kritérium „motivovaného útočníka" je nový pojem, který musí být ještě plně ověřen. Toto kritérium může být užitečné při určování, zda:

- by měl někdo motivaci provést opětovné identifikování a
- zda bude opětovné identifikování možná/pravděpodobně úspěšné.

Kritérium motivovaného útočníka v zásadě zahrnuje uvážení, zda by „útočník" byl schopen dosáhnout opětovného identifikování, *pokud* by měl motivaci, aby se o to pokusil. „Motivovaným útočníkem" je osoba (jednotlivec nebo organizace), která chce identifikovat jednotlivce, z jehož osobních údajů byly odvozeny anonymizované údaje. Toto kritérium má posoudit, zda by byl motivovaný útočník úspěšný. Tento přístup předpokládá, že „motivovaný útočník" je kompetentní a že má přístup ke zdrojům úměrně motivaci, kterou může mít k zpětnému identifikování.

Některé druhy údajů budou pro „motivovaného útočníka" přitažlivější než jiné. Útočník může být například obecně motivovanější k opětovnému identifikování osobních údajů, pokud tyto údaje:

- mají značnou obchodní hodnotu (včetně na černém trhu nebo mimo Evropskou unii), a lze je proto prodat a koupit za účelem dosažení finančního zisku[27],
- lze použít pro účely prosazování práva nebo pro zpravodajské účely,
- odhalují informace o veřejných osobnostech, které jsou zajímavé pro tisk,
- lze je použít pro politické nebo aktivistické účely (např. v rámci kampaně proti určité organizaci nebo osobě),
- mohly by být použity z osobních důvodů ve zlém úmyslu (např. stalking, obtěžování, šikana nebo pouze uvedení jiných osob do rozpaků),
- mohou vyvolávat zvědavost (např. místní osoba chce zjistit, kdo se podílel na incidentu uvedeném v kriminální mapě).

Ačkoli je užitečné přemýšlet o případné motivaci potenciálních útočníků, pracovní skupina podle článku 29 zdůrazňuje, že tento přístup má také značná omezení:

- Hodnocení může být do jisté míry spekulativní.
- V případě neexistence zjevných „motivačních faktorů", jaké byly například popsány výše, může hodnocení vést k falešnému ujištění a může naznačovat, že osobní údaje, které jsou relativně neškodné, mohou být zpřístupněny pro opakované použití bez účinné anonymizace.
- Útočníci mohou být důmyslní, inovativní a „o krok napřed" a najít použití opětovně identifikovaných údajů, která nejsou pro ostatní zjevná.

[27] To může zahrnovat například údaje o transakcích nebo jiné údaje o chování, z nichž je možné odvodit profily jednotlivých spotřebitelů, jež lze poté použít k reklamním účelům nebo cenové diskriminaci; finanční nebo jiné informace, které umožňují krádež identity; citlivé údaje, které mohou být použity k vydírání jednotlivců nebo k jejich diskriminaci; zdravotní údaje, jež mohou použít například pojišťovny k odmítnutí pojištění z důvodu zdravotního stavu; informace umožňující odvození údajů o úvěruschopnosti, jež by mohly být použity k posouzení úvěrových rizik atd.

- S rostoucí tendencí k analýze „hromadných údajů“ existuje větší nebezpečí, že v případě opětovného identifikování mohou zdánlivě neškodné údaje po spojení s jinými informacemi představovat závažnější rizika.

6.5. Ověření opětovného identifikování

V některých případech může být obtížné zjistit riziko opětovného identifikování, zejména v případech, kdy třetí strana může k porovnávání různých anonymizovaných údajů používat složité statistické metody. V rámci celkového posouzení k zjištění rizika opětovného identifikování je proto osvědčeným postupem ověření opětovného identifikování – ověření „proniknutí“ – s cílem odhalit náchylnost k opětovnému identifikování a odstranit ji. To spočívá v pokusu o opětovné identifikování jednotlivců ze souborů údajů, které mají být zveřejněny.

První fází procesu ověření opětovného identifikování by mělo být posouzení souboru údajů, které subjekt veřejného sektoru zveřejnil nebo které zamýšlí zveřejnit. Druhou fází by měla být snaha určit dostupnost jiných údajů (osobních údajů či jiných informací), jež by mohly být spojeny s dotyčnými údaji za účelem opětovného identifikování. Cílené „ověření proniknutí“ by mělo zejména pomoci posoudit, jaká jsou rizika identifikace pomocí mozaiky dat, tj. sestavení různých jednotek informací za účelem získání úplnější představy o určité osobě.

Ověření opětovného identifikování by se samozřejmě nemělo pokládat za všelék a nemělo by vést k falešnému pocitu bezpečí. Ověření může být za prvé obtížně proveditelné, jelikož často vyžaduje značné technické odborné znalosti a odpovídající nástroje a rovněž povědomí o tom, jaké jiné údaje mohou být dostupné. Správci údajů si musí být za druhé vědomi také toho, že se riziko opětovného identifikování může v průběhu času měnit. Nyní jsou například k dispozici stále výkonnější a cenově dostupnější techniky a nástroje pro analýzu dat a vzájemné srovnání s jinými soubory údajů se stává stále jednodušším, jelikož je vytvářeno stále více údajů. Organizace by proto měly provádět pravidelný přezkum své politiky v oblasti zveřejňování údajů a technik používaných k anonymizaci údajů. Rozhodnutí by navíc neměla být nikdy založena pouze na stávajících hrozbách, nýbrž rovněž na předvídatelných budoucích hrozbách.

Jakmile bylo s ohledem na riziko opětovného identifikování provedeno posouzení podle bodu 6.4 a v případě potřeby ověření opětovného identifikování, může subjekt veřejného sektoru stanovit, zda lze soubory údajů považovat za anonymizované, či nikoli, jinými slovy, zda již neobsahují žádné osobní údaje ve smyslu čl. 2 písm. a) a 26. bodu odůvodnění směrnice 95/46/ES. Je-li tomu tak, lze soubor údajů zveřejnit bez jakýchkoli omezení týkajících se ochrany údajů[28]. Je-li na druhou stranu ověření úspěšné, tyto údaje nesmí (nebo již nesmí) být zpřístupněny jako anonymizované údaje, nýbrž musí být pokládány za osobní údaje (a jejich zveřejnění není tudíž možné, nebo může být možné pouze s výhradou požadavků projednaných v oddíle VII).

6.6. Zrušení ohrožených souborů údajů

V případě prokázaného opětovného identifikování údajů ze souboru veřejně přístupných údajů musí být subjekt veřejného sektoru, který soubor údajů poskytl, schopen zastavit přísun dat nebo odstranit soubor údajů z internetových stránek s veřejně přístupnými údaji. V případě odstranění souboru údajů z internetových stránek musí subjekt veřejného sektoru informovat rovněž další uživatele a vyzvat je, aby ukončili zpracovávání a vymazali veškeré údaje pocházející z ohroženého souboru údajů. Jelikož informování všech dalších uživatelů bude v případě režimu veřejné licence, který vyžaduje směrnice o informacích veřejného sektoru, obtížné, musí veřejné subjekty učinit přiměřeně účinné kroky k vyřešení této záležitosti. Ačkoli zrušení může často představovat příliš

[28] Viz však bod 10.3 o „licenčních podmínkách v případě souborů anonymizovaných údajů“, zejména pokud jde o potřebu zavést ochranná opatření s cílem pomoci i nadále zajistit, aby jednotlivci nebyli opětovně identifikováni.

pozdní opatření, než aby se předešlo škodám, je to nezbytný krok, který pomáhá zmírnit případné nepříznivé dopady na subjekty údajů.

VII. Zpřístupnění osobních údajů pro opakované použití

7.1. Příklady veřejně přístupných osobních údajů, které zveřejnily subjekty veřejného sektoru

Ačkoli obvyklým scénářem v případě iniciativ týkajících se opakovaného použití informací veřejného sektoru je zpřístupnění souborů anonymizovaných údajů, v některých případech mohou subjekty veřejného sektoru zpřístupnit pro opakované použití rovněž osobní údaje.

Mnoho veřejně přístupných registrů, například katastry nemovitostí nebo obchodní rejstříky, obsahuje velké množství osobních údajů a tyto registry jsou vzhledem k iniciativám v oblasti elektronické veřejné správy v rostoucí míře dostupné rovněž on-line. Existuje mnoho dalších příkladů, kdy zákonodárci v určitých členských státech stanovili právní základ pro zpřístupňování osobních údajů fyzických osob na internetu nebo na základě žádosti o přístup k dokumentům. K nim mohou patřit například tyto údaje[29]:

- výdaje, platy nebo prohlášení o střetu zájmů vydaná určitými státními zaměstnanci nebo příjemci státní podpory (např. zemědělské dotace),
- názvy organizací nebo jména jednotlivců věnujících dary politickým stranám,
- přiznání k dani podaná fyzickými osobami[30],
- soudní rozhodnutí (se jmény stran či jiných osob, která jsou někdy vymazána nebo nahrazena iniciálami s cílem snížit riziko opětovného identifikování),
- seznamy voličů,
- seznamy vypracovávané soudy (tj. soupisy případů, které budou v určitých dnech projednávány u soudu).

V každém z těchto případů mohou subjekty veřejného sektoru nebo zákonodárci aktivně uvážit, zda chtějí tyto údaje zpřístupnit pro opakované použití (např. k zlepšení veřejných služeb, jako je poskytování přístupu k obchodním rejstříkům nebo katastrům nemovitostí). Na subjekty veřejného sektoru se mohou také obrátit potenciální další uživatelé, kteří požadují opakované použití údajů. V některých jiných případech je rovněž možné, že potenciální další uživatelé jednoduše vezmou osobní údaje, které již jsou dostupné na internetu, a použijí je, aniž by nutně kontaktovali subjekt veřejného sektoru, který informace zveřejnil. Ve všech třech případech musí další uživatelé při nakládání s osobními údaji samozřejmě dodržovat právní předpisy o ochraně údajů.

7.2. Rozdíly ve vnitrostátních režimech přístupu

Zákonné povinnosti týkající se zpřístupňování určitých osobních údajů se mezi jednotlivými členskými státy kvůli rozdílným právním a kulturním tradicím značně liší. V některých členských státech existuje právní základ pro zpřístupňování určitých osobních údajů, zatímco v jiných členských státech by ve stejné situaci bylo zveřejnění týchž osobních údajů zakázáno. Směrnice o informacích veřejného sektoru uznává a objasňuje, že vychází ze stávajících režimů přístupu v členských státech a nemění vnitrostátní pravidla vztahující se na přístup k dokumentům[31].

7.3. Potřeba posouzení dopadu na ochranu údajů a vhodných ochranných opatření

[29] Viz rovněž příklady uvedené v oddíle V při projednávání oblasti působnosti směrnice o informacích veřejného sektoru.

[30] Viz např. rozsudek Evropského soudního dvora ze dne 16. prosince 2008 ve věci Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy en Satamedia Oy, C-73/07.

[31] Jak bylo uvedeno v bodě 5.4, vnitrostátní právní předpisy musí být v souladu s článkem 8 EÚLP a články 7 a 8 Listiny EU, jak je vykládá příslušná judikatura.

Pokud se zvažuje zpřístupnění osobních údajů pro opakované použití, je zpravidla naprosto nezbytný obezřetný přístup. Pracovní skupina podle článku 29 zejména doporučuje, aby před zveřejněním souboru údajů (nebo před přijetím zákona, který vyžaduje zveřejnění) bylo provedeno důkladné posouzení dopadu na ochranu údajů, které hodnotí rovněž možnosti a potenciální dopad opakovaného použití. Obecně je třeba zamezit zpřístupnění osobních údajů pro opakované použití na základě veřejné licence bez jakýchkoli technických a právních omezení vztahujících na opakované použití.

7.4. Význam režimu licencí

Pracovní skupina podle článku 29 navíc doporučuje zavedení přísného režimu licencí, který musí být rovněž náležitě prosazován, aby bylo zajištěno, že osobní údaje nebudou použity k neslučitelným účelům – například k nevyžádaným obchodním sdělením či jinak, a to způsobem, který subjekty údajů považují za neočekávaný, nepřiměřený či jinak problematický.

7.5. Význam pevného právního základu pro zveřejňování i pro opakované použití

Pracovní skupina podle článku 29 znovu zdůrazňuje význam stanovení pevného právního základu pro zpřístupňování osobních údajů s přihlédnutím k příslušným pravidlům ochrany údajů, včetně zásady proporcionality, minimalizace údajů a omezení účelu.

Pracovní skupina podle článku 29 doporučuje, aby případné právní předpisy, které vyžadují veřejný přístup k údajům, jednoznačně upřesňovaly účel zveřejnění osobních údajů. Není-li toto stanoveno, nebo je-li to stanoveno pouze neurčitě a obecně, bude to na úkor právní jistoty a předvídatelnosti. Zejména co se týká žádostí o opakované použití, pro dotčený subjekt veřejného sektoru a potenciální další uživatele bude velmi obtížné určit, jaký byl zamýšlený původní účel zveřejnění, a tudíž jaké další účely budou slučitelné s těmito původními účely. Jak již bylo uvedeno, i v případě zveřejnění osobních údajů na internetu nelze předpokládat, že je lze dále zpracovávat pro jakékoli účely.

Jakékoli další opakované použití musí mít v těchto případech odpovídající právní základ (např. souhlas nebo požadavek právních předpisů) podle čl. 7 písm. a) až f) směrnice 95/46/ES a dodržovat všechny ostatní zásady ochrany údajů.

7.6. Omezení účelu

V případě opakovaného použití informací veřejného sektoru je účinné uplatňování zásady omezení účelu problematické. Na straně jedné je myšlenkou a hybnou silou inovací, z nichž vychází koncepce „veřejně přístupných údajů“ a opakovaného použití informací veřejného sektoru, skutečnost, že by informace měly být zpřístupněny pro opakované použití pro inovativní nové produkty a služby, a tudíž pro účely, které nejsou předem stanoveny a nelze je jednoznačně předvídat. Směrnice o informacích veřejného sektoru rovněž požaduje, aby opakované použití zbytečně neomezovaly licence.

Omezení účelu představuje na druhou stranu hlavní zásadu ochrany údajů a vyžaduje, aby osobní údaje shromážděné pro konkrétní účel nebyly dále používány k jiným neslučitelným účelům[32]. Tato zásada se stejně tak vztahuje na osobní údaje, které jsou veřejně přístupné. Samotná skutečnost, že osobní údaje jsou veřejně přístupné pro určitý konkrétní účel, neznamená, že tyto osobní údaje jsou přístupné pro opakované použití pro jakékoli jiné účely.

Výdaje vyšších státních úředníků jsou například zpřístupněny na internetu s cílem zajistit transparentnost, umožňují však opakované použití ze strany kterékoli občana pro jiné účely, jež nemusí být slučitelné.

Jak je projednáno podrobněji ve stanovisku pracovní skupiny podle článku 29 č. 3/2013 k omezení účelu (viz oddíl III bod 2.2 a příloha 1), posouzení, zda je další zpracovávání osobních údajů slučitelné s účely, pro něž byly tyto údaje shromážděny, vyžaduje posouzení více faktorů. V úvahu je třeba vzít zejména:

a) vztah mezi účely, pro něž byly osobní údaje shromážděny, a účely dalšího zpracovávání;
b) kontext sběru osobních údajů a přiměřená očekávání subjektů údajů ohledně jejich dalšího použití;
c) povahu osobních údajů a dopad dalšího zpracování na subjekty údajů;
d) ochranná opatření, která správce přijal s cílem zajistit korektní zpracování a zamezit případnému nepatřičnému dopadu na subjekty údajů.

Tyto klíčové faktory je třeba posoudit při rozhodování o zveřejnění osobních údajů a rovněž v každém případě, kdy budou osobní údaje použity opakovaně. Níže jsou uvedeny některé příklady:

- Subjekt veřejného sektoru zveřejní v adresáři kontaktní údaje, včetně jména, titulu, pracovní adresy a telefonního čísla svých zaměstnanců. Zjevným (ačkoli nikoli výslovně uvedeným) účelem tohoto adresáře je pomoci veřejnosti určit osobu, na niž je třeba se obrátit s oficiálními dotazy a jinými úředními záležitostmi. Další uživatel chce získat obsah tohoto adresáře a spojit údaje s domácími adresami a telefonními čísly zaměstnanců (pokud jsou veřejně přístupné, například v telefonním seznamu) a poskytnout domácí i pracovní adresy a čísla telefonů na interaktivní mapě s cílem ukázat, kde jednotliví státní zaměstnanci žijí a pracují. Toto spojení a opakované použití údajů je nutno považovat za neslučitelné s původním účelem. Státní zaměstnanec, jehož pracovní kontaktní údaje jsou zveřejněny, aby se na něj mohla obracet veřejnost, nebude přiměřeně očekávat, že tyto informace budou poté vztaženy k jiným údajům, jež zveřejnil k jinému účelu nesouvisejícímu s prací.
- V některých členských státech jsou podle vnitrostátních právních předpisů oznámení o plánovaném sňatku veřejná a může do nich nahlížet kdokoli. Cílem tohoto zveřejnění je oznámit vůli snoubenců uzavřít manželství a umožnit zainteresovaným stranám, aby podaly námitku. Skutečnost, že osobní údaje obsažené ve zveřejněných svatebních oznámeních jsou

[32] Pouze výjimečně – s výhradou přísných ochranných opatření podle článku 13 směrnice 95/46/ES – lze údaje použít způsobem, který není v souladu s účely stanovenými při jejich sběru. Viz oddíl III bod 3 stanoviska pracovní skupiny podle článku 29 č. 3/2013 k omezení účelu.

dostupné komukoli, však třetím stranám neumožňuje tyto informace využít k zasílání obchodních sdělení dotyčným párům. Toto další použití by nebylo slučitelné vzhledem k cíli zveřejnění svatebního oznámení, kterým je umožnit vznést vůči sňatku námitku, jak je stanoveno v právních předpisech.

7.7. Komerční a nekomerční účely

Stanovisko č. 7/2003 vyzdvihuje komerční činnosti jako hlavní pobídku k opakovanému použití informací veřejného sektoru na rozdíl od přístupu k informacím, kdy je účelem právních předpisů o svobodném přístupu k informacím zajištění transparentnosti, otevřenosti a odpovědnosti vůči občanům.

Stanovisko č. 7/2003 rovněž zdůrazňuje, že „[občané] obvykle používají informace pro vlastní, nekomerční účely“. Toto prohlášení je třeba aktualizovat vzhledem ke zkušenostem, jež byly mezitím s opakovaným použitím informací veřejného sektoru získány. Zkušenosti s iniciativami týkajícími se veřejně přístupných údajů ukazují, že opakované použití informací veřejného sektoru může významně přispět rovněž k zvýšení transparentnosti a odpovědnosti a může vést k lepšímu využívání veřejných služeb. Rozlišování mezi opakovaným použitím pro komerční nebo nekomerční účely by při zvažování slučitelnosti dalšího použití osobních údajů nemělo být rozhodující. Posouzení slučitelnosti by nemělo být založeno v prvé řadě na tom, zda je ekonomický model potenciálního dalšího uživatele ziskový či neziskový.

Je třeba pečlivě posoudit, zda jsou účely a způsob, jakým jsou údaje dále zpracovávány, slučitelné s původními účely podle kritérií uvedených v bodě 7.6. V případě opakovaného použití informací veřejného sektoru to nevyhnutelně povede k uvážení celé řady scénářů zpracování, nikoli pouze jednoho.

7.8. Proporcionalita a jiné otázky

Další klíčovou zásadou stanovenou ve směrnici 95/46/ES je proporcionalita[33]. Existuje mnoho různých metod a způsobů zpřístupňování osobních údajů. Některé z nich mohou být rušivější než jiné a představovat více rizik. Některé proto mohou být považovány za přiměřené, zatímco jiné nikoli.

Stejně jako v případě účelu existuje otázka, jak kontrolovat další zpracovávání údajů a zajistit soulad s ostatními zásadami právních předpisů o ochraně údajů, mimo jiné včetně proporcionality. Jakmile byly údaje zpřístupněny veřejnosti, zejména na internetu, je velmi obtížné omezit účinně jejich použití a zajistit soulad s právními předpisy o ochraně údajů.

K některým problémům souvisejícím se zajištěním souladu s právními předpisy o ochraně údajů patří to:

- jak zajistit aktuálnost a přesnost údajů, které jsou odděleny od primárního zdroje,
- jak zajistit, aby bylo použití osobních údajů omezeno na funkce předpokládané u původního účelu zveřejnění,
- jak zajistit včasný výmaz údajů, pokud se zveřejnění osobních údajů předpokládalo pouze po omezenou dobu[34],
- jak uplatňovat práva fyzických osob v případě osobních údajů, které byly zpřístupněny pro opakované použití (včetně práva požádat o opravu, aktualizaci nebo výmaz).

[33] Viz čl. 6 odst. 1 písm. c) směrnice 95/46/ES.

[34] Viz například věc projednávaná Evropským soudním dvorem Volker und Markus Schecke GbR v. spolková země Hesensko (spojené věci C 92/09 a C 93/09), bod 31: „je nemožné po uplynutí doby dvou let stanovené v čl. 3 odst. 3 nařízení č. 259/2008 údaje z internetu odstranit“.

7.9. Právní a/nebo technická omezení vztahující se na opakované použití

Právní předpisy nebo technický návrh systémů někdy omezují konkrétní zpracování nebo stanoví jiná ochranná opatření, která omezují používání veřejných registrů (např. omezení možnosti stáhnout celý obsah registru nebo omezení dotazů použitých při vyhledávání, například na základě jména a příjmení fyzické osoby). V tomto případě by opakované použití mělo být v zásadě přípustné pouze v souladu s těmito konkrétními omezeními a podmínkami.

V této souvislosti je důležité pečlivě zvážit, která opatření (právní i technická) by bylo možno zavést s cílem zajistit, aby byly vyřešeny otázky ochrany údajů, včetně záležitostí uvedených v bodě 7.8. Obzvláště důležité je uvážit, jak budou moci další uživatelé získat přístup k údajům – například prostřednictvím funkce hromadného stahování nebo prostřednictvím uzpůsobeného rozhraní s funkcemi omezujícími přístup s výhradou určitých podmínek. V této souvislosti má zásadní význam skutečnost, jaké dodatečné bezpečnostní kontroly budou zavedeny, například „captcha“[35], systém ověřování, který má zabránit automatickému přístupu a minimalizovat riziko získání celé databáze. Použití zvláštních technických opatření může pomoci omezit zneužití osobních údajů a snížit negativní dopady na subjekty údajů, jež by jinak byly možné v důsledku neomezeného a bezpodmínečného přístupu dalších uživatelů k celým souborům údajů.

Důležité je, že v mnoha případech může být nezbytné zajistit, aby další uživatelé mohli zadávat pouze cílené dotazy prostřednictvím technologií, které mají zamezit hromadnému stahování datových záznamů, například prostřednictvím uzpůsobených aplikačních programovacích rozhraní (API). To může pomoci zajistit přiměřenost použití a omezit rizika zneužití celých databází. Tato uzpůsobená rozhraní mohou mimoto pomoci zajistit, aby byly údaje vždy aktuální a rovněž aby údaje již nebyly prostřednictvím API dostupné, jakmile dotčený subjekt veřejného sektoru přijme rozhodnutí za tímto účelem. Na druhou stranu to může omezovat způsoby opakovaného použití údajů ze strany dalšího uživatele.

7.10. Přesnost, aktualizace a výmaz

Další zvláštní otázkou je to, co se stane, jsou-li osobní údaje zveřejněny či zpřístupněny jinak pouze po omezenou dobu. V čl. 6 odst. 1 písm. e) směrnice 95/46/ES je stanoveno, že osobní údaje musí být uchovávány ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro uskutečnění cílů, pro které jsou shromažďovány nebo dále zpracovávány. Rovněž 18. bod odůvodnění směrnice o informacích veřejného sektoru stanoví, že „rozhodne-li se příslušný orgán, že již nebude určité dokumenty poskytovat pro opakované použití nebo že tyto dokumenty přestane aktualizovat, měl by tato rozhodnutí při nejbližší příležitosti zveřejnit, pokud možno elektronickými prostředky“.

Jakmile byly údaje zveřejněny a zpřístupněny pro opakované použití, je však obtížné či někdy dokonce nemožné zajistit, aby byly tyto údaje vymazány nebo odstraněny.

V této souvislosti může určité (ačkoli v žádném případě dokonalé) řešení představovat to, nejsou-li údaje zpřístupněny ve stahovatelné formě, pouze prostřednictvím uzpůsobeného API a podléhají-li určitým omezením a bezpečnostním opatřením, jak bylo uvedeno výše.

VIII. Údaje z výzkumu

[35] CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart – plně automatický veřejný Turingův test k odlišení počítačů a lidí) je systémový test založený na dotazu a odpovědi, který má rozlišit člověka od automatických programů. CAPTCHA rozlišuje mezi člověkem a počítačem pomocí určitého úkolu, jehož splnění je pro většinu lidí snadné, avšak pro stávající počítačové programy složitější.

Zde je důležité rozlišovat mezi zveřejněním anonymizovaných údajů na straně jedné (viz oddíl VI) a omezeným přístupem na straně druhé. Program veřejně přístupných údajů jednoznačně závisí na veřejné dostupnosti údajů. Značná část výzkumu (co je důležité, vědecký výzkum, a to pro komerční i nekomerční účely, avšak rovněž jiný výzkum) se uskutečňuje zveřejněním údajů v rámci uzavřené komunity, tj. v případě, kdy přístup k údajům má určitý konečný počet výzkumných pracovníků nebo institucí a kdy lze omezit další zveřejnění nebo použití údajů a zaručit jejich bezpečnost.

Omezený přístup je obzvláště důležitý při nakládání s osobními údaji (často v pseudonymizované podobě[36]) odvozenými z citlivých zdrojových materiálů nebo v případě, existuje-li značné riziko opětovného identifikování. Rizika spojená se zveřejněním s omezeným přístupem se mohou přesto vyskytnout, jsou však nižší a lze je lépe omezit, pokud jsou údaje zveřejněny v rámci uzavřené komunity, která pracuje podle zavedených pravidel.

Problémem, s nímž se subjekty používající údaje pro výzkumné účely často potýkají, je skutečnost, že na straně jedné potřebují údaje, které jsou obsáhlé, strukturované a dostatečně použitelné pro jejich účely; na straně druhé chtějí zajistit, aby nedošlo k opětovnému identifikování jednotlivců. Údaje pseudononymizované na osobní úrovni (například jednoduše kódované pomocí klíče) mohou být pro výzkumné pracovníky velmi cenné kvůli strukturování na osobní úrovni a kvůli tomu, že pseudononymizované záznamy z různých zdrojů lze relativně snadno porovnat. To však rovněž znamená, že existuje vysoké riziko opětovného identifikování: možnost propojení několika souborů údajů (pseudononymizovaných, či nikoli) vztahujících se k témuž jednotlivci může být výchozím bodem k identifikaci nebo může usnadnit přímou identifikaci.

Před zveřejněním nebo zpřístupněním souborů pseudononymizovaných údajů pro opakované použití je proto zapotřebí vyšší úroveň prověření a dodatečná obezřetnost. Čím jsou údaje na osobní úrovni podrobnější a lze je snáze propojit, tím omezenější a kontrolovanější by měl být přístup k těmto údajům. Čím jsou údaje agregovanější a méně propojitelné, tím je pravděpodobnější, že mohou být zveřejněny a zpřístupněny pro opakované použití bez značných rizik.

Jedná se o složitou a vyvíjející se oblast a nebylo by vhodné vyloučit kategoricky zveřejnění a opakované použití všech souborů údajů, které nedosahují vysokého limitu „anonymizace“, jak bylo popsáno v oddíle VI. Ačkoli se v každém jednotlivém případě vždy vyžaduje analýza a pečlivé posouzení, pracovní skupina podle článku 29 se obecně domnívá, že zveřejnění souborů údajů na osobní úrovni nebo jiných souborů údajů představujících významné riziko opětovného identifikování za podmínek stanovených ve směrnici o informacích veřejného sektoru nebude často vhodné.

Mimoto je důležité zdůraznit, že pokud by po pečlivém posouzení rizik a přínosů měly být přesto některé takovéto soubory údajů zveřejněny a zpřístupněny, musí být zveřejnění a případné další opakované použití zcela v souladu s právními předpisy o ochraně údajů (viz oddíl VII). Důvodem je skutečnost, že se tyto údaje navzdory určitým (někdy velmi významným) opatřením přijatým k snížení rizika opětovného identifikování i nadále pokládají za osobní údaje.

IX. Historické archivy

Rovněž historické archivy a muzea mají zvláštní charakteristiky, jež vyžadují specifická ochranná opatření. V mnoha případech mohou být v závislosti na faktorech, jako je stáří a citlivost údajů

[36] Viz opět stanovisko č. 4/2007 k pojmu osobní údaje, přijaté dne 20. 6. 2007 (WP 136), zejména na s. 12–21 (pojednávající o „pseudonymizovaných údajích“, „údajích kódovaných pomocí klíče“ a „anonymních údajích“ na s. 18–21). Otázka týkající se informací „o“ určité osobě je projednána na s. 9–12. Jak je uvedeno na s. 3, důležité je rovněž to, že pracovní skupina podle článku 29 v současnosti pracuje na dalších pokynech k technikám anonymizace.

a kontext jejich získání, vhodnější jiné možnosti (například povolení omezeného přístupu pouze s výhradou povinnosti zachovat mlčenlivost) než digitalizace a zpřístupnění údajů pro opakované použití na internetu bez omezení.

Co se týká archivů, je důležité zdůraznit, že ačkoli se citlivost údajů obvykle postupem času snižuje, nepatřičné zveřejnění záznamů starých mnoho desetiletí může mít přesto závažný nepříznivý dopad na jednotlivce, kterých se to přímo týká, avšak rovněž na jiné osoby, například rodinné příslušníky nebo potomky. To platí zejména pro vysoce citlivé údaje. Zveřejněné rejstříky trestů budou například jednotlivce dále stigmatizovat a zabrání jeho rehabilitaci. Informace, že zesnulá osoba byla tajným agentem nebo spolupracovníkem despotického režimu, pedofilem, pachatelem trestných činů, trpěla duševní chorobou vyvolávající stigma nebo dědičnou chorobou, mohou mít negativní dopad rovněž na rodinu (pozůstalého manžela/manželku, děti nebo jiné potomky) zesnulé osoby. Rovněž vzorky DNA zesnulých osob, které jsou někdy uchovávány v archivech veřejných nemocnic, mohou z podobných důvodů vyžadovat ochranu. Tyto informace proto mohou i v případě, že se týkají zesnulých osob, vyžadovat ochranu podle právních předpisů o ochraně údajů a/nebo jiných právních předpisů, které chrání základní práva.

Členské státy mají často zvláštní zákony, které upravují přístup do národních archivů, do archivů z historických období zvláštního zájmu (jako jsou archivy dokládající spolupráci s despotickými režimy) a ke spisům uchovávaným soudy[37]. Tyto zákony často vyžadují odpovídající bezpečnostní opatření a omezení přístupu a jiná ochranná opatření, která mají dosáhnout rovnováhy mezi dotyčnými zájmy a zajistit dostupnost určitých osobních údajů pro účely historického výzkumu, transparentnosti a pátrání novinářů, a současně zaručit, že zveřejnění těchto údajů, je-li nezbytné, je omezeno tak, aby nepoškodilo soukromý a rodinný život a důstojnost dotčených stran.

Co se týká „omezení účelu“, je třeba podotknout, že historické archivy obvykle uchovávají informace pro účely historického výzkumu. Tyto účely se liší od původních účelů, pro něž byly údaje shromážděny. Materiály, které nakonec skončí v archivních sbírkách, byly původně vytvořeny pro zvláštní administrativní účely různými subjekty soukromého sektoru. Po určité době se v případě, že již dokument není pro původní administrativní účely zapotřebí, obvykle provede výběr a dokumenty, u nichž se usuzuje, že mají „historickou“ hodnotu, budou předány do historických archivů. Otázkou je, pro jaké účely by měly být osobní údaje uchovávané v archivech zpřístupněny pro opakované použití. V této souvislosti je důležité provést pečlivé posouzení – vzhledem k možnému významu zpřístupnění archivních materiálů pro opakované použití, avšak rovněž k potenciálnímu dopadu na práva, svobody a důstojnost dotčených osob.

Celkově lze vyvodit závěr, že ačkoli digitalizace určitých záznamů, které obsahují osobní údaje, a jejich zpřístupnění pro opakované použití mohou být v některých případech vhodné a některé údaje mohou být zveřejněny rovněž v anonymizované podobě, v jiných případech jsou nanejvýš důležitá omezení vztahující se na zveřejnění a opakované použití osobních údajů a přiměřená bezpečnostní opatření na ochranu těchto údajů. Důkladné posouzení dopadu na ochranu údajů by mělo zajistit, že archivní sbírka nebude zpřístupněna pro opakované použití, není-li vyloučen možný negativní dopad na dotyčné jednotlivce nebo nejsou-li tato rizika omezena na přijatelné minimum. Oblast archivnictví by mohla uvážit rovněž vypracování kodexů nebo změnu stávajících kodexů za účelem objasnění osvědčených postupů.

X. Vydávaní licencí na opakované použití osobních údajů

10.1. Příslušná ustanovení směrnice o informacích veřejného sektoru

[37] K dalším příkladům by mohly patřit archivy matrik, které v některých členských státech obsahují mimo jiné údaje o příčině smrti, změně pohlaví, jménu partnera (z čehož lze odvodit sexuální orientaci) nebo osvojení dotyčné osoby. Přístup k těmto archivům rovněž podléhá zvláštním podmínkám.

V 15. bodě odůvodnění směrnice o informacích veřejného sektoru je uvedeno, že „předpokladem rozvoje informačního trhu v celém Společenství je zajistit, aby podmínky opakovaného použití dokumentů veřejného sektoru byly jasné a veřejně dostupné. Proto by měly být všechny platné podmínky opakovaného použití dokumentů objasněny potenciálním dalším uživatelům. Členské státy by měly prosazovat vytváření seznamů dostupných dokumentů, případně přístupných on-line, aby podporovaly a usnadňovaly žádosti o opakované použití."

Ve 26. bodě odůvodnění novely směrnice je dále stanoveno, že „v souvislosti s každým opakovaným použitím dokumentu mohou subjekty veřejného sektoru, ve vhodných případech prostřednictvím licence, uložit podmínky ..." a že by „členské státy měly ve vhodných případech podporovat používání otevřených, strojově čitelných formátů".

V čl. 8 odst. 1 se stanoví, že „subjekty veřejného sektoru mohou povolit opakované použití bez dalších podmínek nebo mohou uložit podmínky, případně na základě licence. Tyto podmínky nesmějí zbytečně omezovat možnosti opakovaného použití a nesmějí být použity pro omezování hospodářské soutěže."

10.2. Udělování licencí a ochrana údajů

Licence jsou hlavní součástí režimu vztahujícího se na informace veřejného sektoru. Mohou rovněž ovlivnit způsob zpracovávání osobních údajů a měly by být mezi ochrannými opatřeními, která jsou uplatňována při zpřístupňování osobních údajů (nebo anonymizovaných údajů odvozených z osobních údajů) pro opakované použití. Licence neodstraňují nutnost dodržovat právní předpisy o ochraně údajů, ustanovení o ochraně údajů v licenčních podmínkách však pomůže zajistit soulad s právními předpisy o ochraně údajů připojením roviny „vymahatelnosti". Toto ustanovení může rovněž pomoci zvýšit informovanost tím, že dalším uživatelům připomene jejich povinnosti coby správců údajů.

Co se týká obsahu licencí, je užitečné rozlišovat mezi dvěma různými scénáři.

10.3. Licenční podmínky v případě souborů anonymizovaných údajů

Za prvé, co se týká anonymizovaných údajů (tj. souboru údajů, které již neobsahují osobní údaje), licenční podmínky by měly

- opakovat, že údaje byly anonymizovány,
- zakazovat držitelům licence opětovné identifikování fyzických osob[38],
- zakazovat držitelům licence použití údajů k přijímání opatření nebo rozhodnutí s ohledem na dotyčné jednotlivce a
- ukládat držiteli licence povinnost uvědomit poskytovatele licence v případě, je-li zjištěno, že jednotlivce lze opětovně identifikovat nebo že byli opětovně identifikováni.

Alternativou licenční podmínky by mohlo být zřetelné upozornění dalších uživatelů na portálu veřejně přístupných údajů. Mělo by se však prosazovat stanovení licenčních podmínek, jelikož zajišťuje přidanou hodnotu v podobě smluvní vymahatelnosti.

Zrušení ohrožených souborů údajů

[38] Mohou platit omezené výjimky, například v případech ověřování opětovného identifikování v dobré víře. I v těchto případech by však měl být na výsledky testů upozorněn správce a dotyčný subjekt veřejného sektoru a opětovně identifikované údaje by neměly být zveřejněny či jinak obecně šířeny.

Možnost upozornit poskytovatele licence na skutečnost, že došlo nebo že může dojít k opětovnému identifikování, musí být dostupná pro všechny ostatní uživatele internetových stránek, včetně samotných subjektů údajů. Zjistí-li poskytovatel licence vyšší riziko opětovného identifikování, měl by být v licenci stanoven postup, jehož prostřednictvím může poskytovatel licence „zrušit" „ohrožený" soubor údajů. Jinými slovy, ustanovení o ochraně údajů by mělo poskytovatele licence opravňovat k pozastavení nebo ukončení dostupnosti údajů (např. právo vypnout API nebo odstranit soubor z platformy). Poskytovatel licence by měl vynaložit veškeré úsilí, aby všechny další uživatele požádal o výmaz celých souborů údajů nebo částí souborů, které jsou ohroženy (staly se opětovně identifikovatelnými). To by mělo zahrnovat zřetelná oznámení na internetových stránkách, jako jsou portály veřejně přístupných údajů a fóra / e-mailové seznamy / sociální média, k nimž mají přístup skupiny nebo jednotlivci, kteří budou pravděpodobně údaje opakovaně používat. Nejúčinnějším prostředkem k zrušení souborů údajů může být požadování registrace, to by se však nemělo prosazovat v případě, vyžaduje-li to sběr nových osobních údajů dalších uživatelů a odrazuje-li to obecně od používání internetových stránek s informacemi veřejného sektoru a jiných služeb.

10.4. Licenční podmínky v případě osobních údajů

Pokud se licence týká osobních údajů, je nutno stanovit meze použití těchto údajů. Hlavní otázkou je zajištění, aby případné opakované použití bylo omezeno na to, co je „slučitelné s účely, pro něž byly údaje původně shromážděny"[39]. K dosažení tohoto cíle musí licenční podmínky přinejmenším objasňovat, pro jaké účely byly údaje prvně zveřejněny, a uvádět, co se bude považovat za slučitelné použití osobních údajů, a co nikoli.

Je však třeba podotknout, že to by nemělo „zbytečně omezovat možnosti opakovaného použití" (čl. 8 odst. 1 novely směrnice). To může často znamenat, že obecné podmínky běžných veřejných licencí nejsou vhodné a může být nezbytné vypracovat pro určité osobní údaje zvláštní licence, nebo je možné používat šablony, jež mohou být upravené.

V současnosti vylučují některé běžné veřejné licence (např. veřejná vládní licence ve Spojeném království) osobní údaje – s ohledem na tyto údaje není udělena licence za žádných podmínek.

[39] Viz opět stanovisko pracovní skupiny podle článku 29 č. 3/2013 k omezení účelu.

10.5 V případě opětovného identifikování nebo neslučitelného použití by mělo následovat důsledné vymáhání práva

Pokud byly údaje zveřejněny na základě licence (např. veřejné vládní licence), může být obtížné chránit je před dalším neslučitelným použitím nebo zveřejněním či zajistit jejich bezpečnost. V této souvislosti je velmi důležité sledování opakovaného použití a vymáhání dodržování předpisů v případě jejich porušení, ať už v podobě opětovného identifikování subjektů údajů nebo dalšího použití k neslučitelnému účelu ze strany poskytovatele licence.

Pracovní skupina podle článku 29 znovu vyzdvihuje důležitou úlohu, kterou by měly mít subjekty veřejného sektoru, a rovněž zdůrazňuje, že pokud další uživatel shromažďuje osobní údaje prostřednictvím opětovného identifikování, bude se s největší pravděpodobností mít za to, že zpracovává osobní údaje nezákonně, a mohla by se na něj vztahovat donucovací opatření orgánů pro ochranu údajů. To zahrnuje vysoké pokuty uložené podle navrhovaného nařízení o ochraně údajů.

XI. Závěry

Závěrem pracovní skupina podle článku 29 opakuje, že opakované použití informací veřejného sektoru může zajistit přínosy vedoucí k větší transparentnosti a inovativnímu opakovanému použití informací veřejného sektoru. Výsledná větší dostupnost informací však není bez rizika. V zájmu zajištění ochrany soukromí a osobních údajů jednotlivců je třeba uplatňovat vyvážený přístup a právní předpisy o ochraně údajů musí pomoci řídit proces výběru osobních údajů, které lze, či nelze zpřístupnit pro opakované použití, a opatření, která je nutno přijmout na ochranu osobních údajů.

Bez ohledu na „zásadu opakovaného použití“ stanovenou v novele směrnice není opakované použití ke komerčním či nekomerčním účelům za podmínek stanovených ve směrnici o informacích veřejného sektoru vždy vhodné v případech, kdy informace veřejného sektoru, jež mají být použity opakovaně, obsahují osobní údaje. Pro opakované použití často jsou a měly by být zpřístupněny statistické údaje odvozené z osobních údajů místo osobních údajů.

V některých případech však lze uvážit rovněž zpřístupnění osobních údajů za účelem opakovaného použití za podmínek stanovených ve směrnici o informacích veřejného sektoru, v případě potřeby s výhradou dalších právních, technických nebo organizačních opatření na ochranu dotyčných osob. V těchto případech pracovní skupina podle článku 29 znovu zdůrazňuje význam stanovení pevného právního základu pro zpřístupňování osobních údajů veřejnosti s přihlédnutím k příslušným pravidlům ochrany údajů, včetně zásady proporcionality, minimalizace údajů a omezení účelu. V této souvislosti je také důležité znovu zdůraznit, že případné informace o identifikované nebo identifikovatelné fyzické osobě bez ohledu na to, zda jsou veřejně přístupné, či nikoli, představují osobní údaje. Na přístup k osobním údajům, jež byly zpřístupněny veřejnosti, a jejich opakované použití se proto i nadále vztahují platné právní předpisy o ochraně údajů.

Na základě těchto úvah pracovní skupina podle článku 29 doporučuje toto:

- skutečnost, že některé informace veřejného sektoru mohou obsahovat osobní údaje, by měla být při zvažování zpřístupnění informací veřejného sektoru vzata v úvahu co nejdříve, a to podle zásad „ochrany údajů již od návrhu a standardního nastavení ochrany údajů“,
- maje toto na paměti by dotčený subjekt veřejného sektoru (nebo případně zákonodárce) měl provést posouzení dopadu na ochranu údajů před zpřístupněním informací veřejného sektoru, které obsahují osobní údaje, pro opakované použití (nebo před přijetím zákona, který umožňuje zveřejňování osobních údajů, a tudíž je potenciálně zpřístupňuje pro opakované použití); posouzení dopadu na ochranu údajů by mělo být provedeno rovněž

v případech, kdy budou pro opakované použití zpřístupněny soubory anonymizovaných údajů odvozených z osobních údajů,

- jsou-li údaje anonymizovány, je nezbytné posoudit riziko opětovného identifikování, a osvědčeným postupem je ověření opětovného identifikování,
- výsledek posouzení může pomoci určit vhodná ochranná opatření k omezení rizik na minimum, mimo jiné včetně technických, právních a organizačních opatření, jako jsou vhodné licenční podmínky a technická opatření, která zamezují hromadnému stahování údajů, a odpovídající techniky anonymizace; to může vést rovněž k rozhodnutí upustit od zveřejnění a/nebo zpřístupnění údajů pro opakované použití,
- podmínky licence na opakované použití informací veřejného sektoru by měly obsahovat ustanovení o ochraně údajů, pokud jsou zpracovávány osobní údaje, včetně případů, kdy pro opakované použití budou zpřístupněny soubory anonymizovaných údajů odvozených z osobních údajů,
- vede-li posouzení dopadu na ochranu údajů k závěru, že k odstranění rizik pro ochranu údajů nepostačuje veřejná licence, neměly by subjekty veřejného sektoru zpřístupnit osobní údaje podle směrnice o informacích veřejného sektoru. (Subjekt veřejného sektoru se však může rozhodnout, že uváží opakované použití mimo oblast působnosti směrnice o informacích veřejného sektoru, a může rovněž požadovat, aby žadatelé prokázali, že jsou náležitě odstraněna případná rizika pro ochranu osobních údajů a že žadatel bude údaje zpracovávat v souladu s platnými právními předpisy o ochraně údajů),
- subjekty veřejného sektoru by měly případně zajistit, aby byly osobní údaje anonymizovány a aby licenční podmínky výslovně zakazovaly opětovné identifikování jednotlivců a opakované použití osobních údajů pro účely, které se mohou nepříznivě dotýkat subjektů údajů,
- členské státy by měly uvážit rovněž zřízení znalostních sítí /center excelence a poskytování podpory těmto subjektům, a tím umožnit sdílení osvědčených postupů souvisejících s anonymizací a veřejně přístupnými údaji.

V Bruselu dne 5. června 2013

Za pracovní skupinu
předseda
Jacob KOHNSTAMM

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
e-mail: nejedlam@uoou.cz
internetová adresa: www.uoou.cz

ISSN: 2336-4742