ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

HLÍDACÍ PES PRO OSOBY ZODPOVĚDNÉ ZA GDPR | 3. ročník | číslo 5 | březen 2021

Co přinesly kontroly ÚOOÚ za druhé pololetí?

Kde odhalil ÚOOÚ největší hříšníky? V jakých případech lze vyžadovat kopii občanského průkazu a kdy už je to nadbytečné? Jak se ÚOOÚ staví k biometrickému podpisu? A za co Úřad uděloval pokuty?

Půl roku uběhlo a opět je zde vaše oblíbená rubrika – **analýza postupu ÚOOÚ v rámci své kontrolní činnosti**. V předchozích dílech Zpravodaje jsme vás informovali o tom, jak ÚOOÚ postupoval v rámci kontrol dodržování GDPR různými subjekty v první polovině roku 2020. Díky znalosti aktuální rozhodovací praxe totiž držíme prst na tepu aktuálnosti výkladu různých povinností, což vám **umožňuje revidovat vaše stávající postupy** tak, aby pokud možno před ÚOOÚ obstály. Pokud víme, na co se ÚOOÚ obvykle ptá a dívá, můžeme se z toho poučit a lépe se na to připravit.

První oblasti, které si rozebereme v tomto článku, budou **finanční služby a pojišťovnictví**, v jejichž rámci se nám jako bumerang vrací **problematika dynamického biometrického podpisu**.

Nevyžádaná obchodní sdělení platí i pro telefonáty

Kopie občanského průkazu

ÚOOÚ se podělil o závěry z celkem čtyř kontrol. Hned první kontrola patří mezi ty, jimž bychom měli věnovat pozornost. Na počátku byl stěžovatel (a následně další čtyři, kteří se k němu nezávisle na něm přidali), jemuž se nelíbilo, že **banka podmiňuje zřízení běžného účtu pořízením kopie občanského průkazu**. Při pořizování kopií banka vyžadovala souhlas se zpracováním osobních údajů, který nebyl podle ÚOOÚ sbírán v souladu s GDPR, a tím pádem mělo dojít k jeho porušení.

Téma kopie osobních dokladů rezonuje v této oblasti poměrně často a pravidelně se setkáváme s různými řešeními v praxi, jako je pouze **částečné nahlédnutí do dokladu, anonymizace některých údajů při skenování**, pouhé opsání identifikačního čísla průkazu a podobně.

Odpověď na to, co je správně, nám ÚOOÚ nedal, to se však pravděpodobně změní, neboť samotný **protokol o kontrole byl napaden námitkami, kterým bylo částečně vyhověno**, a ÚOOÚ zahájil se společností správ-

ní řízení, v jehož rámci se bude muset ke sporným otázkám vyjádřit a poskytnout odůvodnění. S trochou štěstí by tak mohl padnout „závazný“ právní názor, jak k této problematice dlouhodobě přistupovat.

Nabídka služeb bez souhlasu

Další z kontrol v této oblasti skončila již **pokutou ve výši 10 000 korun za porušení zásady zákonnosti, korektnosti a transparentnosti** a taktéž za nedostatky v oblasti právního titulu. Předmětem kontroly byly stížnosti ze strany klientů a potenciálních klientů, kteří byli kontrolovanou osobou **kontaktováni s nabídkou produktů a služeb, aniž k tomu dali souhlas**. Je zajímavé, že kontaktování proběhlo přes telefon. Dlužno dodat, že stále přetrvávající myšlenka, že obejdeme legislativu týkající se zasílání obchodních sdělení jednoduše tím, že místo e-mailu subjektu údajů zavoláme, se tímto ukázala jako lichá.

V tomto případě ale šlo o něco jiného – zjednodušeně totiž **zprostředkovatelé prostě přenesli kontakty z jedné společnosti do druhé**, a tím porušili nejen smlouvu s předchozí společností, ale i GDPR. ÚOOÚ se taktéž vyjádřil k tomu, že v tomto případě **kontrolovaná osoba nedisponovala žádným právním titulem** a takové zpracování nesplňuje definiční znaky nezbytnosti pro splnění oprávněného zájmu kontrolované osoby ani třetí strany.

Široký přístup ÚOOÚ

Třetí z kontrol v této oblasti probíhala na základě kontrolního plánu a podle všeho dopadla dobře, protože kontrolor žádná pochybení neodhalil. Jediné, co je na této kontrole zajímavé, je šíře, s jakou se do ní ÚOOÚ pustil, nebo alespoň jakou práci si dal s tím nás o tomto informovat. V rámci této kontroly totiž ÚOOÚ **prověřil vše od způsobu shromažďování osobních údajů po právní tituly, informování, ukládání cookies**, ale i způsob reagování na požadavky subjektů údajů včetně způsobu zabezpečení osobních údajů a vyhodnocení rizik. ÚOOÚ tak kontroloval nejen informace, ale i smlouvy s dodavateli a další dokumentaci. Lze tak přinejmenším upozornit na to, že záběr kontroly ze strany ÚOOÚ je skutečně velmi široký.

Dynamický biometrický podpis

Poslední kontrola z této oblasti je asi nejzajímavější, protože se týká dynamického biometrického podpisu – tedy tématu, na kterém se odborná veřejnost s ÚOOÚ úplně neshoduje. Tato kontrola byla taktéž zahájena na zákla-

Na co se zaměřuje ÚOOÚ při kontrolách:

- způsob shromažďování osobních údajů
- právní tituly
- informační povinnost
- soubory cookie
- reagování na požadavky subjektů údajů
- zabezpečení osobních údajů
- vyhodnocení rizik
- smlouvy s dodavateli

dě kontrolního plánu, ale oproti předchozímu případu bylo v tomto případě s kontrolovanou osobou **zahájeno správní řízení o uložení opatření k nápravě**, a pravděpodobně bude mít případ dohru i v rámci správního řízení. Z našeho pohledu je to rozhodně dobře, protože důvod, jenž k tomu ÚOOÚ vedl, není po prvním přečtení moc pochopitelný a nápadně se podobá již jednou rozhodnuté věci, která však nebyla před správními soudy dále řešena.

Pokud lze smlouvu podepsat vlastnoručně, biometrický podpis je nadbytečný

Obchodní společnost **využívala pro podpis smluvní dokumentace dynamický biometrický podpis**, přičemž kontrolovaný k tomu uvedl následující: *„Dále bylo konstatováno, že pro účely uzavření a uchování smluvní dokumentace není nezbytné využívat dynamický biometrický podpis, neboť v případě podpisu dokumentů v listinné podobě není také vyžadován a jako dostatečný je pro stanovené účely prostý obraz podpisu klienta na dematerializované smluvní dokumentaci, který je srovnatelný s podpisem smluvní dokumentace v listinné podobě.“*

ÚOOÚ dále uvádí: *„Občanský zákoník ani zvláštní právní úprava tedy vysloveně nevyžadují pro platnost právního jednání v písemné formě dynamický biometrický podpis.“* Na základě toho všeho tak **ÚOOÚ konstatoval, že došlo k porušení zásady minimalizace** dle čl. 5 odst. 1 písm. c) GDPR. Ostatně tento názor pokračuje v dlouhodobém názoru na biometrický podpis, který se krystalicky projevil v rozhodnutí č. j. UOOU-10138/18-8 ze dne 21. března 2019, z něhož pochází i výše uvedená citace.

V čem tedy ÚOOÚ spatřuje problém? K věci se staví tak, že **pokud lze smlouvu podepsat i vlastnoručním podpisem, je podepsání dynamickým biometrickým podpisem nadbytečné**, a tudíž dochází k porušování zásady minimalizace. Bližší argumentaci prozatím neznáme. V tomto případě ÚOOÚ konstatuje, že zahájil navazující řízení, takže je dost možné, že se tato otázka přece jen dostane před soudní přezkum, který by v tom mohl udělat jasno.

Závěr

Kontrolní činnost ÚOOÚ je vždy zajímavá, neboť nám často odpovídá na zásadní otázky, které text GDPR bohužel nezodpoví. Ne vždy však ÚOOÚ rozhoduje tak, jak k tomu přistupuje odborná veřejnost, tudíž **se určitě můžeme těšit na další diskuze týkající se dynamického biometrického podpisu**. V příštím díle se podíváme na kontroly z dalších oblastí, jako je například IT či státní správa.

▪▪▪

Mgr. Josef Bátrla,
advokát v oblasti ICT
www.josefbatrla.cz

Pokuta 251 milionů korun pro Grindr

Norský úřad pro ochranu osobních údajů navrhuje udělit společnosti Grindr pokutu ve výši 251 milionů korun. O co v případu jde? A nakládá seznamovací aplikace s tzv. citlivými údaji?

Norský úřad pro ochranu osobních údajů (Datatilsynet) oznámil, že má v plánu uložit americké společnosti Grindr LLC, provozující seznamovací aplikaci určenou pro členy LGBTQ+ komunity, **pokutu ve výši 100 milionů norských korun** (což v přepočtu činí přibližně 251 milionů korun).

Společnost neoprávněně **sdílela osobní údaje uživatelů seznamovací aplikace se třetími stranami** pro marketingové účely. Společnost Grindr LLC konkrétně sdílela GPS polohu uživatelů seznamovací aplikace, data uvedená v uživatelském profilu a samotný fakt, že dotyčný uživatel využívá seznamovací aplikaci Grindr. Pro takovéto sdílení osobních údajů však společnost potřebuje souhlasy uživatelů, které neměla, respektive **souhlasy udělené uživateli nenaplňovaly požadavky GDPR**. Nebylo je totiž možné považovat za svobodné, konkrétní a informované. Aby uživatelé vůbec mohli aplikaci využívat, museli odsouhlasit celé zásady zpracování osobních údajů, jejichž součástí byla i informace o sdílení jejich osobních údajů se třetími stranami pro marketingové účely. Daná informace navíc nebyla uvedena srozumitelně.

Článek 7 odst. 2 GDPR přitom mluví jednoznačně: „*Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků.*“

Navíc dle norského dozorového úřadu samotný fakt, že určitá osoba je uživatelem aplikace Grindr, která je určená pro členy LGBTQ+ komunity, **vypovídá o sexuální orientaci dané osoby**. Jedná se tudíž o informaci spadající do takzvaných **zvláštních kategorií osobních údajů** (viz čl. 9 GDPR) a je tedy nutné věnovat zvýšenou pozornost tomu, o jaký právní základ je zpracování předmětného osobního údaje opřeno.

Souhlas se musí týkat pouze jednoho konkrétního zpracování

Zatím se nejedná o finální rozhodnutí norského dozorového úřadu. Společnost Grindr LLC měla čas do 15. února 2021, aby se k výše popsanému porušení GDPR vyjádřila. Pokud by úřad nakonec uložil pokutu v navrhované výši, jednalo by se o **doposud nejvyšší pokutu uloženou norským úřadem** pro ochranu osobních údajů.

▪▪▪

JUDr. Andrej Lobotka, Ph.D.
www.smart-law.cz

Klikněte a stáhněte si vzor

Jak si dobře vybrat videokonferenční software?

1. Nejprve si stanovte požadavky, například:

- funkčnost i na mobilních platformách – Android, iOS,
- evidence a monitoring uskutečněných hovorů,
- čekací místnost,
- kvalita přenosu videa,
- vizuální hlasová schránka,
- whiteboard,
- možnost portace telefonních čísel,
- maximální počet účastníků,
- délka hovoru atd.

2. Z pohledu GDPR máte na výběr tři druhy videokonferenčního softwaru:

- systém provozuji sám,
- systém provozuje externí poskytovatel IT služeb,
- online služby (software jako služba).

a) Pokud si vyberete systém provozovaný správcem:

- nemusíte uzavírat zpracovatelskou smlouvu;
- nemusíte uzavírat dohodu dvou samostatných správců;
- data a údaje jsou zpracovávány přesně dle potřeby;
- pouze odpovědná osoba může analyzovat a kontrolovat obsah a rámcová data systému;
- musíte přijmout dostatečná technická a organizační opatření.

b) Pokud si vyberete systém provozovaný dodavatelem:

- musíte uzavřít zpracovatelskou smlouvu;
- státní správa a školy raději vlastní systém a provoz;
- zpracovateli musíte jasně definovat požadavky na zacházení s daty a technická a organizační opatření;
- systém je z podstaty zranitelnější;
- nesete odpovědnost i za chyby zpracovatele;
- software používaný nebo nabízený účastníkům by měl být zkontrolován z hlediska úniku dat – zahrnuje diagnostická a telemetrická data, případně další toky dat;
- musíte provést balanční test (jako minimum).

c) Pokud si vyberete online službu:

- musíte uzavřít smlouvu s poskytovatelem, včetně zpracovatelské smlouvy;
- následně musíte zkontrolovat a případně upravit nastavení hlavní konfigurace (například datových toků, přístupových práv a podobně);
- odpovědná osoba musí zajistit soulad se zásadami ochrany údajů výběrem vhodného poskytovatele, jakož i poskytnout příslušné pokyny poskytovateli služby, a nastavením vlastních opatření;
- musíte revidovat prohlášení o ochraně osobních údajů;
- musíte si dát pozor na přenos dat do třetích zemí – USA (Schrems II – neplatnost Privacy shieldu);
- poskytovatel služby musí nabídnout dostatečné záruky;
- musíte zajistit, aby poskytovatel přijal vhodná technická a organizační opatření;
- dejte si pozor na dceřiné společnosti.

Nová vodítka k **rozpoznávání obličejů**

Co přinesla nová vodítka Rady Evropy k technologii pro rozpoznávání obličejů? Jaká pravidla musíte dodržovat? A na co nesmíte zapomenout, aby bylo využití takových technologií etické?

Rada Evropy zveřejnila koncem ledna 2021 **vodítka k technologii pro rozpoznávání obličejů** (face recognition) ve světle Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat (takzvaná Úmluva č. 108). Co v nich najdeme?

Obecně k úmluvě

Úmluva č. 108 z roku 1981 byla **prvním právně závazným dokumentem s mezinárodním rozměrem v oblasti ochrany osobních údajů**. Česká republika podepsala tuto úmluvu v roce 2000 a o rok později ji také ratifikovala. K příležitosti letošního Dne ochrany osobních údajů byla Radou Evropy vydána deklarace k 40. výročí úmluvy. Deklarace mimo jiné konstatuje, že Úmluva č. 108 je dosud jediným právně závazným nástrojem v oblasti ochrany osobních údajů na globální úrovni. Dále pak obsahuje **výzvu zemím k ratifikování protokolu o změně Úmluvy č. 108**, kterým je dosavadní znění úmluvy modernizováno a přizpůsobeno dnešnímu stupni rozvoje digitálního světa. Neoficiální překlad deklarace Rady Evropy pořízený Úřadem pro ochranu osobních údajů naleznete na webových stránkách Úřadu **zde**.

Vodítka Rady Evropy

Vodítka Rady Evropy k technologii pro rozpoznávání obličejů jsou rozdělena do několika částí, přičemž **každá z nich je věnovaná jiným osobám**:

1. zákonodárným sborům,
2. vývojářům, výrobcům a poskytovatelům služeb technologií pro rozpoznávání obličejů a
3. subjektům používajícím technologie pro rozpoznávání obličejů.

Závěrečná (velmi stručná) **část vodítek je pak věnována právům subjektů údajů**. Vodítka Rady Evropy k technologii pro rozpoznávání obličejů je možné najít na webových stránkách Rady Evropy **zde** (dostupné v anglickém jazyce).

Zákonodárný sbor

Jelikož je Úmluva č. 108 značně obecný dokument, je logické, že hlavním požadavkem kladeným na zákonodárné sbory jednotlivých států je **upřesnit právní rámce pro vývoj, výrobu a následné využívání technologií pro rozpoznávání obličejů**. Je přitom důležité rozlišovat, zda je technologie využívána ve veřejném, nebo soukromém sektoru. Speciální pozornost je nutné věnovat využívání technologií pro rozpoznávání obličejů policejními orgány. Rada Evropy zdůrazňuje, že před samotným zahájením případného legislativního procesu **by měla proběhnout konzultace s odpovědným dozorovým úřadem** (tedy v ČR s Úřadem pro ochranu osobních údajů).

Vývojáři, výrobci a poskytovatelé technologií

Vývojáři, výrobci a poskytovatelé služeb technologií pro rozpoznávání ob-

ličejů by měli respektovat čtyři základní požadavky. V první řadě by měli **klást důraz na kvalitu dat a algoritmu**. Požadavek kvality dat je možné nalézt v čl. 5 Úmluvy č. 108. Budou se tak muset vyvarovat nesprávného označování obličejů, což znamená, že **své technologie budou muset testovat na dostatečně rozmanitých fotografiích mužů a žen** různých barev pleti, odlišné morfologie, všech věkových skupin a z různých úhlů pohledu. Z uvedeného testování budou muset vyvodit závěry – **identifikovat a odstranit chyby v (ne)přesnosti**, a to zejména s ohledem na rozdílnou barvu pleti, věk či pohlaví rozpoznávaných osob. Vývojáři, výrobci a poskytovatelé služeb předmětných technologií se tímto postupem mohou vyhnout nezamýšlené diskriminaci, což je problém, s nímž se při používání této technologie stále potkáváme. Technologie rozpoznávání obličejů navíc **vyžaduje periodické obnovování dat** (fotografií obličejů, které mají být rozpoznány), aby bylo možné trénovat a vylepšovat použitý algoritmus.

Vývojáři, výrobci a poskytovatelé služeb technologií pro rozpoznávání obličejů by měli **klást důraz na použitou technologii – na účinnost použitého algoritmu**. Ta totiž nezávisí jenom na datech, ale i na jiných faktorech, jako je **falešná pozitivita, falešná negativita, výkon v různých světelných podmínkách**, spolehlivost při odvracení obličeje od kamery, dopad zakrytí částí obličeje.

Dále by měli podniknout kroky vedoucí k tomu, aby subjekty používající technologie pro rozpoznávání obličejů **uplatňovaly zásadu transparentnosti a respektovaly soukromí subjektů údajů**, tedy by jim měli například poskytnout pomoc v podobě doporučení, návodů a rad, jak s předmětnou technologií nakládat zodpovědně a zákonně.

Rovněž by měli přijmout konkrétní opatření vedoucí k **zajištění souladu daných technologií se základními zásadami zpracování a ochrany osobních údajů**, například:

- **integrovat ochranu osobních údajů** do designu a architektury technologií pro rozpoznávání obličejů, jakož i do interních IT systémů, a integrovat používání specializovaných nástrojů a postupů, například automatického mazání nezpracovaných (primárních) dat po extrahování biometrických šablon;
- **umožnit určitou úroveň flexibility** těchto technologií, aby mohly prostřednictvím technických ochranných opatření reagovat na zásady účelového omezení, minimalizace osobních údajů a omezení doby uložení osobních údajů;
- **implementovat proces interního přezkumu**, jehož cílem je identifikovat a zmírnit potenciální dopady na práva a svobody osob;
- **začlenit přístup zahrnující ochranu osobních údajů do organizačních postupů**, včetně vyčlenění specializovaného personálu na předmětnou agendu, poskytovat školení zaměstnancům v oblasti zpracování a ochrany osobních údajů a provádět posouzení vlivu na ochranu osobních údajů při vývoji nebo úpravě produktů a služeb pro rozpoznávání obličejů.

Testování technologií musí probíhat na dostatečně rozmanitém vzorku

Subjekty používající technologie

Subjekty používající technologie pro rozpoznávání obličejů by dle Rady Evropy měly dodržovat zásadu zákonnosti a transparentnosti, zásady účelového omezení, minimalizace osobních údajů a omezení doby uložení osobních údajů a zásadu přesnosti. Subjekty dále musí dodržovat zásadu zabezpečení údajů – **musí tedy přijmout odpovídající bezpečnostní opatření proti rizikům**, jako je náhodný nebo neoprávněný přístup k osobním údajům, jejich zničení, ztráta, využití, úprava nebo poskytnutí.

Zároveň je nutné, aby tyto subjekty splnily požadavek čl. 10 Úmluvy č. 108, tedy aby zavedly veškerá vhodná opatření tak, aby splňovaly povinnosti vyplývající z předmětné úmluvy

a byly schopny **doložit, že zpracování údajů, které mají pod kontrolou, je prováděno v souladu s ustanoveními dané úmluvy**. Subjekty používající technologie pro rozpoznávání obličejů by tedy například měly:

- **implementovat transparentní směrnice, zásady, politiky a postupy**, které zajistí, že ochrana práv subjektů údajů bude hlavním principem respektovaným při využívání technologií pro rozpoznávání obličejů;
- **transparentně zveřejňovat zprávy** obsahující informace o tom, jak využívají technologie pro rozpoznávání obličejů;
- **zavést pravidelné tréninky a audity osob**, které jsou odpovědné za zpracování dat v rámci procesů využívajících technologie pro rozpoznávání obličejů;
- **zřídit interní kontrolní výbor**, jenž bude hodnotit a schvalovat všechna zpracování osobních údajů využívajících technologie pro rozpoznávání obličejů;
- **smluvně zajistit třetí strany**, které budou zapojeny do procesů využívajících technologie pro rozpoznávání obličejů.

Při použití těchto technologií jsou v sázce základní práva subjektů údajů

Subjekty využívající technologii rozpoznávání obličejů zároveň musí **prověřit pravděpodobný vliv zamýšleného zpracování údajů na práva a základní svobody** subjektů údajů, a to ještě předtím, než takové zpracování zahájí. V rámci daného posouzení se musí kromě jiného **zaměřit na otázku zákonnosti používání těchto technologií** a zranitelnosti subjektů údajů, dále si pak musí ujasnit, která základní práva jsou v sázce při předmětném biometrickém zpracování. V rámci posouzení musí subjekty zároveň navrhnout zpracování osobních údajů takovým způsobem, aby zabránily riziku či minimalizovaly riziko zásahu do těchto práv a základních svobod. Kromě dodržování zákonných požadavků by se dané subjekty měly umět **vypořádat i s etickou stránkou konkrétní aplikace** předmětné technologie.

■■■

JUDr. Andrej Lobotka, Ph.D.
www.smart-law.cz

ÚOOÚ prověřuje rezervační systémy pro očkování proti covidu

Úřad pro ochranu osobních údajů zahájil kontrolu rezervačního systému pro očkování proti koronaviru. Stalo se tak na základě obdržených stížností na porušování GDPR při zpracování osobních údajů v rámci tohoto systému. Konkrétně mělo docházet k tomu, že čísla pojištěnců, a tedy i rodná čísla, byla sdílena se společností Google. Data se tak dostala do systému Google Analytics, který umožňuje webům sledovat chování uživatelů a tato data využívá k marketingovým účelům. Ministerstvo zdravotnictví a Národní agentura pro komunikační a informační technologie to označila za chybu systému a podala 20. ledna ohlášení porušení zabezpečení. Opatření k nápravě byla již přijata, nyní ÚOOÚ prověřuje, zda byla dostatečná. Při kontrole se Úřad zaměří na posouzení oprávněnosti předávání osobních údajů do USA prostřednictvím souborů cookies, prověření bezpečnostních záruk takového předávání a také plnění informační povinnosti při zpracovávání osobních údajů v rámci rezervačního systému.

Zdroj: ČTK

Elektronický zpravodaj pro pověřence | Vydavatel: Nakladatelství FORUM, s. r. o. | Adresa redakce: Střelničná 1861/8a, 182 00 Praha 8 | Šéfredaktorka: Mgr. Anna Zavadilová | Editorka: Anna Pěkná | Zákaznický servis: Petra Pokojová, office@forum-media.cz, tel.: +420 251 115 576, fax: +420 251 512 422 Jazyková redakce: Bc. Vendula Pazderová | Fotografie: www.bigstockphoto.com | Zlom časopisu: Renata Brtnická | Roční předplatné: 2 490 Kč bez DPH Objednávka předplatného: office@forum-media.cz, fax: +420 251 512 422, informace o předplatném: +420 251 115 576 | Redakční uzávěrka: 1. 3. 2021 Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4, ISSN 2571-1504.