VĚSTNÍK

ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ

2017

Částka 73 **Srpen 2017**

OBSAH

Úvod 4116

I. Registrace

Přehled zrušených registrací od 1. října 2016 do 31. července 2017 4117

II. Stanoviska Úřadu

Stanovisko č. 3/2009 (revize červen 2017): Biometrická identifikace nebo autentizace zaměstnanců 4120

III. Sdělení Úřadu

1. K novele zákona o trestní odpovědnosti právnických osob 4125
2. ÚOOÚ ke schválení novely zákona o inspekci práce 4126
3. K DIČ na účtenkách EET 4126
4. Ke zpracování osobních údajů při využívání elektronických karet ve veřejné dopravě 4127
5. K centrálnímu registru dlužníků České republiky (CERD) 4128
6. K oznamovací povinnosti veterinárních lékařů 4128
7. Zveřejňování záběrů zákroků strážníků obecní (městské) policie 4129
8. Postup při vydávání osvědčení o ochraně osobních údajů podle GDPR 4131

Shrnutí stanovisek Pracovní skupiny WP29:

1. Stanovisko č. 01/2017 k návrhu ePrivacy nařízení 4132
2. Pracovní skupina WP29 vydala tři dokumenty k obecnému nařízení o ochraně osobních údajů 4133

ÚVOD

I sedmdesátá třetí částka Věstníku Úřadu pro ochranu osobních údajů obsahuje přehled zrušených registrací. Ty se týkají období od 1. října 2016 do 31. července 2017.

Rubrika Stanoviska Úřadu přináší revizi stanoviska č. 3/2009 - Biometrická identifikace nebo autentizace zaměstnanců. Ta ve svém čl. 9 upravuje zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby. Tato úprava přináší podstatnou změnu v právním pohledu na technologie zpracovávající biometrické údaje, kromě jiného také v tom, že uchovávání biometrických šablon (template) a jejich zpracování za účelem identifikace osob považuje za zpracování zvláštní kategorie osobních údajů.

V rubrice Sdělení Úřadu naleznete důležité informace k novele zákona o trestní odpovědnosti právnických osob a řízení proti nim. Tato úprava má dopad do ochrany osobních údajů.

V souvislosti se zahájením elektronické evidence tržeb podle zákona č. 112/2016 Sb., o evidenci tržeb, se množí dotazy podnikatelů na uvádění daňového identifikačního čísla na vydávaných účtenkách, v jehož důsledku bude docházet ke zpřístupňování jejich rodných čísel v mnohem větším rozsahu, než tomu bylo v souvislosti s dosavadní povinností uvádět daňové identifikační číslo. Věstník obsahuje prohlášení ÚOOÚ v této oblasti.

ÚOOÚ zde zveřejňuje i zásady pro provoz elektronických karet v dopravě, neboť se v poslední době na toto téma více setkával s dotazy veřejnosti.

Dočtete se o varování ÚOOÚ před činností provozovatele registru „Centrální registr dlužníků České republiky“ (CERD), který za úplatu anoncuje vydávání potvrzení o bezdlužnosti.

Naleznete zde článek k oznamovací povinnosti veterinárních lékařů podle § 16 zákona o ochraně osobních údajů.

Věstník se v této částce věnuje i hojně diskutovanému tématu pořizování záběrů zákroků strážníků obecní policie.

Je zde sdělen postup pro vydávání osvědčení o ochraně osobních údajů podle GDPR, kdy se přijetím nařízení EP a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, do právního řádu zavádí mechanismy pro vydávání pečetí, známek a osvědčení o ochraně údajů, které budou prokazovat soulad s nařízením (čl. 42 a 43) o ochraně osobních údajů.

Ve shrnutí stanovisek a dokumentů Pracovní skupiny WP29 se dočteme o schválení stanoviska k revizi směrnice 2002/58/ES o soukromí a elektronických komunikacích. Návrh nového nařízení, které předložila Evropská komise již v lednu 2017, by měl poskytnout uživatelům elektronických komunikací vysokou úroveň ochrany soukromí a rovné podmínky pro všechny účastníky na trhu.

Na závěr Věstník obsahuje zmínku o prvních třech materiálech z řady dokumentů, které mají poskytnout výklad novinek zaváděných obecným nařízením o ochraně osobních údajů.

I. REGISTRACE

Přehled zrušených registrací od 1. října 2016 do 31. července 2017

Číslo registrace	Subjekt	Datum zrušení
00001220/002	Eberspächer spol. s r.o.	27.04.2017
00001942/001	Stacionář Ústí nad Orlicí	10.02.2017
00001985/006	Westrock Packaging Systems Svitavy, s.r.o.	01.11.2016
00002028/001	Credium, a.s., v likvidaci	30.06.2017
00002028/005	Credium, a.s., v likvidaci	30.06.2017
00002028/012	Credium, a.s., v likvidaci	30.06.2017
00004183/007	SALFA a.s.	11.05.2017
00004183/008	SALFA a.s.	11.05.2017
00004183/009	SALFA a.s.	06.05.2017
00004183/010	SALFA a.s.	11.05.2017
00004183/011	SALFA a.s.	11.05.2017
00004183/012	SALFA a.s.	11.05.2017
00004183/013	SALFA a.s.	11.05.2017
00004183/014	SALFA a.s.	11.05.2017
00004183/015	SALFA a.s.	11.05.2017
00005614/003	KROBASC s.r.o.	29.03.2017
00008467/005	Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)	21.04.2017
00009279/001	Jana Zbořilová	24.12.2016
00010407/001	INDEX NOSLUŠ s.r.o.	13.12.2016
00011855/003	Estée Lauder CZ, s.r.o.	26.04.2017
00019116/191	Správa železniční dopravní cesty, státní organizace	22.06.2017
00025959/012	S.B.S. Services s.r.o.	06.06.2017
00025959/013	S.B.S. Services s.r.o.	06.06.2017
00025959/026	S.B.S. Services s.r.o.	06.06.2017
00025959/028	S.B.S. Services s.r.o.	06.06.2017
00025959/029	S.B.S. Services s.r.o.	06.06.2017
00025959/036	S.B.S. Services s.r.o.	06.06.2017
00027286/001	Cushman & Wakefield, s.r.o.	09.05.2017
00027286/004	Cushman & Wakefield, s.r.o.	09.05.2017
00030725/022	Fresenius Medical Care - DS, s.r.o.	23.12.2016
00030828/003	Acebiz s.r.o.	07.03.2017
00032346/001	Archiv bezpečnostních složek	28.03.2017
00032618/003	STARÝ PIVOVAR s.r.o.	17.03.2017
00033197/001	APODEMA s.r.o.	21.02.2017
00033197/002	APODEMA s.r.o.	21.02.2017
00033197/003	APODEMA s.r.o.	21.02.2017
00034899/002	STAHLGRUBER CZ s.r.o.	22.11.2016
00034993/001	Střední odborné učiliště Kyjov, příspěvková organizace	31.12.2016
00035235/001	EUROSIGNAL, a.s.	07.07.2017
00035495/008	Direct Parcel Distribution CZ s.r.o.	30.12.2016
00035739/002	Travelex Czech Republic a.s.	29.07.2017

Číslo registrace	Subjekt	Datum zrušení
00035857/002	Magnalink, a.s.	28.10.2016
00035958/005	CSC Computer Sciences s.r.o.	08.10.2016
00036292/002	Bertiny lázně Třeboň s.r.o.	20.06.2017
00036546/001	KCL CZ s.r.o., „ v likvidaci „	04.11.2016
00036546/002	KCL CZ s.r.o., „ v likvidaci „	04.11.2016
00036867/001	Metaldyne Oslavany, spol. s r.o.	29.03.2017
00039436/001	Eva Benešová	08.02.2017
00040419/013	TSR Czech Republic s.r.o.	22.10.2016
00040419/017	TSR Czech Republic s.r.o.	22.10.2016
00040419/019	TSR Czech Republic s.r.o.	22.10.2016
00041981/001	MĚSTSKÁ DOPRAVA Mariánské Lázně s.r.o.	01.07.2017
00042224/003	Fresenius Medical Care - ČR, s.r.o.	23.12.2016
00042303/001	GREEN & SANDERS s.r.o. v likvidaci	29.03.2017
00044112/001	Lékárenská CZ, spol. s r.o.	21.02.2017
00044112/002	Lékárenská CZ, spol. s r.o.	21.02.2017
00044112/003	Lékárenská CZ, spol. s r.o.	21.02.2017
00044112/004	Lékárenská CZ, spol. s r.o.	21.02.2017
00044112/005	Lékárenská CZ, spol. s r.o.	21.02.2017
00044112/006	Lékárenská CZ, spol. s r.o.	21.02.2017
00046116/001	Fair Credit International, SE	02.11.2016
00046116/002	Fair Credit International, SE	02.11.2016
00046192/008	INVESTMENT AGENCY s.r.o.	03.06.2017
00046192/009	INVESTMENT AGENCY s.r.o.	03.06.2017
00046192/010	INVESTMENT AGENCY s.r.o.	03.06.2017
00046192/012	INVESTMENT AGENCY s.r.o.	03.06.2017
00046192/013	INVESTMENT AGENCY s.r.o.	03.06.2017
00046431/001	BERAN MIROSLAV	22.07.2017
00047106/001	SOLOFORM spol. s r.o.	23.03.2017
00048998/001	PRECHEZA a.s.	08.12.2016
00049046/008	S.B.S. SECURITY s.r.o.	09.06.2017
00049353/001	ProSpanek a.s.	16.12.2016
00049353/002	ProSpanek a.s.	16.12.2016
00049503/001	BEZPECACI.CZ Ltd., organizační složka	27.07.2017
00050518/009	BONVER WIN, a.s.	24.03.2017
00050518/011	BONVER WIN, a.s.	24.03.2017
00050518/041	BONVER WIN, a.s.	24.03.2017
00050518/061	BONVER WIN, a.s.	24.03.2017
00050518/072	BONVER WIN, a.s.	24.03.2017
00050518/105	BONVER WIN, a.s.	20.01.2017
00050518/107	BONVER WIN, a.s.	24.03.2017
00050808/001	Doggino PRO, s.r.o.	04.02.2017
00053061/001	SUNPHARMA CZ, s. r. o.	21.02.2017
00053061/002	SUNPHARMA CZ, s. r. o.	21.02.2017
00053764/001	JV Dřevoprodukt, s.r.o.	04.10.2016
00054249/001	Vratislav Hlásek	20.04.2017

Číslo registrace	Subjekt	Datum zrušení
00055766/004	iCredit s.r.o.	20.04.2017
00055766/005	iCredit s.r.o.	05.06.2017
00055766/007	iCredit s.r.o.	05.06.2017
00055766/008	iCredit s.r.o.	20.04.2017
00055766/009	iCredit s.r.o.	05.06.2017
00055766/010	iCredit s.r.o.	20.04.2017
00055766/011	iCredit s.r.o.	20.04.2017
00055766/012	iCredit s.r.o.	05.06.2017
00056037/001	Buckley Radka, JUDr., advokátní kancelář	24.01.2017
00056037/002	Buckley Radka, JUDr., advokátní kancelář	24.01.2017
00057704/001	DOA plus s.r.o.	03.06.2017
00057716/005	Luxury Brand Management a.s.	07.04.2017
00057716/006	Luxury Brand Management a.s.	07.04.2017
00057716/007	Luxury Brand Management a.s.	07.04.2017
00058889/001	Ivana Daďourková	03.05.2017
00059210/001	Mespil s.r.o.	24.01.2017
00059301/001	Vítězslav Hornig	22.03.2017
00059595/003	GOLDIM spol.s r.o.	11.11.2016
00060090/002	FOLGET, spol. s r.o.	17.06.2017
00060090/015	FOLGET, spol. s r.o.	17.06.2017
00060245/001	Martin Ticháček	06.04.2017
00061058/001	ODBORNÉ UČILIŠTĚ A PRAKTICKÁ ŠKOLA	23.03.2017
00061207/001	Alfa DolFIN s.r.o. v likvidaci	05.11.2016
00061221/001	RST Medistrade s.r.o.	21.02.2017
00061221/002	RST Medistrade s.r.o.	21.02.2017
00061838/001	Petra Sluková	21.06.2017
00062339/001	Mgr. Jaroslav Srp	05.02.2017
00062356/001	CWP výživové poradenství s.r.o.	04.07.2017
00062427/001	Jan Bystřický	07.04.2017
00063506/003	ProSpánek SE	03.05.2017
00063673/001	RESTGAME s.r.o.	24.12.2016
00063691/001	Jarmila Kolaříková	06.01.2017
00064708/001	I.T.A. Fashion s.r.o.	31.03.2017
00064903/001	Francesco Biondo	10.05.2017
00065800/001	Kitos s.r.o.	07.04.2017
00065834/001	Hornig provozní s. r. o.	21.03.2017
00065921/001	Radka Frýzková	07.01.2017
00067111/001	JAROSLAV PELÁN	23.11.2016
00069052/001	Railway Builder, s.r.o.	14.04.2017
00069369/001	Mgr. Lucie Hilscherová	02.03.2017
00070651/001	PERFECT CANTEEN s.r.o.	23.03.2017

II. STANOVISKA ÚŘADU

STANOVISKO č. 3/2009

květen 2009, poslední revize červen 2017

Biometrická identifikace nebo autentizace zaměstnanců

Upozornění na změnu v hodnocení úrovně právní ochrany biometrických údajů

Toto stanovisko, v mezích dosud platného § 4 písm. b) zákona o ochraně osobních údajů, prakticky rozděluje systémy s biometrickými údaji na ty, s nimiž lze zacházet jako s běžnými systémy zpracovávajícími osobní údaje, a na systémy s citlivými údaji, které vyžadují zvláštní, resp. přísnější systém ochrany.

Dne 25. května 2018 nabývá účinnosti evropský předpis, který nově nastavuje ochranu osobních údajů mj. z důvodu proměn a rychlého rozvoje technologií, tzv. obecné nařízení o ochraně osobních údajů (nařízení Evropského parlamentu a Rady, č. 2016/679). Ve svém čl. 9 upravuje zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby. Tato úprava přináší podstatnou změnu v právním pohledu na technologie zpracovávající biometrické údaje, mj. také v tom, že uchovávání biometrických šablon (template) a jejich zpracování za účelem identifikace osob považuje za zpracování zvláštní kategorie osobních údajů.

Obecné nařízení v otázkách zpracování biometrických údajů plně nahradí dosud platné ustanovení zákona o ochraně osobních údajů, nebude tedy možno postupovat v mezích dosavadního stanoviska Úřadu pro ochranu osobních údajů. Kontroly zpracování osobních údajů prováděné v současné době jsou již vedeny s přihlédnutím k této skutečnosti a kontrolní závěry budou formulovány takovým způsobem, aby správci osobních údajů měli informace o postupu, který nebude v rozporu s obecným nařízením. V návaznosti na výsledky kontrol ÚOOÚ zveřejní aktuální stanovisko k biometrickým údajům.

Biometrické technologie, přes jejich stále větší dostupnost a dosažitelnost (technickou i finanční), nejsou plnou náhradou jiných bezpečnostních řešení a samy o sobě nezajišťují větší bezpečnost. Správci pořizující si takové systémy mají nejen povinnost posoudit přiměřenost konkrétního řešení a rizika s ním spojená (např. systémů s databázemi biometrických šablon) ale také musí vhodně kombinovat biometrický systém s dalšími bezpečnostními opatřeními. Správci musí předem i průběžně posuzovat účinnost biometrických systémů a také přitom zkoumat, zda existují vážné hrozby, které instalaci takových systémů odůvodňují.

Úvod

Záměrem stanoviska je vyjádřit základní přístupy Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ“) pro použití systémů umožňujících spolehlivé určení fyzické osoby na základě unikátních biometrických znaků, které se v poslední době velmi rozšířilo i v pracovněprávních vztazích. Nejčastěji je ze strany zaměstnavatele vznášen požadavek na poskytnutí otisků prstů (případně otisku dlaně) zaměstnanců pro použití v přístupových a docházkových systémech. Použití biometrických znaků má vyloučit možnosti klamání zaměstnavatele při použití jiných prostředků, např. identifikačních karet, v docházkových

systémech. V přístupových systémech má otisk prstu zajistit spolehlivé určení osoby oprávněné pro přístup do chráněných prostor nebo k chráněným informacím.

Otiskem prstu se rozumí obraz papilárních linií prstu včetně charakteristických změn (markantů) zaznamenaný na vhodném nosiči a určený pro další použití. V systémech biometrické identifikace nebo autentizace se markanty digitálně vyhodnocují. Systémy se mohou lišit počtem, případně i druhem používaných markantů. Otisk prstu je považován za prakticky unikátní. To zakládá možnost přímého ztotožnění nositele zobrazované biometrické charakteristiky. Tím otisk prstu naplňuje znaky citlivého biometrického údaje jako údaje umožňujícího přímou identifikaci nebo autentizaci subjektu údajů podle § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“).

Jakkoliv ÚOOÚ přísluší posuzovat pouze operace prováděné s osobními údaji ve smyslu definice zpracování osobních údajů podle § 4 písm. e) zákona o ochraně osobních údajů, je třeba konstatovat, že i jiný požadavek na poskytnutí otisku prstu, než je shromažďování osobních údajů ve smyslu § 4 písm. f) citovaného zákona, představuje zásah do osobní integrity fyzické osoby, o jehož oprávněnosti by v případě sporu musel rozhodovat soud.

Odůvodnění

Záměr zaměstnavatele na trvalé ukládání biometrických údajů, například samotných scanů či snímků otisků prstů, často zpracovávaných společně s dalšími identifikačními údaji zaměstnanců v informačním systému zaměstnavatele v podobě, která umožňuje tyto informace dále zpracovávat, je zpracováním citlivých údajů, které je možné jen za podmínek stanovených § 9 zákona o ochraně osobních údajů, tedy buď s výslovným souhlasem subjektu údajů podle § 9 písm. a), nebo bez tohoto souhlasu za podmínek dále tímto ustanovením stanovených.

Přístupové systémy

Pokud se jedná o možnosti využití výjimky v § 9 písm. b) až i) zákona o ochraně osobních údajů pro zpracovávání biometrických údajů zaměstnanců, dá se využít toto ustanovení jen velmi omezeně. Z hlediska zákona o ochraně osobních údajů jde v tomto případě zejména o zpracování citlivých údajů, které je nezbytné pro dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovního práva a zaměstnanosti, stanovené zvláštním zákonem ve smyslu § 9 písm. d), a dále se může jednat o zpracování nezbytné pro zajištění a uplatnění právních nároků ve smyslu § 9 písm. h), když tato možnost vyplývá ze zvláštních právních předpisů.

Z hlediska objektové bezpečnosti stanoví použití biometrické identifikace výslovně pouze vyhláška č. 144/1997 Sb., o fyzické ochraně jaderných materiálů a jaderných zařízení a o jejich zařazování do jednotlivých kategorií, vydaná k provedení zákona č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů. Tato vyhláška v § 8 odst. 2 stanoví: „Každý, kdo je oprávněn vstupovat do střeženého, chráněného a vnitřního prostoru, je vybaven identifikační kartou umožňující automatickou kontrolu a registraci vstupu. Pro kontrolu vstupu osob se minimálně při vstupu do střeženého prostoru zařízení s jaderně energetickými reaktory použije biometrické identifikace (např. geometrie ruky, otisk prstů). Počet osob vstupujících do těchto prostorů se omezuje na nezbytně nutný počet. Aktuální databáze vstupů je dostupná jeden měsíc a zajišťuje se její archivace jeden rok.“

Použití systémů využívajících biometrických znaků, které však nemusejí být založeny na vyhledávání biometrických údajů v databázi za tímto účelem vytvořené, tedy zpracování citlivých údajů ve smyslu zákona o ochraně osobních údajů, může být důvodné i v jiných případech souvisejících s pracovněprávními vztahy. Může jít zejména o přístupové systémy používané z hlediska fyzické bezpečnosti podle § 24 – 33 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, jako technického prostředku pro kontrolu vstupu ve smyslu § 30 odst. 1 písm. b) tohoto zákona. Podrobnosti upravují vyhlášky Národního bezpečnostního úřadu (NBÚ).

V praxi však u přístupových systémů, kde zajištění bezpečnosti zpracováním citlivých biometrických údajů není stanoveno zvláštním zákonem nebo spojeno se zvláštním zákonem předvídanou prováděcí vyhláškou, lze biometrické identifikace s vyhledáváním biometrických údajů v databázi použít jen s výslovným souhlasem jejich nositele podle § 9 písm. a) zákona o ochraně osobních údajů. Současně musejí být dodrženy všechny ostatní povinnosti správce podle zákona o ochraně osobních údajů, zejména § 10. V přístupových systémech by v návaznosti na uvedené mělo vždy platit pravidlo, že jde o mimořádné opatření kdy, kromě ze zvláštního zákona vyplývající povinnosti zajistit bezpečnost přístupu, se zpravidla zpracovávají biometrické údaje omezeného okruhu oprávněných osob, na rozdíl od plošného zpracování biometrických údajů všech zaměstnanců v docházkových systémech.

Docházkové systémy

Podle přístupu ÚOOÚ k této problematice deklarovaného ve výroční zprávě za rok 2007 i v odpovědích na četné dotazy veřejnosti k této problematice nelze použití systémů, v jejichž paměti dochází k uchovávání biometrických údajů v podobě, která umožňuje jejich další zpracování, považovat za nezbytné pro jakoukoliv běžnou evidenci, např. pro evidenci docházky do zaměstnání. Zpracování biometrických údajů zejména v docházkových systémech lze proto posuzovat jako nepřiměřené ve vztahu k rozsahu a účelu zpracovávání, který je povinen stanovit každý správce. V důsledku toho může docházet k porušení povinnosti podle § 5 odst. 1 písm. d) zákona o ochraně osobních údajů, tedy shromažďování osobních údajů neodpovídajících stanovenému účelu a v rozsahu nikoli nezbytném pro naplnění stanoveného účelu, a to i v případě existence výslovného souhlasu subjektu údajů. Na takový postup zaměstnavatele lze podat ÚOOÚ stížnost. Ani splnění oznamovací povinnosti správce podle § 16 problém zaměstnavatele neřeší, protože takové zpracování by nemohlo být ve smyslu § 17 odst. 2 povoleno. Obdobný přístup zaujímá většina úřadů na ochranu dat států Evropské unie.

Problematice zpracování biometrických dat se věnuje Stanovisko č. 3/2012 k vývoji biometrických technologií, které přijala Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená v rámci Evropské komise podle článku 29 směrnice 95/46/ES Evropského parlamentu a Rady (Working Party - WP29).[1]

Prvním podstatným hlediskem je, zda dochází k uchovávání úplných biometrických údajů, nebo zda systém vybírá z úplných biometrických údajů některé rysy specifické pro jednotlivce tak, aby vytvořil biometrickou šablonu, která je redukcí úplného biometrického obrazu. Je žádoucí, aby šablony byly před uložením v systému zpracovávány matematickými operacemi (kódování,

[1] Stanovisko revidovalo a fakticky aktualizovalo předchozí dokument skupiny WP29, Pracovní dokument o biometrii, z 1. srpna 2003.

algoritmy nebo hash funkce) tak, aby nebyly volně čitelné nebo zpětně rekonstruovatelné. Důležité přitom je, že různé systémy mají různé způsoby bezpečného převodu šablony otisku prstů do číselného vyjádření, které je uloženo v systému. Nelze proto říci, že určité takto získané číselné vyjádření je pro subjekt údajů ve všech systémech jednoznačné. Zpracování takovýchto číselných vyjádření šablon tedy nelze posuzovat jako zpracování biometrických údajů.[2]

Jiná situace by ovšem nastala v případě, kdy by existoval pouze jediný způsob převodu, a tudíž by každý subjekt měl ve všech těchto systémech jedinou hodnotu.

Jestliže dojde např. při použití jednosměrného hashování k vytvoření číselného údaje, jehož zpětná rekonstrukce na biometrický údaj není možná, nelze již tento údaj považovat za biometrický a využití takového systému může být v určitých případech přípustné, a to při naplnění povinností správce podle § 5 odst. 1 a dále některé z podmínek § 5 odst. 2 písm. a), b) nebo e) zákona o ochraně osobních údajů i bez souhlasu subjektu údajů, protože nedochází k uchovávání citlivého údaje.[3]

Pro další zpracování údajů o docházce do zaměstnání za účelem plnění práv a povinností vyplývajících z pracovněprávních vztahů je v tom případě aplikovatelná i výjimka áz oznamovací povinnosti podle § 18 odst. 1 písm. b) zákona o ochraně osobních údajů.[4] Dalším důležitým hlediskem je, zda je použitý systém založen na autentizaci (verifikaci) fyzické osoby, nebo na identifikaci subjektu údajů v databázi, v níž jsou uchovávány osobní údaje i dalších subjektů údajů. Autentizační (verifikační) systém pouze ověřuje totožnost fyzické osoby porovnáním údajů 1:1. Při identifikaci systém rozpoznává jednotlivce odlišením od ostatních osob, tedy výběrem jednoho z možných případů.

Plné biometrické údaje nebo biometrické šablony tedy mohou být uchovávány buď pouze v paměti biometrického zařízení nebo v centrální databázi, případně u některých systémů na optických, nebo čipových kartách, které uživatelům umožňují nosit je při sobě jako identifikační prostředek.

Aplikace pro autentizaci (verifikaci) se často používají pro různé úkoly ve zcela odlišných oblastech a v odpovědnosti celé řady různých subjektů. Pro účely autentizace/verifikace není nezbytné uchovávat osobní údaje v databázi, postačuje je uchovávat decentralizovaně. Z hlediska zásady proporcionality jsou jednoznačně upřednostňovány biometrické aplikace, které nezpracovávají data získaná z tělesných stop nevědomě zanechaných jednotlivci a u kterých nejsou data uchovávána v centralizovaném systému.

Povinnostem stanoveným zákonem o ochraně osobních údajů pro zpracování citlivých údajů proto nemusí podléhat systém, který pracuje pouze na principech autentizace, tedy metody kontroly příchodu a odchodu zaměstnance, kdy čtecí zařízení, do kterého otisk prstu vkládá na

[2] Uvedené vyjádření je již v současnosti nutno s ohledem na technologický vývoj považovat za neúplné a nelze jej vztáhnout na všechny moderní biometrické systémy.

[3] Změna s účinností od 25. května 2018. Čl. 9 obecného nařízení považuje zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby za zpracování zvláštní kategorie osobních údajů.

[4] Změna s účinností od 25. května 2018. Obecné nařízení již neukládá povinnost oznamovat zamýšlené zpracování osobních údajů. U zpracování zvláštních kategorií údajů lze však předpokládat povinnosti aplikovat některé z dalších mechanismů a nástrojů ochrany údajů.
Více v sekci Obecné nařízení EU (GDPR):
https://www.uoou.cz/obecne%2Dnarizeni%2Deu%2Dgdpr/ds-3938/p1=3938

základě požadavku zaměstnavatele na kontrolu docházky sám zaměstnanec, porovnává údaje 1:1.

Při příchodu na pracoviště nebo odchodu z něj je po zvolení osobního čísla zaměstnance vložený otisk s přiložením příslušného prstu použit pouze pro ověření totožnosti subjektu údajů. Do dalšího zpracování osobních údajů snímek otisku prstu nebo dlaně však již nevstupuje a systém jeho další zpracování ani neumožňuje. Osobní číslo zaměstnance je v takovémto docházkovém systému druhým identifikátorem, který však může být zaměstnavatelem zpracováván v souladu se zákonem o ochraně osobních údajů i bez souhlasu subjektu údajů ve smyslu § 5 odst. 2 písm. e).[5]

Rozhodné pro posouzení, zda jde o z hlediska zásad ochrany přípustnou autentizaci, nebo o identifikaci, kterou je třeba podrobit přísné regulaci je, zda účelem použití otisku prstu, je pouze ověření totožnosti porovnáním s přiloženým prstem ruky, nebo v systému dochází v návaznosti na přiložení ruky nebo její části (případně karty s RFID čipem, který již tyto informace obsahuje) k vyhledávání a porovnávání informací s údajem uchovávaným v databázi biometrických údajů, která musí být vždy považována za zpracování citlivých údajů, podléhající režimu § 9 zákona o ochraně osobních údajů.

Zaměstnavatel musí důsledně splnit nejen shora uvedené povinnosti podle § 5, 9 a 16, ale dále také informační povinnost podle § 11 a povinnosti při zabezpečení osobních údajů podle § 13 - 15 zákona o ochraně osobních údajů, jestliže by šlo o shromažďování citlivých údajů umožňující jejich další zpracování v databázi, ale v případě jakéhokoliv systému založeného na použití biometrických znaků i informační povinnost o základních pracovních podmínkách a jejich změnách podle § 279 zákoníku práce, neboť může nastat situace, kdy zaměstnanec výlučně vstupní otisk prstu pro ověření totožnosti neposkytne z obavy z jeho možného zneužití.

Závěr

Je třeba zdůraznit, že zejména biometriku založenou na zpracování citlivých údajů v centrální databázi lze v pracovněprávních vztazích využívat jen ve výjimečných situacích. Připomenout je třeba i povinnosti zaměstnavatele podle § 316 zákoníku práce, týkající se zákazu otevřeného i skrytého sledování zaměstnance. Toho by se zaměstnavatel mohl dopustit, pokud by pro kontrolu docházky přípustný systém biometrické autentizace využíval pro kontrolu pohybu zaměstnance na pracovišti nad rámec evidence přítomnosti zaměstnance na pracovišti podle § 96 odst. 1 písm. a) zákoníku práce.

Zaměstnancům, kteří mají pochybnosti o oprávněnosti požadavku zaměstnavatele na poskytnutí otisku prstu, ÚOOÚ doporučuje využít práva, které dává zákon o ochraně osobních údajů v § 21: Požádat zaměstnavatele o vysvětlení, na jakém základě systém funguje. V případě, že by šlo o systém založený na zpracování biometrických údajů jejich vyhledáváním v databázi, nemusejí k tomu dávat souhlas a mohou se s podnětem obrátit na ÚOOÚ.

[5] Změna s účinností od 25. května 2018. Čl. 9 obecného nařízení považuje zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby za zpracování zvláštní kategorie osobních údajů.

III. SDĚLENÍ ÚŘADU

K novele zákona o trestní odpovědnosti právnických osob

Dne 1. prosince 2016 nabyl účinnosti zákon č. 183/2016 Sb., kterým se mění zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim. Úřad pro ochranu osobních údajů informuje, že tato úprava má dopad do ochrany osobních údajů.

V § 7 zákona o trestní odpovědnosti právnických osob mění výčet trestných činů, jichž se může dopustit právnická osoba, tj. pozitivní výčet, na výčet trestných činů, jichž se právnická osoba dopustit nemůže, tj. negativní výčet. Týká se to i § 180 nového trestního zákoníku, neoprávněné nakládání s osobními údaji, který doposud trestným činem, jehož se právnická osoba mohla dopustit, nebyl.

§ 180

Neoprávněné nakládání s osobními údaji

(1) Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.

(3) Odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) spáchá-li takový čin tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem,

c) způsobí-li takovým činem značnou škodu, nebo

d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

ÚOOÚ ke schválení novely zákona o inspekci práce

V sobotu 29. července vstoupila v účinnost novela zákona o zaměstnanosti. Její součástí je i článek IV, který mění zákon o inspekci práce.

Podstatou novely č. 206/2017 Sb., kterou se mění zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a další související zákony, je zavedení správního trestání porušení § 316 nového zákoníku práce třemi skutkovými podstatami:

a) narušení soukromí zaměstnance,
b) neinformování zaměstnance o kontrole,
c) vyžadování nedovolených informací od zaměstnance.

Trest za prostřední přestupek je až sto tisíc korun. Za ostatní dva až jeden milion korun.

Procesní novinkou těchto deliktů je, že je nebude stíhat Úřad pro ochranu osobních údajů (ÚOOÚ), ale Státní úřad inspekce práce (SÚIP). Důvodem je, že se nejedná o porušení ochrany osobních údajů, ale o zásah do soukromí zaměstnance, kde se stát touto novelou rozhodl, že soukromoprávní ochrana zaměstnance, tedy prostřednictvím soudu, nestačí.

ÚOOÚ jednal intenzivně o této novele s Ministerstvem práce a sociálních věcí a SÚIP od ledna 2015. Naši partneři přijali názor ÚOOÚ na neúčelnost veřejnoprávního trestání některých jednání zaměstnavatele a na výši pokuty za méně závažný přestupek. Nyní bude nezbytné dopracovat spolupráci mezi ÚOOÚ a SÚIP tak, aby se oba úřady navzájem informovaly o správních řízeních, která mají dopad na druhý úřad. Cílem je zabránit dvojímu trestání při respektování rozsudku vrchního soudu (T. v P. v. MŽP z 25. 5. 1998, sp. zn. 6 A 168/95, SJS 626, Soudní judikatura 3/2000, p. 195, ASPI 19835CZ) a kontrolního řádu, ale přitom napravit trestuhodné chování.

K DIČ na účtenkách EET

V souvislosti se zahájením elektronické evidence tržeb podle zákona č. 112/2016 Sb., o evidenci tržeb se množí dotazy podnikatelů na uvádění daňového identifikačního čísla na vydávaných účtenkách, v jehož důsledku bude docházet ke zpřístupňování jejich rodných čísel v mnohem větším rozsahu, než tomu bylo v souvislosti s dosavadní povinností uvádět daňové identifikační číslo.

Dle ustanovení § 20 odst. 1 písm. b) zákona č. 112/2016 Sb., zákona o evidenci tržeb, je nyní poplatník povinen uvádět své daňové identifikační číslo na účtence, vydávané tomu, od koho evidovaná tržba plyne. Tedy každému zákazníkovi, který může s účtenkou jako dokumentem dále disponovat. Konstrukce daňového identifikačního čísla na základě rodného čísla je stanovena v § 130 odst. 3 zákona č. 280/2009 Sb., daňový řád. Na základě daňového řádu a zákona o evidenci tržeb tak bude docházet k dalšímu zpřístupňování rodných čísel podnikatelů.

Na velkou problematičnost využití rodného čísla v rámci daňového identifikačního čísla Úřad pro ochranu osobních údajů již v minulosti upozorňoval, nemá však kompetenci, aby mohl zákonný podklad pro stávající praxi používání rodných čísel změnit.

Současně je třeba upozornit, že ten, kdo účtenku obdrží, nemůže s takto získaným rodným číslem libovolně zacházet. Pokud by s ním dále neoprávněně nakládal nebo číslo neoprávněně využíval, dopustil by se přestupku podle zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech.

V poslední době Úřad pro ochranu osobních údajů obdržel větší množství nesouhlasných podnětů namířených proti takto nastavené zákonné úpravě. Zde je nutno upozornit, že v této věci je třeba obracet se na gestora zákona, Ministerstvo financí, a další subjekty, které mají přímý vliv na legislativní proces.

Ke zpracování osobních údajů při využívání elektronických karet ve veřejné dopravě

„Inteligentní“ elektronické karty (vybavené čipem RFID, magnetickou páskou, apod.) mohou být současně používány v různých službách k různým účelům a osobní údaje spojené s jejich užíváním mohou být dostupné většímu počtu osob a organizací. Karty mohou sloužit k monitorování chování jednotlivých uživatelů a zlepšování podmínek služeb, příp. pro marketingové účely, vč. využívání údajů o místu využívání karet, tj. také o místu pobytu fyzických osob. Různorodost jednotlivých účelů zpracování údajů klade na správce a zpracovatele velký nárok na technická a procedurální opatření na ochranu soukromí a osobních údajů zákazníků.
Úřad pro ochranu osobních údajů upozorňuje na níže uvedené zásady pro provoz elektronických karet v dopravě, neboť se v poslední době více setkával s dotazy veřejnosti na používání elektronických karet ve veřejné hromadné dopravě.
Uvedenou problematikou se již zabývala pracovní skupina WP29 a Evropská komise nechala pro tuto oblast zpracovat expertní studii Study on Public Transport Smartcards.

Dopravní karty a anonymita
Dopravní společnosti jako správci údajů jsou oprávněny zpracovávat osobní údaje primárně jen pro účely přepravní smlouvy a proto při využívání inteligentních karet musí zohlednit situace, kdy zákaznicí své karty nehodlají využívat jinak než pro veřejnou hromadnou dopravu. Informační systémy dopravních společností měly být navrženy a realizovány tak, aby sladily právo na volný pohyb osob s požadavky na efektivní veřejnou dopravu. Organizace pro veřejnou dopravu a dopravní společnosti musí nabízet alternativní způsoby, aby zákazníci mohli cestovat anonymně a bez zbytečných překážek, např. prostřednictvím zaplacení v hotovosti nebo anonymního předprodeje. Informační systémy dopravních podniků by tedy měly být navrženy a realizovány pomocí přednostního využívání anonymních dat. Pokud není v elektronických systémech možno anonymitu zajistit, neboť se používá (přímo či nepřímo) identifikovatelná informace, měla by být uložena nejkratší možnou dobu a poté automaticky vymazána.

Informování zákazníků
Nejen dopravní společnosti, ale také další organizace poskytující služby spojené s využíváním karet musí poskytnout subjektům údajů jednoznačné informace o zpracování osobních údajů. V systémech předprodejů služeb musí být jasně vysvětleny konkrétní účely zpracování údajů požadované jednotlivými správci (poskytovateli služeb) a uvedeno, jaké druhy osobních informací jsou o dotčených osobách shromažďovány a ukládány a jak jsou tyto informace používány.

Použití dopravních karet pro jiné účely
Vedle dopravního podniku mohou údaje spojené s využíváním karty zpracovávat pro další služby soukromé společnosti i městské a veřejné organizace. Z hlediska podmínek pro zpracování osobních údajů je nutno odlišit účel zpracování údajů dopravním podnikem jako správcem údajů pro přepravní smlouvu a další účely zpracování jinými správci, s využitím karty jako platebního či autentizačního prostředku.

Pražská karta Lítačka
Výše uvedené přístupy připomenul Úřad pro ochranu osobních údajů v rámci poskytnuté konzultace k novému systému využívanému pro pražskou integrovanou dopravu, používajícímu elektronickou kartu Lítačka, také k obměně dosavadní karty Opencard. Základním východiskem jednání bylo, že papírové i elektronické kupony pro veřejnou dopravu by měly být vydávány za, z hlediska ochrany osobních údajů, srovnatelných podmínek. Po uskutečněné konzultaci provozovatelé systému výše uvedená doporučení ÚOOÚ přijali a potvrdili, že systém je po technické stránce připraven vydávat elektronické karty bez následné evidence osobních údajů. Od letošního roku by tedy měly být upraveny podmínky pro vydávání a využívání karet se zahrnutím karty bez evidence, na jejíž používání si veřejnost již v minulosti zvykla.

K centrálnímu registru dlužníků České republiky (CERD)

Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“) varuje před činností provozovatele registru „Centrální registr dlužníků České republiky“ (CERD), který anoncuje vydávání za úplatu potvrzení o bezdlužnosti. Přes varování státních orgánů, finančních institucí i řady odborníků také v minulém roce lidé platili za potvrzení o bezdlužnosti, aniž by se seznámili s podmínkami nabízených služeb, přičemž následně zjistili, že vydané potvrzení o bezdlužnosti není státními úřady ani finančními institucemi uznáváno, resp. neobsahuje relevantní informace vzhledem k tomu, že CERD není zapojen do legálních dlužnických registrů, které mohou být na základě právních předpisů vedeny.
ÚOOÚ sděluje, že s ohledem na to, že provozovatel registru je usídlen mimo území EU, je možnost účinné kontroly a vymáhání opatření prostřednictvím zákona o ochraně osobních údajů v podstatě nemožná.
ÚOOÚ upozorňuje, že zákony České republiky neumožňují provozovat žádný centrální registr dlužníků ve smyslu CERD anoncovaným, z něhož by bylo možno vydávat obecně platné potvrzení o bezdlužnosti, navíc na základě sdružování informací z různých státních a soukromých registrů. ÚOOÚ doporučuje, aby se lidé v případě řešení dluhů a insolvence obraceli výlučně na veřejné databáze, jejichž činnost je stanovena zákonem (insolvenční rejstřík), nebo na takové registry, jejichž serióznost věrohodně potvrzují bankovní instituce a významní poskytovatelé úvěrů.

Oznamovací povinnost veterinárních lékařů

Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“) obdržel dotaz v souvislosti s oznamovací povinností veterinárních lékařů.

Podle § 16 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, je ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování podle tohoto zákona, s výjimkou zpracování uvedených v § 18, povinen tuto skutečnost písemně oznámit ÚOOÚ před zpracováváním osobních údajů.

Podle § 18 odst. 1 písm. b) zákona o ochraně osobních údajů se oznamovací povinnost podle § 16 nevztahuje na zpracování osobních údajů, které správci ukládá zvláštní zákon nebo je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona.

Z uvedeného vyplývá, že pokud veterinární lékař zpracovává osobní údaje zaměstnanců nezbytné z pohledu pracovně právního vztahu, např. pro plnění povinností plynoucích ze zákonů z oblasti sociálního zabezpečení, zdravotního pojištění, zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů atp., jedná se o postup v režimu ustanovení § 18 - oznamovací povinnost podle § 16 zákona o ochraně osobních údajů se na něj nevztahuje.

Obdobnou úpravu lze aplikovat i na zpracování osobních údajů fyzických osob v souvislosti s evidencí nezbytnou pro plnění povinností stanovených zvláštními právními předpisy, např. zákony č. 166/1999 Sb., o veterinární péči a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, č. 154/2000 Sb., o šlechtění, plemenitbě a evidenci hospodářských zvířat a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, č. 167/1998 Sb., o návykových látkách a o změně některých dalších zákonů, ve znění pozdějších předpisů, č. 381/1991 Sb., o Komoře veterinárních lékařů České republiky, ve znění pozdějších předpisů atp.

Rovněž zpracování nezbytných osobních údajů klientů např. v souvislosti s dodáním objednaného zboží, plněním povinností vyplývajících např. ze zákonů z oblasti účetního výkaznictví, reklamačního řízení atp., nepodléhá oznamovací povinnosti podle § 16 - je v režimu § 18 odst. 1 písm. b) zákona o ochraně osobních údajů.

25. května 2018 však nabude účinnosti nařízení Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „nařízení“), které nahradí dosud platný zákon o ochraně osobních údajů. Oznamovací povinnost a registrace zpracování ve smyslu ustanovení §§ 16 až 19 a 35 zákona o ochraně osobních údajů pozbude platnosti.

Zároveň je nutné uvést na pravou míru informace o povinnosti zabezpečení osobních údajů formou šifrování či anonymizace. Zákon o ochraně osobních údajů upravuje v § 13 povinnost zabezpečit osobní údaje, přičemž se nevyžaduje jako podmínka jejich šifrování či anonymizace. To není ani podmínkou Obecného nařízení. Zabezpečení osobních údajů musí být v rozsahu s kontextem, účelem a rozsahu zpracovávaných osobních údajů.

U veterinárních lékařů nelze předpokládat, že by zpracovávali rizikové osobní údaje a tudíž povinnost zabezpečení by měla být v rozumné míře odpovídající charakteru osobních údajů.

Ke zveřejňování záběrů zákroků strážníků obecní (městské) policie

Pořizování záběrů zákroků strážníků obecní policie, je-li to potřebné pro plnění jejich úkolů, je zpracováním osobních údajů v rámci zákonného postupu, který je předvídán v § 24b odst. 1 zákona č. 553/1991 Sb., o obecní policii. Pořízený záznam může být použit jako důkaz, že byl spáchán trestný čin, přestupek nebo jiný správní delikt. Zveřejnění pořízených záznamů, tedy zpřístupnění záznamů široké veřejnosti, však může představovat porušení povinností při

zpracování osobních údajů, případně zásah do práv na ochranu osobnosti, tedy práva upraveného především občanským zákoníkem.

Zásadní z hlediska posouzení legálnosti každého zpracování osobních údajů orgánem veřejné moci je v prvé řadě jeho zákonem vymezený účel. Podle § 24b odst. 1 zákona č. 553/1991 je obecní policie oprávněna, je-li to potřebné pro plnění jejích úkolů podle tohoto nebo jiného zákona, pořizovat zvukové, obrazové nebo jiné záznamy z míst veřejně přístupných, popřípadě též zvukové, obrazové nebo jiné záznamy o průběhu zákroku nebo úkonu. Primárním účelem pořizování záznamů zákroků a úkonů strážníků tak musí být, jak je výše uvedeno, zajištění případných důkazů, že byl spáchán trestný čin, přestupek nebo jiný správní delikt ve smyslu § 10 zákona č. 553/1991 Sb.

Při své dozorové činnosti se přitom ÚOOÚ setkává na straně obecní policie s praxí zveřejňování videozáznamů (typicky prostřednictvím serverů jako YouTube), které je prováděno s úmyslem podílet se na prevenci kriminality, případně pouze upozornit na jednání, které je v rozporu s obecně akceptovanými normami chování (typicky opilost na veřejnosti), a také s úmyslem informovat veřejnost o činnosti obecní policie. Je nepochybné, že obecní policie je oprávněna působit v oblasti prevence kriminality a stejně tak informovat o své činnosti. Jako orgán veřejné moci však při plnění těchto svých úkolů musí důsledně dbát základní zásady, vyplývající z ústavního pořádku České republiky, tedy, že uplatňovat veřejnou moc lze jen v případech a v mezích stanovených zákonem, a to způsobem, který zákon stanoví.

V případech, kterými se ÚOOÚ zabýval, se ukázalo, že zveřejňování pořízených nahrávek, tedy osobních údajů těch subjektů údajů, vůči kterým obecní policie činila určité úkony, nebylo ani pro jeden z výše uvedených účelů (prevence či informování) nezbytné. Ze strany obecní policie současně nebylo objasněno, jakým způsobem může zveřejnění audiovizuálního záznamu zachycujícího jednání identifikovatelných osob přispět k prevenci kriminality, ani proč by měla být veřejnost informována o činnosti obecní policie tímto způsobem. Zveřejněné videozáznamy tak sloužily ve výsledku především jako zdroj pobavení pro širokou veřejnost. Z pohledu ochrany soukromí a ochrany osobních údajů je přitom zveřejňování audiovizuálních záznamů ve srovnání s jinými formami přenosu zpráv, např. písemným sdělením, obvykle spojeno s vyšší mírou zásahu do práv subjektů údajů. V audiovizuálním záznamu je totiž základní sdělení vždy neoddělitelně spojeno s dalšími údaji (např. oblečení, gesta, vyjadřování snímaných osob, okolní prostředí anebo komentáře strážníků či dalších osob), které pak obvykle vedou k tomu, že zachycené osoby mohou být s jejich pomocí identifikovány.

Důsledná anonymizace záznamů je proto velmi obtížná, ne-li nemožná, neboť s ohledem na jedinečný charakter jednání a vystupování osob ve spojení s konkrétními okolnostmi daného případu, povede vždy k tomu, že osobu zachycenou na záznamu lze poznat. V této souvislosti je podstatné, že k zásahu do právem chráněného zájmu na ochranu soukromí dojde i v případě, kdy je osoba rozpoznána jen v omezeném okruhu svých rodinných příslušníků či známých.

Je proto třeba důsledně odlišit situaci, kdy je záznam strážníky obecní policie pořizován např. z důvodu zajištění nezbytného důkazního materiálu, anebo k jejich vlastní ochraně. V takovém případě jsou občané povinni pořizování zvukového, obrazového nebo jiného záznamu o průběhu zákroku či úkonu strážníka strpět. Zcela jinou situací je však následné medializování případů.

V tomto směru je zároveň nutno uvést, že k zásahu do práv nedochází v souvislosti se

zveřejněním záznamů pouze ve vztahu k osobě, se kterou strážníci obecní policie jednají, ale například i vůči přítomným nezletilým dětem.

ÚOOÚ proto na základě poznatků ze své dozorové činnosti považuje za nepřijatelné, aby v oblasti výkonu veřejné moci, tedy při zajišťování veřejného pořádku a bezpečnosti, byly mimo výslovně zákonem stanovené případy zveřejňovány záznamy soukromých osob. Záznamy veřejně činných osob (zejména samotných strážníků) pro účel prevence či propagace činnosti obecní policie veřejnosti zpravidla zpřístupnit lze.

V případě, že přesto dojde ke zveřejnění osobních údajů, jímž se některá ze zachycených osob bude cítit dotčena, pak lze v prvé řadě doporučit, aby se obrátily na příslušnou obecní policii s žádostí o odstranění příslušného záznamu podle § 21 odst. 1 písm. b) zákona o ochraně osobních údajů, dle kterého je právem každého subjektu údajů, který zjistí nebo se domnívá, že dochází ke zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života nebo v rozporu se zákonem, požadovat, aby správce nebo zpracovatel takto vzniklý stav odstranil.

Postup při vydávání osvědčení o ochraně osobních údajů podle GDPR

Přijetím nařízení EP a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, se **do právního řádu zavádí mechanismy pro vydávání pečetí, známek a osvědčení o ochraně údajů**, které budou prokazovat soulad s nařízením (čl. 42 a 43) o ochraně osobních údajů.

Získání tohoto osvědčení je dobrovolným rozhodnutím správce osobních údajů, nikoli jeho novou povinností.

Vydávat osvědčení o ochraně údajů může podle tohoto nařízení subjekt, který je pro tuto činnost akreditován:

- přímo příslušným dozorovým úřadem (v případě České republiky je to Úřad pro ochranu osobních údajů),
- vnitrostátním akreditačním orgánem, kterým je Český institut pro akreditaci, o.p.s. (v souladu s nařízením Evropského parlamentu a Rady (ES) 2008/765 a v souladu s normou ČSN EN ISO/IEC 17065 a požadavky stanovenými příslušným dozorovým úřadem),
- lze využít i kombinace obou výše uvedených postupů.

ÚOOÚ se rozhodl pro Český institut pro akreditaci. Důvodem jsou zejména:

- jeho dlouholeté zkušenosti s touto činností,
- jeho nezávislost,
- možnost celoevropského uznávání takto vydaných osvědčení.

ÚOOÚ již zahájil jednání o spolupráci s Českým institutem pro akreditaci. **Pro vytvoření systému vydávání osvědčení o ochraně osobních údajů je podle nařízení nezbytné vytvořit dva základní dokumenty:**
- Kritéria pro akreditaci subjektů pro vydávání osvědčení,
- Kritéria pro vydávání osvědčení.

Příprava obou dokumentů bude probíhat následujícím postupem: Návrh kritérií připravených ÚOOÚ bude konzultován a upraven na základě připomínek a návrhů uplatněných v rámci úzké pracovní skupiny. Ta bude k tomuto účelu zřízena ÚOOÚ a bude složená ze subjektů se zkušenostmi v oblasti vydávání osvědčení/certifikací a v oblasti praktické ochrany osobních údajů. Výsledný text bude poté předložen k široké diskusi na webových stránkách ÚOOÚ.

Subjektům, které projeví zasláním svých kontaktních údajů na adresu certifikace@uoou.cz o problematiku hlubší zájem, budou materiály k připomínkám a návrhům úprav textu zasílány přímo.

Shrnutí stanovisek Pracovní skupiny WP29:

Stanovisko č. 01/2017 k návrhu ePrivacy nařízení

Shrnutí

Pracovní skupina WP29 v dubnu 2017 schválila stanovisko k revizi směrnice 2002/58/ES o soukromí a elektronických komunikacích. Návrh nového nařízení, které předložila Evropská komise již v lednu 2017, by měl poskytnout uživatelům elektronických komunikací vysokou úroveň ochrany soukromí a rovné podmínky pro všechny účastníky na trhu.

WP29 ve svém stanovisku kladně ohodnotila zvolenou formu nařízení namísto směrnice, dojde tak k souladu s GDPR. Rovněž ocenila rozhodnutí rozšířit oblast působnosti na tzv. nové komunikační služby „Over-the-Top" (OTT) typu Skype, WhatsApp aj., které budou muset splňovat stejná kritéria jako telefonní operátoři, co se týče důvěrnosti komunikace uživatelů. Stejně tak WP29 ocenila snahu o modernizaci pravidel, která by byla aplikovatelná na sledování v online světě. Zástupci skupiny WP29 přivítali, že by se měla zásada důvěrnosti zakotvená v tomto nařízení vztahovat rovněž na přenos komunikace mezi stroji (M2M).

Zároveň pracovní skupina vyjádřila znepokojení ohledně čtyř bodů. Sledování Wi-Fi, analýzu obsahu a metadat, tzv. tracking walls a standardní nastavení ochrany soukromí (privacy by default) u koncového zařízení a softwaru.

Pokud tyto body zůstanou v textu nezměněny, mohly by snížit ochranu, kterou má zaručit GDPR. U sledování Wi-Fi vyzývá WP29 k větší podpoře technických norem mobilních zařízení, aby se mohlo automaticky zamezit sledování uživatelů, aniž by však byli nadměrně zatíženi požadavky na odmítnutí sledování (opt-out).

Obsah a metadata by měla být zpracována se souhlasem všech koncových uživatelů (odesílatele i příjemce) a měla by mít stejnou ochranu. Podle WP29 jsou však v novém návrhu metadata definována příliš úzce. Praxe, kdy je odmítnut přístup k webu či službě, pokud uživatelé neodsouhlasí sledování (tzv. tracking walls) by měla být dle WP29 zakázána. Zástupci WP29 doporučují, aby konečná zařízení a software musela nabízet standartní nastavení ochrany soukromí, která by byla srozumitelná a snadná pro instalaci.

Výbor Evropského parlamentu LIBE, pořádal k ePrivacy slyšení v polovině dubna, kterého se zúčastnili zástupci státní, soukromé i akademické sféry.
Odkaz na směrnici 2002/58/ES o soukromí a elektronických komunikacích.

Pracovní skupina WP29 vydala tři dokumenty k obecnému nařízení o ochraně osobních údajů

WP29 vydala první z řady dokumentů, které mají poskytnout výklad novinek zaváděných obecným nařízením o ochraně osobních údajů. Tři publikované materiály se týkají práva na přenositelnost údajů, pověřenců pro ochranu osobních údajů a problematiky určování tzv. vedoucího dozorového orgánu v souvislosti s přeshraničním zpracováním osobních údajů. Podrobné informace naleznete v tiskové zprávě WP29.

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: Mgr. Vojtěch Marcín, tel.: 234 665 484
e-mail: vojtech.marcin@uoou.cz
internetová adresa: www.uoou.cz

ISSN: 2336-4742