PRO

OCHRANA OSOBNÍCH ÚDAJŮ V PRAXI

Číslo 6/2023, ročník III. Měsíčník SMS - služby s. r. o. www.dpopro.cz

Krásné hřejivé dny, vážení čtenáři!

Ochrana osobních údajů není jeden obor, který by měl nějaké hranice. Prolíná se jakoukoli činností, jakýmkoli odvětvím, osobní údaje zkrátka najdete úplně všude. A kdo to říká? Říkám to já v úvodním rozhovoru červnového a předdovolenkového čísla DPO, který tentokrát nevedu, ale je zcela nezvykle veden se mnou, neboť jsem se stala pověřenkyní roku 2022.

Co dalšího po tomto netradičním úvodu v časopise najdete?

Ve zpravodaji samozřejmě nechybí aktuální informace o činnosti Spolku pro ochranu osobních údajů. Dozvíte se mimo jiné jména dalších oceněných pověřenců.

Rozesíláním obchodních sdělení se zabýval Nejvyšší správní soud a konstatoval, že je nezbytné, aby si šiřitelé obchodních sdělení, ať už jde o zadavatele (objednatele) či faktické rozesílatele, dostatečně ověřili, zda jim adresáti udělili pro takové zasílání souhlas.

Úřad pro ochranu osobních údajů zveřejnil ke konzultaci metodiku pro kamerové systémy. Jejím posouzením se zabýval František Nonnemann.

Kdy je možné použít pořízený zvukový nebo obrazový záznam úřední osoby? Je přípustné další zpracování osobních údajů úřední osoby zachyceného nahrávkou bez jejího svolení? Odpovědi na tyto otázky přináší ve svém článku Veronika Gabrišová.

Ptáte se, zda je to vše? Kdepak. Časopis obsahuje i další informace a inspirativní podněty pro vaši práci.

Ničím nerušené čtení a pohodové dny vám přeje **Eva Janečková**
šéfredaktorka

Pověřenkyní roku 2022 je šéfredaktorka měsíčníku DPO PRO – Eva Janečková. Co jsme o ní dosud nevěděli?

Eva Janečková se stala pověřenkyní roku 2022 za veřejnou správu. Spolek pro ochranu osobních údajů to oznámil u příležitosti slavnostního vyhlášení, které se konalo ve čtvrtek 25. května v Praze. Jaké to bylo pro šéfredaktorku časopisu DPO PRO překvapení? Za co si ocenění zasloužila? Co všechno obnáší její funkce pověřenkyně pro Městskou část Praha 8 a jí zřizované organizace? A čemu všemu se kromě toho ještě věnuje?

Je to pro vás asi nezvyklé, že úvodní rozhovor zpravodaje, kterého jste šéfredaktorkou, nevedete tentokrát vy a že jsme vás postavili do role respondenta?

Je to velmi nezvyklé. Rozhovory moc často neposkytuji, dalo by se říci, že před nimi utíkám. Domnívám se, že svět je plný mnohem zajímavějších lidí, než jsem já, lidí, kteří mají co říct.

Už u této první otázky si uvědomuji, jak je těžké na některé dotazy odpovídat. Respondenty vždy prosím, aby jejich odpovědi byly alespoň stejně dlouhé jako dotazy, což se ne vždy podaří. A teď už chápu proč. Stojím proto raději na druhé straně a dotazy pokládám já.

Ano, tomu naprosto rozumím. Ale teď k těm cenám. Ty byly předány ve dvou kategoriích: veřejná správa a samospráva a soukromý sektor. Vy jste vyhrála tu první jmenovanou. Víte, kdo vás nominoval?

Vím. Předpokladem pro nominaci byl souhlas nominovaného, tedy v tomto případě souhlas můj. Proto vím, že mě nominovaly SMS-služby. Byť musím prozradit, že můj souhlas byl

získán až ex post, tedy až poté, co k nominaci došlo. Ale nezlobila jsem se.

Co to pro vás znamená? Máte z ocenění radost?

To je pro mě hrozně zapeklitá otázka. Jsem člověk, který se dívá dopředu, na výzvy, které má před sebou. Práci, která již byla odvedena, beru jako něco, co zůstává za mnou, co už bylo, a moc se za tím neohlížím. Často se mi stává, že mi lidé kladou podobnou otázku jako vy ohledně knih, jež jsem napsala. Vždycky mě to překvapí. Vždyť je to něco, co už bylo uzavřeno a není třeba se k tomu vracet.

Proto nijak nepřeháním, když řeknu, že mě ocenění překvapilo. Přimělo mě skutečně se ohlédnout a zrekapitulovat svou práci v oblasti ochrany osobních údajů a, aniž bych se chtěla chlubit, byla jsem poměrně překvapená tím, co za mnou je. Tomuto tématu se věnuji od roku 2005 jako praktik, pracovala jsem na Úřadu pro ochranu osobních údajů, následně jsem přešla „na druhou stranu barikády" a věnovala se práci pověřence. Od roku 2005 také školím, publikuji články a knihy, kterých je nakonec nemalé množství, poskytuji konzultace… Té práce je za mnou opravdu hodně.

Pokud se tedy ptáte, co pro mě ocenění znamená, tak ocenění veškeré této práce, kterou jsem dosud tak úplně nevnímala komplexně. A ano, mám z něj radost. Je zjevné, že si někdo mé práce všiml.

Víte, proč vybrala komise právě vás? Jak vám to zdůvodnili?

Tahle otázka mě přiměla k úsměvu. Vlastně nevím. Nějaké krátké zdůvodnění zaznělo, ale v rámci předávání ceny, kdy jsem se dokonce musela fotit, což jsou pro mě vždy muka, jsem to úplně nezavnímala.

Pohled na ochranu osobních údajů je často odlišný ve veřejném a v soukromém sektoru. Odlišná je často i role a práce pověřenců ve veřejném a soukromém sektoru. Proto Spolek z celkem 30 nominací, které letos obdržel, oceňuje ty nejlepší právě v těchto sektorech. V čem je specifický ten „váš sektor"?

„Můj" sektor se od soukromého liší zejména v tom, že je velmi svázán nejrůznějšími právními předpisy. Zpracování osobních údajů obvykle probíhá v rámci plnění právní povinnosti a znalost těchto právních předpisů je velmi důležitá, vlastně bez ní není možné tuto práci vykonávat. Soukromý sektor má přece jen „volnější ruce".

Postavení pověřence pro ochranu osobních údajů je ve veřejném sektoru také specifické tím, že v rámci tohoto sektoru není možné udělovat finanční sankce, na což mnoho správců osobních údajů hřeší a této oblasti nevěnuje takovou pozornost, jakou by si zasloužila s ohledem na množství osobních údajů, které veřejná správa zpracovává.

Zkusme být více konkrétní. Vy jste pověřenkyně pro Městskou část Praha 8 a jí zřizované organizace. Jaká je náplň této vaší práce a kolik času jí zhruba musíte věnovat?

Náplní práce je být k ruce všem organizacím, dozorovému úřadu a subjektům údajů. Udržovat si přehled o tom, jaké činnosti každá organizace vykonává. Nelze si říct, že je škola jako škola. Každá má svá specifika. Je také nutné udržovat aktualizovanou veškerou dokumentaci, komunikovat s vedoucími všech organizací, musí o mně vědět, znát mě a vědět, s čím se na mě lze obracet. Také musím sledovat změny právních předpisů a reagovat na ně, sledovat metodiky Evropského sboru pro ochranu osobních údajů, metodiky našeho národního dozorového úřadu i dalších centrálních úřadů, sledovat judikaturu evropských i národních soudů, číst odbornou literaturu, udržovat a zvyšovat si odbornost i v takových oblastech, jako je kybernetická bezpečnost.

Nelze proto specifikovat, kolik času práci musím věnovat. Je to nepřetržitý proces, který značně přesahuje pracovní dobu.

Není to tak dávno, kdy jsme oslovili do zpravodaje SMSka pověřence, kteří vykonávají tuto službu pro venkovské oblasti. A ti si vybavovali i velmi kuriózní situace, neboť si je kvůli zveřejněnému kontaktu na webech obcí občané často pletou s obecními zaměstnanci a volají jim například kvůli krávám, které se zaběhly, apod. To se vám asi v Praze neděje… Nebo si vybavíte také nějakou perličku?

Ano, i mě lidé kontaktují s nejrůznějšími dotazy, počínaje stížnostmi na hluk, konče problémy s parkováním, ale až takové perličky, jako je řešení problémů s krávami, se ke mně nedostávají. Lidé často netuší, co si pod pojmem „pověřenec" mají představit, takže se na něj obrací s problémy, které neumí zařadit.

Vidíte, a tady se mi nepovedlo odpověď napsat tak, aby byla delší než dotaz…

Další obsah

Je vidět, že délku svých odpovědí opravdu sledujete odborným okem. Není divu, že jste šéfredaktorkou zpravodaje, který se specializuje na ochranu osobních údajů. Jak je možné, že je měsíc co měsíc už několik let každé číslo plné článků na toto téma?

To je samozřejmě tím, že jsme strašně nápaditá a schopná *(smích)*.

Ale vážně… Ochrana osobních údajů není jeden obor, který by měl nějaké hranice. Prolíná se jakoukoli činností, jakýmkoli oborem, osobní údaje najdete úplně všude. Proto je možné hledat neustále témata, kterými se časopis plní. Horší už je hledat autory, kteří by dokázali napsat čtivý článek, to je na celé té práci asi nejtěžší.

Proto bych ráda poděkovala všem svým autorům, zejména těm, kteří sami nabízí témata a dodržují termíny odevzdání textu.

Jak vidíte budoucnost zpravodaje? Bude pořád o čem psát?

Vzhledem k tomu, co bylo řečeno výše, a vzhledem k tomu, že ochrana dat obecně, nejen osobních údajů, nabývá na důležitosti, určitě bude o čem psát. Jen se ta témata budou postupně proměňovat, protože to, co je v danou chvíli nejzajímavější a nejtíživější, se poměrně rychle proměňuje.

Obecné nařízení pro ochranu osobních údajů známé pod zkratkou GDPR platí v Evropské unii již pět let. Když budeme dnes u této příležitosti i rekapitulovat, připomeňme, co bylo vlastně důvodem pro přijetí tohoto nařízení?

Asi tím hlavním důvodem bylo to, že původní právní úprava byla již velmi stará, pocházela z roku 1995 (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) a rychlý vývoj v oblasti zpracování osobních údajů už tento právní předpis překonal. Ten právní předpis byl v podobě směrnice, tedy předpisu, který musel být implementován do národní úpravy, což

vedlo k tomu, že jednotlivé národní úpravy byly hodně rozdílné.

Při tvorbě nového předpisu, který by odpovídal současnému stavu zpracování osobních údajů, bylo proto zvoleno nařízení, které je přímo účinné, a úprava je tedy jednotná. Záleží pak samozřejmě na tom, jak je v jednotlivých státech aplikována.

Jaký vývoj očekáváte v této oblasti v následujících pěti letech? Jaký má dopad stále se rozšiřující digitalizace?

Domnívám se, že i v oblasti ochrany osobních údajů budou hrát čím dál větší roli IT technologie a kybernetická bezpečnost. Přesun do online prostředí sice umožňuje mít mnohem lepší přehled o zpracovávaných osobních údajích, mít je mnohem dostupnější, ale zároveň jsou také z určitého úhlu pohledu mnohem zranitelnější. Odborníci na ochranu osobních údajů budou muset mít i značné znalosti IT, což dnes ještě není samozřejmostí.

Je na tento vývoj připraveno i GDPR? Nebo si myslíte, že EU bude muset přistoupit k jeho revizi?

O revizích GDPR už se diskuze vedly. Otázkou bude, jestli do jeho znění zasahovat nějak zásadně nebo jestli jej nechat jako obecný předpis a specifika upravit ve zvláštních právních předpisech.

Od zavedení GDPR – tedy od 25. května 2018, byla udělena řada pokut za porušení tohoto nařízení. Novinové titulky hlásají, že pokuty padají jedna za druhou. Jak jsme na tom v ČR s těmi pokutami a který stát v tom vede a proč?

Nemám úplný přehled o tom, kdo vede v ukládání pokut, ani co se týká množství, ani co se týká výše pokut. Nicméně určitě musím zmínit irský úřad, který ukládá pokuty takovým subjektům, jako je Facebook nebo Instagram, a je pověstný vysokými pokutami.

Český dozorový úřad je podstatně mírnější a nevěnuje se zpracování osobních údajů takovými subjekty, jako ten irský. Nerada bych spekulovala o tom, jestli důvodem je personální poddimenzování úřadu, nedostatečná kvalifikace jeho zaměstnanců nebo zcela jiný přístup a priority.

Odhlédněme nyní od GDPR, toho bude ostatně plný zpravodaj, a využijme té situace, kdy vás můžeme čtenářům více představit jako pozoruhodnou ženu mnoha profesí a zájmů. Víme, že vaším hlavním zájmem není pouze GDPR, v dalších časopisech, které vydávají SMS-služby, uvádíme, že jste expertka na školské právo. V čem školám zejména radíte?

Ve všem, co se týká činnosti škol a právní úpravy. Netroufám si zasahovat do pedagogiky a financování, ale cokoliv, kde škola váhá, jak aplikovat nějaký právní předpis, je moje parketa. Jsou to nejčastěji oblasti plnění povinností podle školského zákona, vztahy se zákonnými zástupci, pracovní právo ve školách, které má svá specifika díky zvláštní právní úpravě…

Předpokládám, že ani tady nejsme s výčtem vašich profesních aktivit u konce. Co o vás čtenáři ještě nevědí?

Asi nevědí, že kromě práv mám vystudovanou historii a daří se mi věnovat i této oblasti. Napsala jsem několik knih a občas spolupracuji s Českým rozhlasem při natáčení pořadů, které se týkají dějin. Věnuji se také pracovnímu právu.

Jak ráda trávíte volný čas?

Tak tady je odpověď velmi jednoduchá a stručná… Sportem.

Mou láskou a životní vášní je squash, který doplňuji ještě celou řadou dalších sportů, ale squash je naprosto dominantní.

Děkujeme za svěží rozhovor a přejeme další úspěchy vám, ale i časopisu DPO PRO!

Rozhovor vedly
Marie Machačová a Lenka Matějová

Spolek ocenil nejlepší pověřence roku 2022! Ocenění putuje do médií, samosprávy, farmaceutického průmyslu a na úřad vlády

Spolek pro ochranu osobních údajů již popáté ocenil nejlepší pověřence pro ochranu osobních údajů jmenované podle GDPR. Tentokrát vybíral ty nejlepší a nejaktivnější z nich v roce 2022. Ocenění byla předána na slavnostním vyhlášení, které se konalo 25. května v Praze. Spolek v červnu pokračoval i ve své vzdělávací a osvětové činnosti, zapojil se do veřejné konzultace a vyjádřil se k aktuální kauze utlumování použití rodných čísel.

Ale zpátky k cenám pro nejlepší pověřence. Ty se udělovaly ve dvou kategoriích: Veřejná správa a samospráva a soukromý sektor. Kdo byl letos oceněn?

Pověřenkyní roku za veřejnou správu a samosprávu je Eva Janečková

Za veřejnou správu a samosprávu získala titul pověřenkyně roku Eva Janečková, která v roce 2022 vykonávala funkci pověřenkyně pro Městskou část Praha 8 a jí zřizované organizace. V oblasti veřejné správy a samosprávy porota rovněž ocenila čestným uznáním Jaroslava Vítka, který již řadu let vykonává funkci pověřence na Úřadu vlády České republiky. U obou porota kromě kvalitního výkonu role pověřence a výborné orientace v komplexní problematice zpracování dat ve veřejné správě a samosprávě ocenila i sdílení zkušeností v rámci profesionální komunity i práci na popularizaci tématu ochrany soukromí.

Pověřenkyní roku v soukromém sektoru je Martina Růžičková

V soukromém sektoru si titul nejlepší pověřenec vysloužila Martina Růžičková, která tuto roli zastává v mediálním a vydavatelském domě Czech News Center a v AC Sparta Praha fotbal, a. s. Čestné uznání pak obdržel Michal Merta, pověřenec pro ochranu osobních údajů farmaceutické firmy Zentiva. Zpracování osobních údajů v oblastech žurnalistiky i vývoj, testování a distribuce léčiv je velmi rozsáhlé a citlivé a představuje řadu rizik pro dotčené osoby. Porota u obou oceněných vyzdvihla právě kvalitní výkon role pověřence v takto komplexní oblasti spolu s přesahem do souvisejících oblastí.

Pátý ročník zaštítil předseda Jiří Kaucký

Nad pátým ročníkem opět převzal záštitu Jiří Kaucký, předseda Úřadu pro ochranu osobních údajů. Ten kromě zdůraznění role pověřenců ocenil i význam udělovaného ocenění a činnost Spolku. *„Jsem přesvědčen, že činnost Spolku pro ochranu osobních údajů pomáhá při prosazování respektu k ochraně osobních údajů a soukromí. Spolek hraje zcela zásadní roli i proto, že jde o dobrovolné sdružení profesionálů,"* řekl.

Spolek v červnu pokračoval i ve své vzdělávací a osvětové činnosti

Zástupci Výboru Spolku, Vladan Rámiš a Martin Cach, vystoupili na 6. ročníku EPI konference v Tatranské Lomnici. Vladan Rámiš s příspěvkem o nové digitální legislativě, Martin Cach se ve svém vystoupení zabýval problematikou střetu zájmů pověřence pro ochranu osobních údajů.

V pátek 9. června se pak uskutečnil online workshop s názvem „Je koncept správce a zpracovatele osobních údajů překonaný?". Členové Spolku František Nonnemann a Jakub Hruška na něm představili několik praktických problémů spojených s určením, zda je poskytovatel některých externích služeb, například prošetřovatel whistleblowing oznámení, v postavení správce či zpracovatele. Diskutovalo se rovněž o modelu regulace poskytovatelů služeb, jenž využívají například v Kalifornii.

Ve čtvrtek 22. června zorganizoval Spolek páté setkání pověřenců ve zdravotnictví. Dějištěm události byl Jindřichův Hradec, město dalo akci i záštitu. Pověřenci pro ochranu osobních údajů z řad členů Spolku i širší odborná veřejnost na setkání diskutovali o aktuálních otázkách a problematice zpracování a ochrany osobních dat ve zdravotnictví.

A v pátek 23. června Spolek uspořádal online seminář na téma „Whistleblowing a ochrana osobních údajů". Na tomto semináři jsme i za účasti zástupce gesčního úřadu, Ministerstva spravedlnosti, diskutovali o konkrétních otázkách nastavení whistleblowing systému v návaznosti na přijatý zákon o ochraně oznamovatelů. S ohledem na jeho účinnost, která je pro organizace nad 250 zaměstnanců stanovena na letošní 1. srpen, je praktických otázek k řešení celá řada.

Stanoviska a výkladové materiály

Spolek se rovněž zapojil do veřejné konzultace návrhu metodiky ÚOOÚ ke kamerám a kamerovým systémům. Na základě praktických zkušeností a poznatků svých členů zdůraznil několik bodů, které by v návrhu metodiky doporučil upřesnit či vyjasnit.

Nakonec se Spolek vyjádřil také k aktuální kauze utlumování použití rodných čísel. Ve stanovisku k této věci zdůrazňuje nutnost koncepčního přístupu, včetně důslednějšího vymáhání současné právní úpravy v zákoně č. 133/2000 Sb., o evidenci obyvatel a rodných číslech.

Není rozhodující, kdo ve skutečnosti obchodní sdělení rozesílá

Nejvyšší správní soud letos 16. března ve svém rozhodnutí podpořil rozhodnutí Městského soudu v Praze, když konstatoval, že je nezbytné, aby si šiřitelé obchodních sdělení, ať už jde o zadavatele (objednatele), či faktické rozesílatele, dostatečně ověřili, zda adresáti obchodních sdělení udělili pro takové zasílání souhlas.

Vymezení věci a řízení před krajským soudem

Rozhodnutím Úřadu pro ochranu osobních údajů ze dne 20. 8. 2018 byla žalobkyně shledána vinnou ze spáchání přestupků podle § 11 odst. 1 písm. a), c) a d) zákona č. 480/2004 Sb., o některých službách informační společnosti, ve znění účinném do 30. 6. 2017, neboť v období od června 2016 do března 2017 šířila obchodní sdělení z různých e-mailových adres, aniž disponovala souhlasem adresátů těchto sdělení, v těchto sděleních neuváděla totožnost odesílatele, jehož jménem se komunikace uskutečňuje, a ani v nich neuváděla platnou adresu, na kterou by mohl adresát přímo a účinně zaslat informaci, že si nepřeje další zasílání těchto obchodních sdělení. Za uvedené delikty byla žalobkyni uložena pokuta ve výši 1 400 000 Kč. [1]

Žalobkyní podaný rozklad předsedkyně žalovaného zamítla a rozhodnutí správního orgánu I. stupně potvrdila. [2]

Proti rozhodnutí o rozkladu žalobkyně brojila žalobou. [3]

Důvodnou neshledal městský soud ani námitku, že správní orgány porušily zásadu in dubio pro reo, neboť nebylo dokázáno, že by se na šíření obchodních sdělení podílela žalobkyně. Městský soud zdůraznil, že přestupková odpovědnost právnické osoby je koncipována jako odpovědnost objektivní. Uvedl, že není rozhodné, kdo ve skutečnosti obchodní sdělení rozesílal, postačí skutečnost, že obchodní sdělení bylo šířeno ve prospěch žalobkyně. Zdůraznil přitom smysl zákona o některých službách informační společnosti. Dále připomněl, že žalobkyně nevyloučila, že obchodní sdělení rozeslal některý z jejích partnerů; ani tato skutečnost by ale dle městského soudu nezbavila žalobkyni odpovědnosti za přestupky, neboť soukromoprávní poměr inter partes se nedotýká odpovědnosti za porušení veřejnoprávní povinnosti. Tvrzení žalobkyně, že s obchodními sděleními nemá nic společného, vyhodnotil městský soud s ohledem na skutková zjištění jako nevěrohodné. Detailní informace o původu toho kterého e-mailu není nezbytná. Řetězec důkazů podle městského soudu dostatečným způsobem prokazuje odpovědnost žalobkyně za popsané přestupky. [5]

Kasační stížnost

Proti rozsudku městského soudu podala žalobkyně (stěžovatelka) kasační stížnost dle § 102 a násl. zákona č. 150/2002 Sb., soudní řád správní (dále jen „s. ř. s."). [8]

Stěžovatelka uvedla, že ačkoli odpovědnosti právnické osoby za přestupek nebrání, pokud se nepodaří zjistit konkrétní fyzickou osobu, která jednala ve smyslu § 20 odst. 2 zákona o odpovědnosti za přestupky, je však nezbytné, aby správní orgán zjistil, že k jednání neztotožněné osoby skutečně došlo, přičitatelnost musí být prokázána. Z obsahu správního spisu ani ze správních rozhodnutí takové skutečnosti nevyplývají. K nápravě nedošlo ani v odvolacím (rozkladovém) řízení, ani v řízení před městským soudem. [10]

Stěžovatelka považuje závěry městského soudu týkající se nezohlednění pochybností za nesprávné. Nebylo prokázáno, že se přestupku dopustila stěžovatelka nebo že se na šíření obchodních sdělení podílela. Správní orgány nezjistily, od koho obchodní sdělení pochází. Stěžovatelka vylučuje jakoukoli svoji účast na šíření obchodních sdělení. O takové činnosti nevěděla, nikomu ji nezadala ani ji u nikoho neobjednala. Stěžovatelka uvedla, že nemůže vyloučit, že obchodní sdělení odeslal bez jejího vědomí či souhlasu některý z jejích affiliate partnerů. Jednání se také mohla dopustit konkurenční společnost za účelem poškození stěžovatelky. Správní orgán provedl dokazování v nedostatečném rozsahu. Dokazování nesměřovalo ke zjištění, který subjekt obchodní sdělení skutečně odeslal a jaké jsou faktické či právní vazby mezi subjektem, který sdělení odeslal, a stěžovatelkou. Odpovědnost stěžovatelky za šíření obchodních sdělení nelze dovodit. Stěžovatelka nesouhlasí s argumentací, že obchodní sdělení bylo šířeno ve prospěch stěžovatelky, a není rozhodné, kdo ve skutečnosti obchodní sdělení rozesílal. Stěžovatelka zdůraznila, že jednáním třetí osoby byla naopak poškozena, zákonná sazba pokuty dosahuje až 10.000.000 Kč. Stěžovatelka namítá markantní porušení zásady in dubio pro reo. Závěry správního orgánu i městského soudu se opírají pouze o předpoklady. Pokud obchodní sdělení skutečně rozeslal některý z affiliate partnerů stěžovatelky, nejednalo se o ujednání inter partes, jak uvádí správní orgán a městský soud. Správní orgán nedostál svým povinnostem vyplývajícím z vyšetřovací zásady a městský soud nezákonný postup správního orgánu schválil. [12]

Stěžovatelka dále namítla, že s ohledem na zásadní nedostatky je zřejmé, že uložená pokuta je zcela nepřiměřená okolnostem. Výše pokuty je pro stěžovatelku až likvidační. Správní orgán se měl stěžovatelky dotázat na majetkové poměry a vyžádat si podklady. I v tomto ohledu je dle stěžovatelky rozhodnutí nezákonné.

Stěžovatelka proto navrhla, aby Nejvyšší správní soud rozsudek městského soudu zrušil a zároveň zrušil rozhodnutí předsedkyně žalovaného ze dne 14. 12. 2018 a věc vrátil žalovanému k dalšímu řízení.[14]

Vyjádření žalovaného

Žalovaný ve svém vyjádření uvedl, že stěžovatelka nevysvětlila, proč pro ni má být pozdější právní úprava příznivější. Dále žalovaný mj. uvedl, že stěžovatelka provozovala e-shop podporovaný obchodními sděleními a byla držitelkou domény krizomat.cz. Stěžovatelka využívání adresy newsletter@krizomat.cz k rozesílce obchodních sdělení v řízení potvrdila. Grafická a textová podoba obchodních sdělení zasílaných z elektronické adresy newsletter@krizomat.cz byla identická s ostatními sděleními zasílanými z jiných adres. Žalovaný připomněl princip odpovědnosti správce osobních údajů. Je-li zřejmé, že šiřitelem sdělení byla stěžovatelka, je její subjek-

tivně sledovaný cíl irelevantní. Žalovaný rovněž uvedl, že stěžovatelka svoji ekonomickou situaci ani likvidační charakter pokuty v průběhu správního řízení ani soudního řízení nijak nedoložila. [15]

Posouzení věci Nejvyšším správním soudem

Argumentace stěžovatelky, že městský soud zjevně nesprávně vyložil žalobní námitku týkající se použití příznivější pozdější právní úpravy, Nejvyšší správní soud nepřesvědčil. Městský soud v návaznosti na žalobní bod, v němž stěžovatelka uváděla, že „v rámci časové působnosti je na místě uplatnit retroaktivitu ve prospěch s ohledem na odpovědnost právnické osoby ve vztahu k přičitatelnosti jednání…", zcela přezkoumatelně vysvětlil svůj závěr, že pozdější právní úprava pro stěžovatelku příznivější nebyla. Vysvětlil, že znak přičitatelnosti neznamená, že pro závěr o odpovědnosti právnické osoby je nezbytné identifikovat fyzickou osobu, jejíž jednání bude přičteno právnické osobě. Odkázal přitom na § 20 odst. 6 zákona o odpovědnosti za přestupky. Byť městský soud výslovně neodkázal na přechodné ustanovení § 112 odst. 1 zákona o odpovědnosti za přestupky, na podstatu žalobní námitky odpověděl. Dále ve vztahu určení příznivější úpravy pro stanovení druhu a výměry sankce ve smyslu § 112 odst. 3 zákona o odpovědnosti za přestupky městský soud připomněl asperační zásadu uplatňovanou dle právní úpravy obsažené v zákoně o odpovědnosti za přestupky a s odkazem na rozhodnutí správního orgánu I. stupně vysvětlil, že pozdější právní úprava by umožnila stěžovatelce uložit pokutu vyšší. Ani v tomto ohledu tedy není pozdější právní úprava pro pachatele příznivější. [18]

Uvedené závěry považuje Nejvyšší správní soud za srozumitelné a souhlasí s nimi též věcně. Z § 20 odst. 6 zákona o odpovědnosti za přestupky vyplývá, že správní orgán nemusí zjišťovat konkrétní fyzickou osobu, která za právnickou osobu, v její prospěch či v jejím zájmu jednala a tím založila odpovědnost za přestupek. Je-li tedy na základě zjištěného skutkového stavu zřejmé, že učiněné přestupkové jednání je přičitatelné právnické osobě, není nezbytné, aby bylo najisto postaveno, která fyzická osoba (§ 20 odst. 2 zákona o odpovědnosti za přestupky) se jednání dopustila. V tomto ohledu současná explicitní úprava přičitatelnosti navazuje na koncepci objektivní odpovědnosti právnických osob za správní delikt. Pozdější právní úprava obsažená v zákoně o odpovědnosti za přestupky tedy nebyla pro stěžovatelku příznivější ani z hlediska podmínek odpovědnosti (§ 112 odst. 1 věta druhá zákona o odpovědnosti za přestupky), ani z hlediska druhu či výměry sankce (§ 112 odst. 3 zákona o odpovědnosti za přestupky). [19]

Dále stěžovatelka namítala, že ze správních rozhodnutí ani ze správního spisu nevyplývá, že k jednání neztotožněné fyzické osoby skutečně došlo a že bylo nade vší pochybnost prokázáno, že se skutku, byť v objektivním smyslu, dopustila stěžovatelka. Ani s těmito námitkami se Nejvyšší správní soud neztotožnil. [20]

Správní orgány i městský soud správně zdůraznily, že odpovědnost právnických osob za přestupek je odpovědností objektivní. Jak již bylo výše vysvětleno, právní konstrukt objektivní odpovědnosti právnických osob stejně jako koncepce přičitatelnosti nevyžaduje, aby byla zjištěna osoba, která fakticky jednala, jestliže bylo zjištěno, že faktické jednání fyzické osoby se právně přičítá právnické osobě (srov. rozsudky Nejvyššího správního soudu ze dne 25. 1. 2017, č. j. 6 As 131/2016-25, ze dne 3. 10. 2017, č. j. 9 As 213/2016-60, č. 3642/2017 Sb. NSS). [21]

Šíření obchodních sdělení v rozporu se zákonnými požadavky je jednoznačně doloženo spisovým materiálem. Rozhodnutí správního orgánu I. stupně podrobně vysvětluje, na základě jakých skutkových zjištění a úvah dospěl příslušný správní orgán k závěru, že v právní rovině byla šiřitelem inkriminovaných obchodních sdělení právě stěžovatelka. [22]

Argumentace jednáním ve prospěch či v zájmu právnické osoby (stěžovatelky), zde konkrétně k podpoře její podnikatelské činnosti, odráží podstatu objektivní odpovědnosti právnické osoby a odpovídá na tvrzení stěžovatelky, že s rozesíláním inkriminovaných obchodních sdělení neměla nic společného či že se jednalo o možný exces jejích affiliate partnerů. Jednáním uvedeným ve výrocích rozhodnutí správního orgánu I. stupně bylo propagováno zboží nabízené v e-shopu provozovaném stěžovatelkou. Za těchto okolností pak nemůže obstát argumentace stěžovatelky, že se jednalo o exces jejích affiliate partnerů, za který nenese (objektivní) odpovědnost. Jak správně s důrazem na účel právní úpravy ve svém rozhodnutí uvedla předsedkyně žalovaného, je nezbytné, aby si šiřitelé obchodních sdělení, ať už jde o zadavatele (objednatele) či faktické rozesílatele, dostatečně ověřili, zda adresáti obchodních sdělení udělili pro takové zasílání souhlas, resp. v obecné rovině, zda rozesílka obchodních sdělení probíhá zákonným způsobem. [23]

Ze zásady racionalizované materiální pravdy (§ 3 zákona č. 500/2004 Sb., správní řád) vyplývá, že je třeba zjistit relevantní skutkový stav, a to bez rozumných (důvodných) pochybností. Námitky stěžovatelky jsou postaveny na paušální negaci skutkových zjištění. Skutečnost, že účastník řízení subjektivně nesouhlasí se zjištěným skutkovým stavem, resp. hrozícími právními následky, však sama o sobě nečiní provedené dokazování nedostatečným. Nejvyšší správní soud uzavírá, že v projednávaném případě byly zjištěny všechny rozhodné okolnosti, jak vyžaduje § 50 odst. 3 věta druhá správního řádu, a to bez důvodných pochybností, jak předpokládá § 3 správního řádu. Ze zásady racionalizované materiální pravdy ani ze zásady vyhledávací nevyplývá povinnost správního orgánu zjistit úplný skutkový stav „nade vší pochybnost" či pokračovat v dokazování jen proto, že účastník řízení vyslovil nesouhlas se zjištěným skutkovým stavem. Nejvyšší správní soud se shoduje se správními orgány a městským soudem, že zjištěné skutkové okolnosti v souhrnu konsekventně vedou k závěru, že jednání uvedeného ve výrocích správního rozhodnutí I. stupně se dopustila právě stěžovatelka. [24]

Zpracovala Eva Janečková

Úřad pro ochranu osobních údajů předložil k veřejné konzultaci návrh vlastní metodiky ke kamerovým systémům

Kamerami a kamerovými systémy, resp. zpracováním osobních údajů prostřednictvím kamer, se zabývá Úřad pro ochranu osobních údajů (ÚOOÚ) již poměrně dlouho. První stanovisko k tomu tématu, tedy aplikaci předchozího zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, na kamery, Úřad publikoval již v lednu roku 2006 [1]. Na tento dokument pak navazovala řada dalších, které řešily především využití kamer v některé specifické oblasti či při určité činnosti, například v bytových domech, osobních automobilech atd.

Zájem veřejnosti na ochraně jejich soukromí při zpracování osobních údajů kamerami dokládají i čísla z výročních zpráv ÚOOÚ. V roce 2022 obdržel celkem 2.192 stížností, z nich 10 % se týkalo právě kamer. V roce 2021 to bylo 13 % ze 2.430 přijatých stížností a v roce 2020 se kamer týkalo 13 % z 1.855 stížností, které ÚOOÚ obdržel.

Kamery a GDPR

Většina stanovisek a metodik, které ÚOOÚ vydal k aplikaci předchozí právní úpravy na kamery, byla po účinnosti GDPR z jeho webu stažena.

Proč?

Obecné nařízení o ochraně osobních údajů (GDPR)[2] sice definice základních pojmů, hlavních pravidel a povinností souvisejících se zpracováním osobních dat a věcné působnosti této právní úpravy změnilo jen minimálně, do hry ale vstoupil Evropský sbor pro ochranu osobních údajů (EDPB). Na počátku roku 2020 EDPB vydal pokyny č. 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky. A český úřad, který se výkladových vodítek a pokynů EDPB drží, pakliže není v národním právu důvod pro odlišný postup, své předchozí dokumenty stáhl.

Návrh nové metodiky ÚOOÚ ke kamerám ve veřejné konzultaci

Aplikace GDPR a uvedených pokynů EDPB ale zřejmě není v praxi zcela snadná. Proto ÚOOÚ v dubnu tohoto roku předložil k veřejné konzultaci návrh vlastní detailní metodiky ke kamerovým systémům. Veřejná konzultace probíhala do 9. června. ÚOOÚ neuvedl, do kdy by mohl obdržené připomínky zapracovat a zveřejnit konečnou verzi metodiky. Věřme tedy, že by se tak mohlo stát již letos na podzim.

Jak ÚOOÚ zdůraznil, metodika není závazným právním aktem, prováděcí vyhláškou či něčím podobným. Jde, resp. půjde o dokument, který má především správcům, provozovatelům kamerových a obdobných systémů, pomoci s aplikací GDPR a pokynů EDPB na kamery. K dosažení souladu s požadavky GDPR tak může každý provozovatel kamerového systému použít i jiné procesy a postupy, pokud je bude schopen v případě sporu či kontroly Úřadu obhájit. ÚOOÚ také při zveřejnění návrhu metodiky uvedl, že má usnadnit pozici malých správců osobních údajů, zejména při provozu běžných kamerových systémů.

Zásadní rozšíření působnosti GDPR na online kamery

Pojďme již k samotnému textu návrhu metodiky. Jaké novinky přináší?

Tou největší a podle mého názoru nejvýznamnější je jednoznačné rozšíření působnosti GDPR i na online kamery. ÚOOÚ již od vydání shora zmíněného stanoviska č. 1/2006 vycházel z toho, že právní úprava zpracování osobních údajů se vztahuje pouze na kamery či kamerové systémy, které pořizují záznam zachycených obrazů. Podíváme-li se však striktně na základní pojmy určující působnost GDPR, a předtím zákona č. 101/2000 Sb., tedy osobní údaj a zpracování údajů, jednoznačnou oporu pro tento závěr v normativních textech nenalezneme. Záběr identifikovatelné fyzické osoby je jistě jejím osobním údajem. A zachycení tohoto záběru a jeho přenos a zpřístupnění často i neomezenému okruhu příjemců, což je typická činnost kamer v režimu online, podle mého soudu může v řadě případů odpovídat pojmu zpracování osobních údajů.

Výše uvedený závěr ÚOOÚ nebyl potvrzen judikaturou ani českých, ani evropských soudů. EDPB se ve svých pokynech č. 3/2019 k této otázce rovněž explicitně nevyjádřil. Z řady bodů těchto pokynů však vyplývá, že EDPB s tímto kritériem vůbec nepracuje a aplikuje GDPR podle toho, zda daná kamera či kamerový systém zpracovává, tedy např. přenáší, osobní údaje, obrazové záběry týkající se určených či určitelných lidí.[3]

V návrhu metodiky tedy již ÚOOÚ jednoznačně řekl, že GDPR se vztahuje i na některé online kamery. Proč některé? ÚOOÚ navrhuje rozdělit kamery podle kvality přenášených či zachycených obrazů do šesti kategorií:

- Monitorování, prostor či objekt je snímaný s rozlišením více než 80 mm na pixel
- Zjištění, rozlišení více než 40 mm na pixel
- Pozorování, rozlišení více než 16 mm na pixel
- Rekognoskace, rozlišení než 8 mm na pixel
- Identifikace, rozlišení více než 4 mm na pixel
- Prozkoumání, rozlišení více než 1 mm na pixel

1) Jednalo se o stanovisko č. 1/2006, Provozování kamerového systému z hlediska zákona o ochraně osobních Údajů, které je nyní dostupné už jen v archivu na webu ÚOOÚ.
2) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
3) Především body č. 11, 22, 99 a 116 pokynů EDPB č. 3/2019.

V působnosti GDPR by pak měly být všechny kamery či kamerové systémy, online i ty pořizující dlouhodobý záznam, kromě kamer v režimu monitorování a zjištění. V tomto případě totiž bez vynaložení nepřiměřeného úsilí nelze ze zachycených obrazů identifikovat konkrétní osoby. Nejedná se tak o osobní údaje ve smyslu GDPR.[4] U ostatních kategorií ale ano a GDPR se v plném rozsahu vztahuje na všechny kamery, kamerové systémy, fotopasti a podobná zařízení zachycující či přenášející záběry fyzických osob bez ohledu na to, jestli pořizují dlouhodobý záznam nebo ne.

Jednotlivé povinnosti

V další části návrhu metodiky se ÚOOÚ zabývá některými povinnostmi a právy vyplývajícími z GDPR a jejich vhodným uplatněním na kamerové a obdobné sledovací systémy. Pro jistotu zopakujme, že bez ohledu na to, jestli pořizují či nepořizují dlouhodobý záznam.

Jedná se zejména o:

- určení legitimního účelu a právního důvodu (titulu) ke zpracování osobních údajů,
- zásadu minimalizace zpracování, zejména ve vztahu k době uchování záznamu,
- plnění informační povinnosti a realizace práv dotčených osob, subjektů údajů,
- využití zpracovatele,
- zabezpečení kamerových systémů, včetně přenosových a záznamových zařízení.

Detailní popis či analýza všech těchto částí by přesáhla možnosti tohoto článku. Proto pojďme stručně projít ty body či závěry, které jsou podle mého názoru pro nasazení a provoz kamerového systému klíčové.

ÚOOÚ uvádí dva základní a poměrně široké **účely**, které lze obecně pro zpracování osobních údajů kamerami shledat jako legitimní. Jsou jimi ochrana majetku a ochrana bezpečnosti osob. V praxi bude vždy na správci, provozovateli kamer, aby doložil, pro který účel kamery provozuje a zda daný účel odpovídá jeho podmínkám. Jinak řečeno, zda je pro ochranu majetku či bezpečnosti osob toto zpracování skutečně nezbytné.

Tím se dostáváme k **právním důvodům** ke zpracování. Podle návrhu metodiky obvykle přicházejí v úvahu tři právní důvody: oprávněný zájem správce, souhlas dotčených osob a provádění úkolu ve veřejném zájmu či při výkonu veřejné moci. Podle mého názoru a zkušeností je v praxi aplikovaný, resp. aplikovatelný, především oprávněný zájem. Souhlas je s ohledem na své charakteristiky, obtížnost získání a snadnost odvolání[5] pro zpracování osobních údajů za uvedené účely použitelný jen ve zcela výjimečných situacích. Právní důvod veřejného zájmu pak v kontextu kamer svědčí především veřejnoprávním institucím, například obecní policii v § 24b odst. 1 zákona č. 553/1991 Sb., o obecní policii[6]. Pro úplnost dodejme, že ani takto formulovaný veřejný zájem, resp. zpracování osobních údajů při provádění úkolů při výkonu veřejné moci, není neomezený. Provozovatel kamer musí plnit veškeré další povinnosti, které vyplývají z GDPR či dalších předpisů, například ze zákona č. 110/2019 Sb., o zpracování osobních údajů.

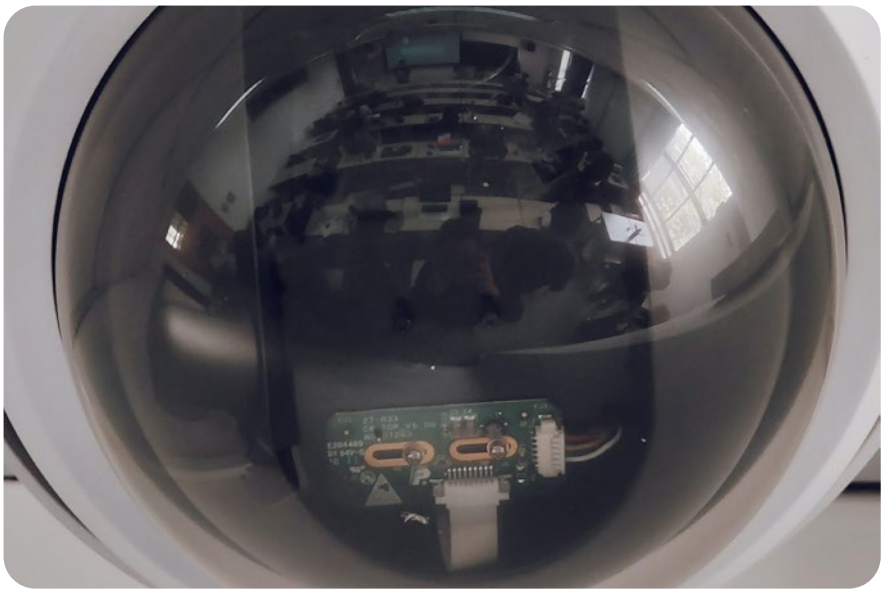
Poměrně kontroverzní je podle mého názoru ta část návrhu metodiky, která se zabývá **dobou uchování** pořízených osobních údajů, tedy nahrávek či zachycených snímků. ÚOOÚ k tomu uvádí, že „doba uchování údajů by ve většině případů měla být stanovena v rozmezí jednoho až dvou dní, v zásadě by neměla přesáhnout 72 hodin". Odůvodňuje to tím, že právě v této lhůtě by měl být správce schopen zjistit, zda došlo či mohlo dojít k protiprávní či jiné relevantní události, pro jejíž dokumentování je nutné prověřit záznam, a případně, pokud je to nezbytné, jeho relevantní část uchovat déle. I když Úřad v odůvodněných případech připouští delší dobu uchování, obecně se kloní právě k maximálně 72 hodinám.

Z řady praktických důvodů může být tato lhůta příliš krátká. Ne každý objekt, který je střežen kamerami, je pod nepřetržitým dohledem, aby byl případný incident odhalen ihned či v řádu hodin. Naopak, často je z ekonomických a provozních důvodů právě neustálý dohled nahrazován kamerami či obdobnými sledovacími systémy. Stejně tak i orgány činné v trestním řízení v praxi požadují záznamy z kamer často za delší období, než je právě těchto 72 hodin. Zajištění fyzické bezpečnosti, například i s využitím kamer, je pak nedílnou součástí plnění povinností řady organizací, typicky v oblasti kybernetické bezpečnosti. Zkrátka takto obecně formulovaná lhůta se mi jeví dosti krátkou a v praxi jen obtížně aplikovatelnou.

Dalším z klíčových principů pro zpracování osobních údajů, jejichž plnění nemusí být v kontextu provozu kamerového systému zcela snadné, je **transparentnost zpracování**, tedy informování dotčených osob o zpracování jejich osobních údajů. V tomto kontextu považuji za důležité, že ÚOOÚ potvrdil možnost uplatnění tzv. vrstveného přístupu (layers approach), kdy při vstupu do monitorovaných prostor jsou subjektu údajů prostřednictvím informačních tabulek poskytnuty základní informace a detaily může získat jinde, např. u pověřeného zaměstnance, na internetu atd. Uvedení všech informací o zpracování osobních údajů, které požaduje čl. 13 GDPR, by v praxi vedlo k nepřehlednosti informačních tabulí, a tím v důsledku ke snížení transparentnosti zpracování jako takového. Na druhou stranu ÚOOÚ v návrhu metodiky i tak uvádí, že by informační tabule měly obsahovat informace, které by podle mého názoru mohly být součástí až „druhé vrstvy", např. informace o právech subjektu údajů.

Návrh metodiky se také poměrně detailně zabývá uplatněním práv subjektu údajů, zejména **práva na přístup** ke zpracovávaným osobním údajům. Právě to může být při zpracování prováděném prostřednictvím kamer se záznamem komplikované. Typickým problémem při uplatnění tohoto práva je na prvém místě identifikace žadatele, subjektu údajů, dále pak úprava poskytované části záznamu tak, aby nezachycoval další identifikované či identifikovatelné osoby, a i celé nastavení procesu tak, aby v krátké lhůtě pro uchování záznamu byl správce vůbec schopen takovou žádost zpracovat. Metodika se k některým problematickým bodům uplatnění práv v rámci kamerových systémů vyjadřuje, podle mého názoru ale spíše z technického

4) Srov. čl. 4 bod 1) a recitál č. 26 GDPR.
5) Blíže viz bod 3.1.1 návrhu metodiky.
6) „Obecní policie je 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."



hlediska. Například otázka, jak identifikovat žadatele jako osobu zachycenou na záznamu, není v návrhu metodiky řešena prakticky vůbec.

Na provozu či vyhodnocování záběrů z kamerových systémů se často podílejí další osoby, typicky bezpečnostní agentury atd. Z pohledu pravidel pro zpracování osobních údajů se jedná o **zpracovatele osobních údajů**, kteří se podílejí na zpracování za správce. Metodika v příslušné části pouze opisuje požadavky na smlouvu se zpracovatelem podle čl. 28 odst. 3 GDPR, bohužel ještě ne všechny a ne zcela přesně. Chybí např. povinnost zpracovatele podílet se na provádění posouzení vlivu na ochranu osobních údajů či nad rámec právních povinností je uváděna povinnost zpracovatele navrhnout správci řešení v případě porušení zabezpečení osobních údajů.[7)]

Dovolím si uvést, že praxe by jistě rovněž ocenila metodickou podporu, jak reflektovat specifika zpracování osobních údajů pomocí kamer při plnění dalších povinností souvisejících se zapojením dalších osob. Typicky na co zaměřit kontrolu zpracovatele vyžadovanou čl. 28 odst. 1 GDPR či jak řešit kritické body v situaci, kdy kamerový systém provozuje za jedním účelem více subjektů, které jsou v postavení společných správců. Například více společností, které sídlí v jednom areálu a svůj majetek střeží společným kamerovým systémem, více bytových družstev či SVJ, které rovněž provozují společný kamerový systém, atd.

Velkou pozornost návrh metodiky věnuje rovněž otázce **zabezpečení** kamer, resp. kamerami zpracovávaných osobních údajů. V porovnání s některými dalšími povinnostmi vyplývajícími z GDPR, které jsou řešeny velmi stručně, např. pouhá jedna věta věnovaná posuzování vlivu na ochranu osobních údajů či dvě věty věnované předávání osobních údajů do zahraničí, to může působit až poněkud nepřiměřeně a nevyváženě.

Přejděme však k obsahu této části návrhu metodiky. ÚOOÚ navrhuje rozdělit kamery z hlediska bezpečnosti do čtyř kategorií, a to podle kombinace koeficientů možných dopadů na subjekty údajů (zejména míra újmy způsobená kamerovým systémem), na správce údajů, pravděpodobnosti výskytu (realizace) této újmy a koeficientu míry porušení práv a zájmů subjektů údajů. Pro jednotlivé kategorie pak metodika navrhuje konkrétní bezpečnostní opatření, od fyzických opatření přes řízení přístupu k datům až po školení obsluhy a zpracování dokumentace. Zjevnou nepřesností je, že návrh metodiky některá opatření u více rizikových kategorií formuluje jako povinné, ačkoliv ÚOOÚ v úvodu sám zdůrazňuje, že metodika bude toliko nezávazným, doporučujícím dokumentem. Ostatně k vydání závazného pokynu, prováděcího předpisu, nemá ÚOOÚ zákonné zmocnění. Stejně tak je otázkou, jestli ÚOOÚ bude tuto klasifikaci rizikovosti zpracování osobních údajů a z nich plynoucích doporučení pro jejich zabezpečení používat i u jiných nástrojů pro zpracování dat, jakým způsobem a proč.

Přílohy pro aplikaci metodiky v praxi

Návrh metodiky obsahuje rovněž tři přílohy, vzorové dokumenty pro plnění některých povinností správce osobních údajů. Jedná se o vzor plnění informační povinnosti, vzorový záznam o činnosti zpracování prováděném kamerovým systémem a vzorový balanční test při zpracování osobních údajů prováděném na základě oprávněného zájmu.

Zejména poslední uvedený dokument je skutečně komplexní a posouzením oprávněných zájmů správce a subjektů údajů se věnuje na 13 stranách. A to s velkou mírou detailu a využitím řady externích informací, např. o ceně nátěru fasády bytového domu při úmyslu instalovat kamery právě v okolí bytového domu za účelem ochrany majetku jeho majitele. Tento rozsah a míra detailu podle mého názoru opět zcela nekorespondují se snahou usnadnit správcům, zejména menším, aplikaci GDPR na kamery.

Shrnutí

Aplikace některých pravidel a povinností stanovených GDPR na kamery není v praxi zcela jednoduchá. Proto osobně vítám snahu ÚOOÚ v této oblasti správcům pomoci. Stejně tak je nutno ocenit, že návrh metodiky byl předložen k veřejné konzultaci s poměrně dlouhou dobou na zaslání připomínek, což, doufám, odborná veřejnost využila.

Za další pozitivní body v návrhu metodiky považuji zejména vyjasnění aplikace GDPR na online kamery, větší sladění ÚOOÚ s přístupem a pokyny EDPB, konkrétní doporučení k některým povinnostem správce či šablony v příloze metodiky.

Pokud bychom chtěli shrnout některé výše kritizované aspekty, které by v konečné verzi mohly být ještě upraveny, pak bych na prvém místě uvedl do jisté míry nekonzistentnost celé metodiky. U řady právních a procesních povinností se do značné míry omezuje víceméně na opis GDPR, někdy ne zcela přesný, bez toho, aby upřesnila specifika pro aplikaci konkrétního ustanovení či povinnosti GDPR při používání kamer. Jiné důležité právní či procesní aspekty v návrhu metodiky zcela chybí, například vztah společných správců, požadavky na zpracovatele atd.

Naproti tomu při řešení technických aspektů jde návrh metodiky do velkých detailů, například i s ambicí správcům ukládat konkrétní bezpečnostní opatření, k čemuž, jak je uvedeno výše, ÚOOÚ postrádá jakékoliv zákonné zmocnění či oprávnění. Za dosti problematické považuji obecné stanovení vhodné doby pro uchování záznamu na 72 hodin, protože v praxi jsou záznamy z řady legitimních důvodů uchovávány déle. Kupříkladu u tohoto bodu bych více uvítal, kdyby Úřad formuloval podmínky či kritéria, které je vhodné při stanovení doby uchování záznamu zohlednit, a stanovení konkrétní doby více nechal na jednotlivých správcích. Samozřejmě včetně odpovědnosti.

Uvidíme tedy, jaké připomínky Úřad k návrhu metodiky obdrží, jak je zohlední a jaká bude finální verze metodiky. Věřme, že již na podzim tohoto roku.

František Nonnemann
Autor je právník. Je také členem Výboru Spolku pro ochranu osobních údajů.

7) Čl. 28 odst. 3 písm. f) GDPR.

Nahrávky úředních osob a kdy je lze použít?

V dubnovém čísle časopisu DPO PRO jsme se věnovali problematice nahrávání úředních osob.[1] Připomeňme si, že nahrávání úředních osob bez jejich svolení jsme připustili zejména za účelem ochrany oprávněných zájmů účastníků řízení a dalších osob dotčených jejich jednáním. Nyní se zaměříme na to, jak naložit s pořízenou nahrávkou. Kdy je možné použít pořízený zvukový nebo obrazový záznam úřední osoby? Je přípustné další zpracování osobních údajů úřední osoby zachycených nahrávkou bez jejího svolení?

Výchozí pravidlo pro použití nahrávek

Bez ohledu na to, zda na zvažované zpřístupnění pořízené nahrávky budeme nahlížet jako na další zpracování[2] osobních údajů úředních osob nebo použití zvukového či obrazového záznamu ve smyslu § 88 občanského zákoníku,[3] platí v zásadě stejná pravidla jako při pořízení nahrávky (zachycení podoby a projevů osobní povahy, resp. zpracování osobních údajů). Přípustnost šíření nahrávky (dalšího zpracování) souvisí se zákonností samotného pořízení nahrávky.[4] **Bez svolení dotčené osoby (subjektu údajů) je pořízení i použití nahrávky přípustné, jen pokud sleduje legitimní účel** (ochranu jiných práv nebo právem chráněných zájmů) **a je přiměřené (nezbytné)**. Dodržení těchto dvou podmínek současně představuje základní pojistky před zneužitím nahrávky.

Použití nahrávky musí sledovat legitimní účel

Použití nahrávky úřední osoby k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob by mělo souviset s výkonem působnosti daného správního orgánu, resp. výkonem pravomoci oněch úředních osob,[5] jak je nahrávkou zachycen. **Použití nahrávek je přípustné pro účely důkazní v různých řízeních,[6] pro účely kontroly[7] nebo při vyřizování stížnosti na nevhodné či neprofesionální jednání úřední osoby.[8]**

Nelze vyloučit použití důkazu záznamem schůzky, rozhovoru, telefonního hovoru bez svolení nahrávané osoby, děje-li se tak za účelem výkonu a ochrany práv jiného. **Nemusí se navíc nutně jednat přímo o vlastní práva či zájmy pořizovatele nahrávky**, děje-li se tak za účelem výkonu a ochrany soukromých práv jiného (např. člena rodiny).[9]

Poskytnutí nahrávky může být **i projevem veřejné kontroly**[10] – lze upozornit např. nadřízeného nebo kárný orgán na konkrétní nevhodné či korupční jednání osoby, i když jím pořizovatel nahrávky nebyl přímo dotčen. **Zákon chrání soukromí úředních osob, ale ne jejich neprofesionální či dokonce protiprávní jednání.**

Použití nahrávky musí být přiměřené a nezbytné

Požadavek přiměřenosti použití[11] či nezbytnosti zpracování[12] pro účely oprávněných práv a zájmů osoby dotčené jednáním nahrávané úřední osoby, případně veřejnosti, **znamená poměřovat (testovat) při použití nahrávky konkurující si práva a zájmy**, aby pořízené nahrávky (bez svolení dotčené úřední osoby) bylo možné použít např. jako důkazní prostředky pro účely soudních nebo správních řízení, děje-li se tak za účelem ochrany či jiného uplatnění práv a zájmů jiných osob v těchto řízeních. Nejvyšší soud zdůrazňuje, že to platí

1) Blíže příspěvek autorky: Nahrávání úředních osob? Co na sebe nechcete prozradit, nikomu nesdělujte.
2) Už v rozhodnutí Soudního dvora evropské unie ze dne 6. 1. 2003, C – 101/01, Bodil Lindqvist, konstatoval soud, že zveřejnění osobních údajů 18 osob na internetu je zcela nebo částečně automatizovaným zpracováním osobních údajů. V rozsudku ze dne 14. 2. 2019, C -345/17, Sergejs Buivids, soud rozhodl, že pro to, aby bylo aplikováno Obecné nařízení o ochraně osobních údajů, postačuje, že došlo k zaznamenání videozáznamu fyzické osoby jen jednou.
3) Podle § 88 odst. 1 občanského zákoníku *svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.*
4) Srov. zásadu účelového omezení zpracování ve smyslu článku 5 odst. 1 bod b) Obecného nařízení o ochraně osobních údajů.
5) VEDRAL, J.: Správní řád. Komentář. II. aktualizované a rozšířené vydání. Praha: RNDr. Ivana Hexnerová – BOVA POLYGON, 2012, ISBN 978-80-7273-166-4, s. 230
6) Přípustností záznamů hovorů fyzických osob se Ústavní soud zabýval několikrát. Srov. např. usnesení ze dne 20. 10. 2011 ve věci sp. zn. II. ÚS 143/06, kdy poukázal na to, že *„v trestních řízeních tak nelze zásadně s ohledem na ustanovení § 89 odst. 2 trestního řádu vyloučit možnost, aby byl k důkazu použit i zvukový záznam, který byl pořízen soukromou osobou bez souhlasu osob, jejichž hlas je zaznamenán. Přípustnost takového důkazu je ovšem i tak vždy nezbytné posuzovat též s ohledem na respektování práva na soukromí zakotveného v čl. 8 Úmluvy, práva na nedotknutelnost osoby a jejího soukromí ve smyslu čl. 7 a čl. 10 odst. 2 Listiny.*
Přípustností nahrávek soukromých osob v přestupkovém řízení se zabýval veřejný ochránce práv ve zprávě o šetření ze dne 14. února 2017, sp. zn. 4346/2016/VOP, dostupná: https://eso.ochrance.cz/Nalezene/Edit/4976
Potměšil, J.: Použitelnost zvukových a obrazových záznamů, Správní právo č. 3/2010, dostupné: https://www.mvcr.cz/npo/clanek/pouzitelnost-zvukovych-a-obrazovych-zaznamu-jako-dukazu.aspx
7) K přípustnosti nahrávek v rámci kontroly se ochránce vyjádřil ve svých doporučeních kontrolním orgánům, srov. https://www.ochrance.cz/vystupy/edice-stanoviska/Sbornik_Kontrolni-organy.pdf
8) Srov. zprávu o šetření veřejné ochránkyně práv ze dne 16. 12. 2016, sp. zn. 1914/2016/VOP, dostupná: https://eso.ochrance.cz/Nalezene/Edit/4568
9) Lavický, P. a kol.: Občanský zákoník I. Obecná část (§ 1–654). Komentář. 1. vydání, Praha: C. H. Beck, 2014, s. 536
10) Srov. nález Ústavního soudu ze dne 11. 11. 2005 I. ÚS 453/03, který mj. uvádí: „Věcí veřejnou jsou veškeré agendy státních institucí, jakož i činnost politiků místních i celostátních, úředníků, soudců, advokátů, popř. kandidátů či čekatelů na tyto funkce. Tyto veřejné záležitosti, resp. veřejná činnost jednotlivých osob, mohou být veřejně posuzovány."
11) Srov. § 90 občanského zákoníku: „Zákonný důvod k zásahu do soukromí jiného nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu **nesmí být využit nepřiměřeným způsobem** v rozporu s oprávněnými zájmy člověka."
12) Srov. čl. 6 odst. 1 písm. f) Obecného nařízení o ochraně osobních údajů.

„zvláště za situace, kdy by použitím záznamu mohlo dojít k zásahu do takových přirozených práv člověka, která nejsou omezitelná obyčejnými zákony, nýbrž pouze na základě imanentních ústavních omezení, tj. omezení plynoucích přímo z ústavního pořádku samotného, jako kupř. u cti a vážnosti člověka (srov. nález Ústavního soudu sp. zn. IV. ÚS 23/05). [13] *V takovém případě je pak nutno i zde podle konkrétních okolností uvážit, zda při střetu ústavního práva na spravedlivý proces (čl. 36 a násl. Listiny, resp. čl. 6 Úmluvy) a přirozených osobnostních práv není dána bezdůvodně přednost jednomu právu před právem druhým."* [14]

Základní střet představuje zájem na ochraně osobnostních práv (soukromí) úředních osob (na jedné straně) a zájem na zjištění skutečného průběhu a obsahu úředního jednání, zájem na dodržování základních zásad činnosti správních orgánů (na straně druhé).

Střet konkurujících si práv a zájmů nelze řešit v obecné rovině, ale v kontextu okolností konkrétního případu, a to **pomocí tzv. testu proporcionality** skládajícího se ze tří kroků – zkoumání vhodnosti a potřebnosti konkrétního opatření a dále proporcionality v užším smyslu, tj. právě přiměřenosti opatření s ohledem na zamýšlený cíl. [15]

I utajená nahrávka může posloužit jako důkaz

Nejvyšší správní soud připustil, že *„důkaz utajenou nahrávkou pořízený soukromou osobou nelze ze správního řízení zcela vyloučit, i pokud zasahuje do osobnostních práv nahrávané osoby a byl pořízen bez jejího souhlasu"* [16]. Podle Nejvyššího správního soudu je však vždy nutné poměřit jednak legitimitu cíle, kterého mělo být pořízením záznamu dosaženo, a jednak přiměřenost užitého postupu. Nad ochranou osobnostních práv může převážit zájem společnosti na potrestání deliktního jednání.

Ústavní soud skryté nahrávání profesionálních i soukromých jednání v obecné rovině odsoudil: *„za běžných okolností je svévolné nahrávání soukromých rozhovorů bez vědomí jejich účastníků hrubým zásahem do jejich soukromí. Takovýto postup s rysy záludnosti je ve velké většině případů morálně i právně zcela nepřijatelný, zejména je-li veden záměrem nahrávanou osobu poškodit.* ***Ústavní soud se rozhodně staví proti nekalým praktikám vzájemného elektronického sledování a skrytého nahrávání při soukromých i profesionálních jednáních****, jež zpravidla jsou nejen v rozporu s právem, ale hodnoceno po stránce sociálně-etické šíří ve společnosti atmosféru podezíravosti, strachu, nejistoty a nedůvěry."* [17]

Ústavní soud však dodal, že ***„zcela odlišně je třeba posuzovat případy, kdy je tajné pořízení audiozáznamu rozhovoru… způsobem dosažení právní ochrany pro výrazně slabší stranu…***[18] *Zásah do práva na soukromí osoby, jejíž mluvený projev je zaznamenán, je plně ospravedlnitelný zájmem na ochraně slabší strany právního vztahu, jíž hrozí závažná újma. Opatření jediného nebo klíčového důkazu touto cestou je analogické k jednání za podmínek krajní nouze či dovolené svépomoci."*

Závěry ústavního soudu lze aplikovat na skryté nahrávání a použití nahrávek jednání úředních osob pořízených bez souhlasu nahrávaných osob, neboť i na osoby dotčené jednáním úředních osob lze nahlížet jako na „slabší stranu", neboť nemusí být za všech okolností znalé svých práv. Je třeba si uvědomit, že řada úředních jednání probíhá standardně za „zavřenými dveřmi", bez přítomnosti dalších osob. Nahrávka tak může být v podstatě jediným důkazem – stejně jako v případě, který řešil Ústavní soud – schopným prokázat, jak jednání skutečně probíhalo, zda se úředník choval profesionálně a v souladu s právními předpisy. V opačném případě nastávají situace „tvrzení proti tvrzení", které nelze zpětně objektivizovat.

Shrnutí

I nahrávky osob pořízené bez svolení nahrávaných osob jsou právně přípustné a je třeba je, samozřejmě kriticky, zkoumat. Nahrávky nelze odmítat jen z důvodu, že byly pořízeny bez souhlasu nahrávané osoby.

Základním kritériem, jež má v konečném důsledku vést k rozhodnutí o použitelnosti či nepoužitelnosti nahrávky bez vědomí nahrávané osoby jako důkazu, je poměřování chráněných práv a zájmů, které se v konkrétním případě střetávají.

Požadavek na přiměřené (nezbytné) použití nahrávky k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů dotčených osob mj. znamená, že nahrávky úřední osoby by měla dotčená osoba primárně využít k ochraně práv a právem chráněných zájmů prostřednictvím opravných prostředků, které jí právní řád nabízí (odvolání, námitky podjatosti, stížnosti, podnětu k přezkumu, správní žalobě apod.). Zveřejnění nahrávky lze připustit; mělo by mu ale předcházet „neúspěšné vyčerpání opravných prostředků" a jeho primárním cílem by nemělo být znevážení (zesměšnění) nahrávané úřední osoby. [19]

Procesní ochranu před neoprávněnými zásahy do osobnostních práv úředních osob může poskytnout v konečném důsledku soud. [20]

Veronika Gabrišová
Autorka pracuje v Kanceláři veřejného ochránce práv, je vedoucí odboru veřejného pořádku a místní správy, pověřenkyní pro ochranu osobních údajů a členkou rozkladové komise Úřadu pro ochranu osobních údajů.

13) Srov. také nález Ústavního soudu ze dne 11. 11. 2005, sp. zn. I. ÚS 453/03: *„Čest je také integrální a důležitou součástí důstojnosti člověka. Formuje rovněž základ mnoha rozhodnutí činěných členy demokratické společnosti, která jsou fundamentální pro její dobré fungování. Čest hraje roli ve vztazích jako např. koho zaměstnavatel zaměstná, resp. pro koho pracovník chce pracovat, je rozhodující při úvaze o tom, kdo má postoupit do vyšších pracovních či funkčních pozic, čest je důležitá pro rozhodnutí o tom, s kým navázat obchodní vztahy nebo komu bude dán hlas v politickém životě. Je-li jednou čest pošpiněna neopodstatněným obviněním vyjádřeným veřejně, a tím spíše v médiích, může být pověst a čest osoby poškozena navždy a zvláště pak v situaci, není-li dána možnost rehabilitace. Pokud taková situace nastane, prohrává jak osoba sama, tak i společnost. A právě proto nelze vycházet z toho, že ochrana pověsti, resp. cti, je záležitostí důležitou pouze pro dotčeného jednotlivce, případně jeho rodinu. Z těchto důvodů je ochranu pověsti, resp. cti, třeba vnímat i jako ochranu veřejného statku. Je proto ve veřejném zájmu, aby čest a pověst osob působících ve veřejném životě nebyla diskutována ve skutkově posunutých rovinách. Jak na poli politiky, tak ve sdělovacích prostředcích volič potřebuje být schopen rozeznat dobro od zla, aby nakonec mohl učinit informovaný výběr ve vztahu k politikovi i k médiím."*

14) Srov. rozsudek Nejvyššího soudu ze dne 24. 9. 2019, sp. zn. 4 Tdo 1064/2019.

15) Srov. nález Ústavního soudu sp. zn. Pl. ÚS 24/11 ze dne 20. 12. 2011 (N 217/63 SbNU 483; 43/2012 Sb.).

16) Srov. rozsudek Nejvyššího správního soudu ze dne 18. listopadu 2011, č. j. 2 As 45/2010 – 68.

17) Srov. nález Ústavního soudu sp. zn. II. ÚS 1774/14 ze dne 9. 12. 2014 (N 221/75 SbNU 485).

18) V posuzovaném případě si ústavní stěžovatel nahrávku pořídil za účelem prokázání svých tvrzení o skutečném důvodu výpovědi z pracovního poměru.

19) Srov. nález Ústavního soudu ze dne 11. 11. 2005, sp. zn. I. ÚS 453/03: *„Důležité pro zvážení legitimního zveřejnění informace je zkoumání motivu zveřejnění. Legitimitu zveřejnění informace nelze dovodit, pokud byla dominantně motivována touhou poškodit difamovanou osobu, pokud šiřitel sám informaci nevěřil anebo pokud ji poskytl bezohledně, aniž by se řádně staral o to, zda je či není pravdivá."*

20) Srov. § 82 občanského zákoníku: *„Člověk, jehož osobnost byla dotčena, má právo domáhat se toho, aby bylo od neoprávněného zásahu upuštěno nebo aby byl odstraněn jeho následek."*

Dark Patterns při zpracování osobních údajů

Na začátku letošního roku zveřejnil Evropský sbor pro ochranu osobních údajů vodítka ke klamavým praktikám sociálních sítí v oblasti zpracování osobních údajů. Tyto praktiky bývají nazývány *Dark Patterns*, což by se do češtiny dalo přeložit jako temné vzorce. Sama vodítka označují tyto praktiky jako klamavé designové vzory (*Deceptive Design Patterns*). Vodítka míří na sociální sítě, nicméně jejich využití je univerzální a týká se všech správců osobních údajů, zvláště těch, kteří poskytují své služby na internetu. Společné pro dark patterns je to, že se úmyslně nebo neúmyslně snaží, aby subjekt údajů nebyl informován o zpracování osobních údajů, nebo se snaží subjekt údajů odradit od využívání práv spojených s ochranou osobních údajů. Správce může formálně povinnosti podle GDPR splňovat, nicméně takovým způsobem, který je se zásadami GDPR neslučitelný. Vodítka popisují celou řadu dark patterns a uvádí jejich příklady. Sbor také identifikuje, v čem spatřuje porušení GDPR, a představuje příklady dobré praxe. Protože neexistuje český překlad vodítek, uvádím v článku anglické názvy těchto praktik. V závorce je možný český překlad.

Overloading (zahlcení)

Subjekt údajů je zahlcen lavinou různých informací a možností, a tudíž předá správci více osobních údajů, než původně zamýšlel, nebo neúmyslně povolí zpracování osobních údajů pro další účely. Uživatel je tlačen do toho, aby poskytl více osobních údajů, než je třeba, nebo je neustále tázán na poskytnutí určitého údaje. Tento tlak vede k tomu, že uživatel údaj poskytne, aby nebyl dále „obtěžován". Při registraci je upozorňován na vyplnění telefonního čísla z bezpečnostních důvodů nebo je na telefonní číslo při každé návštěvě dotazován. Souhlas daný tímto způsobem není svobodný, a pokud je ještě účel zpracování vágně vymezen, nejedná se ani o souhlas poskytnutý ke konkrétnímu účelu nebo účelům.

Dalším druhem overloadingu je složitost uplatnění práv nebo nalezení informace. Uživatelé jsou nuceni procházet řadou stránek a činit více kroků, aby našli požadovanou informaci, což je může od hledání odradit. Informace o odvolání souhlasu je ukrytá pod několika podsekcemi apod. Tato praktika naráží na zásadu transparentnosti a korektnosti a také na povinnosti správců podle čl. 12 GDPR, jelikož uživatelé nejsou informováni transparentním, srozumitelným a snadno přístupným způsobem. Stejné povinnosti správců jsou porušovány, pokud nabídnou uživatelům příliš mnoho možností, v jejichž rámci může uživatel snadno určité nastavení přehlédnout.

Skipping (přeskakování)

U skippingu je uživatelské rozhraní nebo prostředí navrženo tak, aby uživatelé zapomněli na ochranu osobních údajů nebo o některých jejich aspektech nepřemýšleli. Uživatelům je nabídnuto více možností, z nichž je předem zaškrtnuta ta, která umožňuje nejextenzivnější zpracování osobních údajů. Toto je v rozporu se svobodně uděleným souhlasem a dále se zásadou podle čl. 25 GDPR, tedy data protection by design and by default.

Dalším druhem této praktiky je poskytnutí informací, které s ochranou osobních údajů nemusí souviset a tím mohou uživatele zmást. Toto porušuje zásadu transparentnosti a korektnosti stejně jako povinností podle čl. 12 GDPR.

Stirring (pohnutí)

U této praktiky se správce snaží ovlivnit volbu uživatele tím, že apeluje na jeho emoce nebo mu určitou možnost podsouvá. Správce používá slovní nebo vizuální prvky způsobem, který uživatelům poskytuje informace buď výrazně pozitivně, díky čemuž se uživatelé cítí dobře, bezpečně nebo odměňováni, nebo naopak velice negativně, kvůli čemuž uživatelé mohou cítit strach nebo vinu. Ovlivňování emočního stavu uživatelů pravděpodobně přiměje tyto uživatele k akci, která je v rozporu s jejich zájmy v oblasti ochrany údajů. Emoční ovlivňování je opět v rozporu se zásadou transparentnosti a korektnosti, ale může být v rozporu s informovaným souhlasem, nebo dokonce v rozporu s podmínkami pro souhlas dítěte.

Správce také může použít vizuální styl nebo techniku, která uživatelům podsouvá rozsáhlejší zpracování osobních údajů. Toto je v rozporu se zásadou korektnosti, svobodného souhlasu a také s čl. 12 GDPR.

Obstructing (zabránění)

Správce brání uživatelům, aby provedli zamýšlenou akci, nebo se snaží její provedení ztížit. Uživatelé hledají informace nebo odkaz, který nakonec nenajdou, protože odkaz pro přesměrování buď nefunguje, nebo není vůbec dostupný. Například po zahájení procesu registrace nejsou uživatelům poskytovány žádné odkazy na informace o ochraně osobních údajů. Uživatelé tyto informace nemohou najít, protože nikde v přihlašovacím rozhraní nejsou uvedeny. Tato praktika je v rozporu s čl. 12 a čl. 25 GDPR.

Další variantou této praktiky je situace, kdy se uživatelé pokusí aktivovat možnost související s ochranou osobních údajů, ale cesta k této možnosti vyžaduje více kroků, než je nezbytně nutné. Kromě porušení čl. 12 a čl. 25 GDPR může toto znamenat porušení práva na námitku nebo práva odvolat souhlas.

Formou obstructingu je i rozpor mezi informacemi a možnostmi dostupnými uživatelům, který je nutí udělat něco, co neměli

původně v úmyslu. Správce v tomto případě porušuje zásadu transparentnosti a korektnosti a je také v rozporu s pravidly pro informovaný souhlas.

Fickle (nestálost)

Fickle znamená, že rozhraní je nekonzistentní a nejasné, což ztěžuje, aby se uživatel orientoval v možnostech ochrany osobních údajů a porozuměl účelu zpracování. Informace související s ochranou osobních údajů postrádají hierarchii. Informace se objevují v textu několikrát a jsou prezentovány několika různými způsoby. Uživatelé budou pravděpodobně zmateni a nebudou schopni plně porozumět tomu, jak jsou jejich údaje zpracovávány a jak nad nimi mohou vykonávat kontrolu. Informace o ochraně dat nebo možnost související s ochranou osobních údajů jsou umístěny na stránce, která se tematicky vůbec neshoduje se stávajícím obsahem. Uživatelé pravděpodobně nenajdou informace nebo možnost, protože je intuitivně na konkrétní stránce nehledají.

Rozhraní není konzistentní (např. nabídka související s ochranou dat nezobrazuje stejné položky na mobilu a na počítači) nebo se neshoduje s očekáváním uživatelů (např. umístění odkazu na stránce). Tyto rozdíly mohou vést uživatele k tomu, že nenaleznou požadovaný prvek či informace nebo si zvolí ochranu dat, kterou si nepřejí.

Dalším příkladem této praktiky jsou informace související s ochranou osobních údajů, jež nejsou poskytovány v jazyce země, kde uživatelé žijí a využívají službu, zatímco samotná služba se jazykově shoduje. Pokud uživatelé neovládají jazyk, ve kterém jsou informace o ochraně osobních údajů poskytovány, nebudou schopni je snadno přečíst, a proto pravděpodobně nebudou vědět, jak jsou jejich údaje zpracovávány. Všechny tyto praktiky jsou v rozporu s čl. 12 GDPR. Nekonzistentní volba jazyka je navíc v rozporu s právem na informace podle čl. 13 a 14 GDPR.

Left in the dark (ponechání ve tmě)

U této praktiky je rozhraní navrženo tak, aby skrylo informace nebo možnosti ochrany osobních údajů nebo aby si uživatelé nebyli jisti, jak jsou jejich údaje zpracovávány a jak mají uplatnit svá práva.

Dalším příkladem je poskytování informací o ochraně osobních údajů, které spolu nějakým způsobem kolidují. Uživatelé si pravděpodobně nebudou jisti tím, co by měli dělat a jaké by byly důsledky jejich jednání, a je proto pravděpodobně, že si žádnou z nabízených možností nezvolí a přijmou výchozí nastavení. Praktika left in the dark se může projevovat v používání nejednoznačných a vágních termínů obsažených v informacích o ochraně osobních údajů. Uživatelé si nebudou jisti, jak budou údaje zpracovávány nebo jak nad nimi vykonávat kontrolu. Kromě porušení čl. 12 GDPR jsou tyto prakticky navíc v rozporu se zásadou korektnosti a s požadavkem na informovaný souhlas.

Závěr

Evropský sbor pro ochranu osobních údajů vodítky k dark patterns jednoznačně potvrdil, že správce musí dbát zásad ochrany osobních údajů. To znamená, že subjekt údajů musí být skutečně informován a musí mít skutečnou možnost volby. Pouhé formální plnění povinností stanovených v GDPR nestačí k naplnění smyslu regulace ochrany osobních údajů. Na tomto místě je vhodné poznamenat, že přestože Sbor připouští, že zahlcení informacemi transparentnost snižuje, legislativa jde přesně opačným směrem. Vznikají tak nové informační povinnosti, které fakticky snižují informovanost uživatelů.

Eva Fialová

Autorka je právnička se specializací na ochranu osobních údajů a právo ICT. Působí v advokátní kanceláři GHS Legal.

DPO PRO. Ročník III, číslo 6. Vychází každého 28. dne v měsíci v Praze. Cena ročního předplatného činí 1 990 Kč bez DPH. Vydávají SMS-služby s. r. o. se sídlem V Rovinách 40, 140 00 Praha 4-Podolí, IČ: 067 84 771. Adresa redakce: Národní 41, 110 00 Praha 1-Staré Město. Webové stránky: https://www.dpopro.cz. Minimální rozsah 12 stran A4. Evidenční číslo: MK ČR E 24123. ISSN 2695-1363. Šéfredaktorka: JUDr. et Mgr. Eva Janečková, eva.janeckova@sms-sluzby.cz. Redakční rada: JUDr. et Mgr. Eva Janečková, Ing. Mgr. Oldřich Kužílek, Ing. Michal Merta, MBA, MSc., LL.M., JUDr. Adam Furek. Jazyková redakce: Marie Machačová. Předplatné: Magdalena Komárková, magdalena.komarkova@sms-sluzby.cz, tel.: +420 723 644 867. Grafické práce: Studio Matrix. Redakční uzávěrka: 25. 6. 2023.