PRO
OCHRANA OSOBNÍCH ÚDAJŮ V PRAXI

Číslo 2/2023, ročník III. Měsíčník SMS - služby s. r. o. www.dpopro.cz

Čtyři roky s GDPR ve školách aneb Jaká je realita?

Rozhovor

Obecné nařízení (GDPR) vneslo v posledních letech nové otázky a nové situace také do škol. V médiích se od roku 2018 objevovaly články o tom, že v souvislosti s ochranou osobních údajů si na nejednu školu došlápli rodiče s kdovíjakou záminkou, neboť se stále větší znalostí problematiky mají v rukou daleko lepší „munici" než za předchozí právní úpravy. I proto musí být školy velmi pečlivé při řešení nastalých otázek. To potvrzuje také Ludmila Zhoufová, která je ředitelkou Základní školy Černošice, jež se nachází v okrese Praha-západ.

Obecné nařízení (GDPR) bylo v roce 2018 velkým tématem, kterého se všichni děsili. Jaká je realita po čtyřech letech účinnosti tohoto právního předpisu? Řeší rodiče ochranu osobních údaje svých dětí a jejich bezpečnost?

Ano, rodiče to řeší. Je proto potřeba mít od nich vyplněné a centrálně zaevidované souhlasy se zpracováním osobních údajů žáků. Na začátku roku, ojediněle i během roku, dochází k jejich aktualizaci vzhledem k tomu, že z určitých důvodů se rodič během docházky svého dítěte na ZŠ rozhodne změnit svůj názor na poskytování těchto údajů.

Velkým tématem bylo pořizování a zveřejňování fotografií dětí. Některé školy dokonce přestaly fotografie pořizovat a zrušily své účty na sociálních sítích. Dotkla se nová pravidla zpracování osobních údajů i činnosti vaší školy?

Ano, tento problém také řešíme. V centrální databázi souhlasů se zpracováním osobních údajů žáků je uvedeno, kteří rodiče si nepře-

Vážení čtenáři,

nejen pověřencům pro ochranu osobních údajů je určeno únorové číslo časopisu DPO PRO.

Nenechte si ujít rozhovor s ředitelkou základní školy v Černošicích Ludmilou Zhoufovou. Povídaly jsme si o tom, jak je to nyní s ochranou osobních údajů ve školách.

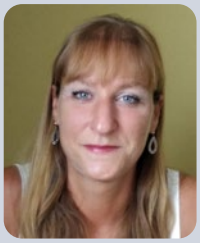
Ani tentokrát nechybí aktuální informace o činnosti Spolku pro ochranu osobních údajů, který se zabýval předáváním dat mimo EU a aktuální judikaturou.

Podrobněji se věnujeme rozhodnutí Městského soudu v Praze, jenž dospěl k závěru, že za subjekt, který šíří obchodní sdělení, nelze považovat pouze přímého odesílatele tohoto sdělení, nýbrž subjekt, který jeho odeslání inicioval a jehož jménem došlo k jejich šíření.

Jak je tomu v současné době s předáváním osobních údajů do USA, se ve svém článku zaobírala Monika Kovář Staňková.

Různými aspekty bankovní identity jako metody digitálního ověření totožnosti osob se zabývali Vojtěch Dlouhý a David Musil.

Ptáte se, zda je to vše? Kdepak. Časopis obsahuje mnohem více. Tak tedy ničím nerušené čtení a mnoho inspirativních podnětů pro vaši práci přeje **Eva Janečková**
šéfredaktorka



jí zveřejňovat fotografie svých dětí. Při zveřejňování fotografií činností dětí ve škole nebo jejich výsledcích z různých soutěží se toto pravidlo dodržuje. Proto je nyní méně uveřejněných fotografií na sociálních sítích i webových stránkách, než bylo dříve.

Dotkly jsme se sociálních sítí. Jejich využívání školami by se mělo řídit přísnějšími pravidly. Využívá vaše škola nějakou sociální síť? Je dodržování přísných pravidel pro školu komplikované?

Škola provozuje oficiální facebookovou stránku, kde uveřejňuje příspěvky. Tyto příspěvky uveřejňuje zodpovědná osoba, která dostává podklady se zohledněním na ochranu osobních údajů žáků a zveřejňované informace korespondují s těmi, které jsou na webových stránkách školy.

V době covidu probíhala distanční výuka pomocí nejrůznějších online platforem. Některé z evropských států část platforem zakázaly využívat kvůli nedostatečnému zabezpečení osobních údajů dětí. Rezonuje tato otázka i v diskuzích mezi českými školami, resp. řediteli škol?

Škola během covidových opatření využívala v rámci distanční výuky pouze centrální platformy, které řeší ochranu osobních údajů (Bakaláři, webové stránky). Konkrétně v případě online výuky se jednalo též o zabezpečenou platformu (Microsoft Office 365 – Teams), která byla jednotným komunikačním kanálem mezi školou a žáky.

V souvislosti s covidem a distanční výukou zřídily školy svým žákům e-mailové účty. I tento úkon souvisí se zpracováním osobních údajů a přináší rizika. Jsou školní e-mailové účty využívány i v současné době?

Škola má pro žáky zřízeny centrálně účty Microsoft Office 365. Nyní jsou běžně využívány při výuce a žáci je mají k dispozici i na svých zařízeních. V rámci využití online výuky v aplikaci MS Teams byla v jednotlivých výukových blocích striktně omezena a zablokována práva pro koncové uživatele, aby nedošlo k neoprávněným přístupům.

Aktuálním problémem souvisejícím se zpracováním osobních údajů je testování tělesné zdatnosti žáků, kdy se údaje předávají České školní inspekci. Poskytla ČŠI nějakou metodiku a pomoc při realizaci tohoto projektu? Jak jste řešili zpracování osobních údajů v souvislosti s předáním údajů žáků?

Ludmila Zhoufová
je ředitelkou základní školy v Černošicích, v roce 2014 získala díky nominaci žáků titul Středočský Ámos.

Ano, ČŠI poskytla metodiku a zaslala pokyny ohledně formy a provedení testování. Přístup na portál InspIS měla pouze jedna osoba, která údaje na tento portál naimportovala a poskytla všechny požadované informace.

Rozhovor vedla Eva Janečková

Spolek pro ochranu osobních údajů se zabýval předáváním dat mimo EU a aktuální judikaturou

Online konferenci zaměřenou na předávání osobních údajů do třetích zemí uspořádal v pondělí 23. ledna Spolek pro ochranu osobních údajů. Přednášky předních odborníků zabývajících se ochranou osobních údajů a lidskými právy z několika členských zemí EU přilákaly kolem 120 účastníků z řady evropských států i USA.

Německo zastupoval člen představenstva německé asociace pověřenců BvD Christoph Bausewein a expertka na právní systém Číny a profesorka na Technické univerzitě v Braniborsku Katrin Blasek. Francii zastupoval generální sekretář EFDPO Pierre-Yves Lastic, Rakousko jednatel Research Institute – Digital Human Rights Center a člen vedení neziskové organizace NYOB Christof Tschohl. Za Českou republiku hovořil advokát ROWAN LEGAL a člen českého Spolku pro ochranu osobních údajů Filip Beneš a v neposlední řadě také Soňa Matochová z Úřadu pro ochranu osobních údajů. Konferenci moderoval Michal Nulíček, partner advokátní kanceláře ROWAN LEGAL a člen Spolku pro ochranu osobních údajů a IAPP.

O rizicích a přínosech současné regulace a praxe v oblasti předávání osobních údajů mimo EU

Účastníci v rámci panelové diskuze hovořili o rizicích a přínosech současné regulace a praxe v oblasti předávání osobních údajů mezi kontinenty. Jedná se o velmi aktuální téma, které trápí všechny společnosti, jež dnes předávají zejména data z EU do USA – ty si jednak nejsou jisté, zda je jejich aktuální přístup v souladu s GDPR, současně ale otazníky visí i nad tím, zda nové připravované rozhodnutí Komise (tzv. adequacy decision), které má situaci vyjasnit, obstojí před očekávaným soudním přezkumem evropských soudů.

Kromě Spolku bylo dalšími organizátory konference největší mezinárodní sdružení profesionálů v oblasti ochrany soukromí International Association of Privacy Professionals (IAPP) a Evropské sdružení pověřenců pro ochranu osobních údajů, jehož je český Spolek zakládajícím členem.

Další vzdělávání cílí na členy Spolku

Spolek pokračuje i ve vzdělávacích aktivitách zaměřených především na své členy. V únoru tak pokračovala tradiční série seminářů, tentokrát na téma zveřejňování soudních rozsudků. Na jaro jsou již připravována další témata, ať už z oblasti informační a kybernetic-

Další obsah

ké bezpečnosti, která je i s ohledem na novou regulaci velmi aktuální, nebo ohledně styčných bodů a rozdílů právní úpravy ochrany osobních údajů a bankovního tajemství.

Spolek pořádá diskuze k novým rozhodnutím Soudního dvora EU

Spolek pokračoval i v interních seminářích k aktuální judikatuře z oblasti zpracování a ochrany osobních údajů. Aktivita zejména Soudního dvora EU je značná, pro usnadnění orientace v jeho rozhodovací praxi tak Spolek začal v roce 2022 pořádat interní diskuze k novým rozhodnutím. Letos v pátek 20. ledna rozebírali účastníci diskuze dopady rozsudků Soudního dvora EU v kauze Google a právo na výmaz (rozhodnutí C-460/20 ze dne 8. prosince 2022), v kauze Rakouská pošta a právo na informace o zpracování osobních údajů (rozhodnutí C-154/21 ze dne 12. ledna 2023) a případ maďarského úřadu pro ochranu dat, ve kterém se řešila souběžná občanskoprávní žaloba proti správci a správní žaloba proti rozhodnutí dozorového úřadu v téže věci (rozhodnutí C-132/21 ze dne 12. ledna 2023).

Další interní seminář je v plánu 3. března

Soudy ve své aktivitě nepolevují, proto se v pátek 3. března uskuteční další interní seminář pro členy Spolku zaměřený na aktuální judikaturu.

Setkání s významnou expertkou na ochranu dat

Přednášku jedné z nejvýznamnějších odbornic na pravidla pro zpracování a ochranu osobních údajů, dlouholeté pracovnice Úřadu pro ochranu osobních údajů, členky řady mezinárodních orgánů a autorky odborných textů Miroslavy Matoušové uspořádal Spolek ve středu 1. února. Došlo i na společnou diskuzi ohledně základních otázek a poznatků z oblasti zpracování informací, řeč byla i o některých aktuálních tématech.

Pověřenec roku 2023 – nominace už jen do konce března!

Už jste nominovali některého z pověřenců pro ochranu osobních údajů roku, který by si zasloužil ocenit, vyzdvihnout? Takového, který funkci pověřence vykonával alespoň šest měsíců v roce 2022, vykonával ji kvalitně, efektivně a případně měl i přesah do dalších oblastí? Pokud ne, pak máte jedinečnou příležitost tak učinit v klání „Pověřenec pro ochranu osobních údajů roku", které Spolek pořádá již pátým rokem. Více informací a nominační formulář naleznete zde: www.dporoku.cz.

Kdo je šiřitel obchodního sdělení?

Za subjekt, který šíří obchodní sdělení, nelze považovat pouze přímého odesílatele tohoto sdělení, nýbrž subjekt, který jeho odeslání inicioval a jehož jménem došlo k jejich šíření. K takovému závěru dospěl dne 7. dubna 2020 Městský soud v Praze. Jeho rozhodnutí najdeme pod č. j. 14 A 242/2018–40. A tady jsou podrobnosti.

Základ sporu

Žalobce se podanou žalobou domáhal zrušení rozhodnutí, kterým byl zamítnut jeho rozklad a potvrzeno rozhodnutí Úřadu pro ochranu osobních údajů (ÚOOÚ). [1]

Žalovaný, kterým je v tomto případě ÚOOÚ, provedl u žalobce ve dnech 3. 11. 2017 až 8. 2. 2018 kontrolu. Podkladem pro zahájení kontroly byly stížnosti na šíření nevyžádaných obchodních sdělení. Předmětem kontroly pak bylo dodržování povinností vyplývajících ze zákona o některých službách informační společnosti, jež se týkaly rozesílání obchodních sdělení prostřednictvím elektronických prostředků. [3]

V průběhu řízení žalobce opakovaně tvrdil, že odpovědným subjektem za rozesílání obchodních sdělení může být výhradně jeho partner, společnost POLITEKS LTD, se sídlem Peremogy str. 170, 880 00 Užhorod, Ukrajina, IČO: 326 37 205 (dále jen „partner"). Žalobce upozorňoval na čl. 3.1 smlouvy uzavřené mezi ním a partnerem, dle něhož se partner zavázal pro žalobce propagovat jeho služby, a to mimo jiné zasíláním sdělení o výrobcích a službách žalobce na e-mailové adresy, k čemuž bude mít partner souhlas třetích osob. Zároveň ve smlouvě partner žalobce výslovně prohlásil, že pořádáním marketingové kampaně pro žalobce nebudou žádným způsobem porušeny právní předpisy. Smluvní strany se rovněž dohodly, že žalobce sám nebude odesílat žádná reklamní sdělení a ani mu nebudou předány žádné osobní údaje třetích osob. Žalobce také partnera po upozornění na možné protiprávní jednání ihned kontaktoval, ten jej však ujistil, že disponuje souhlasy se zasíláním obchodních sdělení. [4]

V odůvodnění rozhodnutí žalovaný mj. uvedl, že žalobce nijak nedoložil, že jeho partnerovi byly uděleny souhlasy se zasíláním obchodních sdělení ve prospěch žalobce. Dále upozornil, že je dána objektivní odpovědnost za šíření obchodních sdělení bez souhlasu adresátů, přičemž zákonné povinnosti se nelze zřeknout smluvním přenesením odpovědnosti. [7]

K rozkladu žalobce předsedkyně žalovaného prvostupňové rozhodnutí potvrdila. [8]

V odůvodnění konstatovala, že došlo k zákonem předvídanému škodlivému následku, a sice zásahu do soukromí adresátů obchodních sdělení, resp. jejich obtěžování. Stalo se tak v důsledku hromadného či opakovaného šíření obchodních sdělení elektronickými prostředky ve prospěch žalobce, a to bez souhlasu adresáta, resp. bez jejich řádného označení jako obchodních sdělení. [9]

Předsedkyně žalovaného považovala za prokázané, že k faktickému odeslání obchodních sdělení došlo z vůle žalobce na základě jím vydaného příkazu k odeslání. Je přitom nerozhodné, jaký převažující smluvní typ s partnerem uzavřel, neboť tato smlouva zavazuje výhradně inter partes. Ačkoliv nelze žalobci upřít oprávnění jednat v soukromoprávních věcech svobodně dle svého uvážení, veřejné právo včetně správní odpovědnosti za přestupky se aplikuje odděleně a nezávisle, přičemž smlouva nemůže mít vůči dozorčímu orgánu žádné účinky. Navíc i zákon předpokládá, že šiřitel může šířit obchodní sdělení nejen vlastními silami, ale i prostřednictvím jiného subjektu, kdy podle § 7 odst. 4 písm. b) zákona o některých službách informační společnosti a contrario musí každé obchodní sdělení obsahovat informaci o odesílateli, jehož jménem se komunikace uskutečňuje, resp. v jehož prospěch je obchodní sdělení šířeno. [10]

Žalobce v dané věci určil jak účel, tak i prostředky zpracování osobních údajů, čímž naplnil definici správce osobních údajů, přičemž je primárně povinností správce zajistit souladnost zpracování se zákonnými podmínkami. Pokud by bylo možno smluvně přenést odpovědnost za nezákonné šíření obchodních sdělení na jiný subjekt, a to včetně subjektů mimo místní působnost státních autorit, principy ochrany osobních údajů, jakož i soukromí v obecném slova smyslu, by byly zcela anulovány, a to za současného profitu odesílatele obchodních sdělení, jenž proces faktické rozesílky inicioval a řídil. [10]

Dále předsedkyně žalovaného uvedla, že § 11 odst. 1 zákona o některých službách informační společnosti je konstruován na základě objektivní odpovědnosti, tj. odpovědnosti za právní stav, kdy ve vztahu k právnické osobě není třeba zkoumat zavinění vzniklého protiprávního stavu. I proto je třeba za šiřitele obchodních sdělení považovat také ty osoby, které k faktickému odeslání udělily pokyn, příkaz, uzavřely smlouvu či jiným způsobem faktické odeslání obchodních sdělení iniciovaly. A bylo prokázáno, že pro ve výroku zmíněné kontakty neměl žalobce právní titul pro šíření obchodních sdělení a ani žádným dostatečně průkazným způsobem neověřil, že takovými právními tituly disponuje jeho partner, se kterým za účelem rozeslání obchodních sdělení uzavřel smlouvu. A navíc za situace, kdy byl žalobce na nezákonnost rozesílky opakovaně upozorňován, nelze pouhé slovní ujištění partnera považovat za dostatečné naplnění spravedlivě očekávatelných kroků k ověření a zabezpečení zákonnosti dalšího šíření obchodních sdělení. [12]

Obsah žaloby

Žalobce namítá, že napadené rozhodnutí nereflektuje skutečné znění zákona o některých službách informační společnosti. Žalovaný nemůže posuzovat smysl a účel tohoto zákona na základě směrnice Evropského parlamentu a Rady č. 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (dále jen „směrnice č. 2002/58/ES“), navíc při výkladu toho, co je zakázané, musí státní orgán vykládat povinnosti spíše restriktivně, než je výkladem rozšiřovat. A stanoviska publikovaná na webových stránkách žalovaného nemohou mít obecnou závaznost. [14]

Žalobce uvádí, že nebyl šiřitelem ani odesílatelem obchodních sdělení prostřednictvím elektronické pošty, a odmítá, že by měl být odpovědný za jednání partnera. Ten se zavázal provést pro žalobce marketingovou akci, přičemž žádný právní předpis neukládá žalobci povinnost ověřovat, zda disponuje rozesílatel obchodních sdělení všemi povoleními, která má mít k dispozici. Žalobce smluvně zavázal partnera k povinnosti dodržovat právní předpisy a výslovně si nechal potvrdit, že partner disponuje souhlasy (žalovaný komunikaci mezi žalobcem a partnerem značně bagatelizuje). [15]

Žalobce odkazuje na závěry odborné literatury, která neklade rovnítko mezi pojmy šíření obchodního sdělení a šíření obchodního sdělení elektronickými prostředky. I zde si žalovaný dle žalobce počíná značně extenzivně. Žalobce nesplňuje definici šiřitele obecně, protože pouze komunikoval v rámci obchodního vztahu s partnerem. Už vůbec pak nelze o žalobci uvažovat jako o šiřiteli elektronickými prostředky, protože nebyl odesílatelem obchodních sdělení prostřednictvím e-mailů. Žalobce upozorňuje, že reálně neměl žádnou možnost si ověřit, zda partnerovi byly souhlasy uděleny. I proto již ve smlouvě výslovně zakotvil smluvní povinnost partnera dodržovat právní předpisy a následně byl v dobré víře v plnění smlouvy. [17]

Vyjádření žalovaného ÚOOÚ

Žalovaný uvádí, že při výkladu právní normy se nelze omezit na její jazykový výklad. Ačkoli nelze směrnicím přiznat přímý účinek již ze smyslu jejich přijímání, tj. harmonizace práva, je zřejmé, že při interpretaci národního práva se nelze od nich oprostit. Ze směrnice č. 2000/31/ES i ze směrnice č. 2002/58/ES vyplývá, že za odesílatele obchodních sdělení je nutno považovat osobu, na jejíž objednávku obchodní sdělení probíhá, tj. osobu, jejíž zboží, služby či image je marketingovou činností podporováno. [23]

Žalovaný trvá na názoru, že žalobce je odpovědnou osobou za šíření obchodních sdělení označených ve výroku prvoinstančního rozhodnutí. [24]

Posouzení žaloby Městským soudem v Praze

Soud předně zdůrazňuje, že obecně je zasílání nevyžádaných obchodních sdělení nežádoucí, neboť odesílatel přenáší rozhodující část nákladů marketingové kampaně na někoho jiného. Náklady na distribuci nesou hlavně poskytovatelé internetových služeb a potažmo též jejich příjemci (časové či finanční). Nadto může být jejich zasíláním narušeno řádné fungování interaktivních sítí, může dojít k zahlcení mail-serverů apod. Přesto je však zasílání nevyžádaných obchodních sdělení v oblasti marketingu velmi využíváno, neboť náklady odesílatele takových zpráv jsou minimální a jím odeslané sdělení se může dostat k velkému množství adresátů. [37]

Ochranu soukromí při elektronické komunikaci zajišťuje množství zákonů (vedle dále zmíněných např. občanský zákoník nebo zákon o regulaci reklamy). V případě zasílání marketingových nabídek prostřednictvím elektronické pošty, jiných internetových komunikačních systémů, textových zpráv na mobilní telefony apod., je však nutno v prvé řadě aplikovat zákon o některých službách informační společnosti. Ten z hlediska ochrany soukromí vystupuje v postavení zvláštního zákona, který má aplikační přednost před zákonem obecným. [38]

V dané věci žalobce především zpochybňuje, zdali jej bylo možno považovat za subjekt šířící předmětná obchodní sdělení, ačkoli nebyl jejich přímým odesílatelem. [40]

Zákon o některých službách informační společnosti v rámci definičních ustanovení (viz § 2 citovaného zákona) vymezuje z hlediska subjektů zapojených do šíření obchodních sdělení elektronickými prostředky pouze poskytovatele služeb (§ 2 písm. d) a uživatele (§ 2 písm. e). Dále pak definuje obchodní sdělení (§ 2 písm. f) jakožto všechny formy sdělení, včetně reklamy a vybízení k návštěvě internetových stránek, určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku osoby, která je podnikatelem nebo vykonává regulovanou činnost. Pojem šíření obchodního sdělení, s nímž pracuje § 7 citovaného zákona, však není zákonem o některých službách informační společnosti definován. Zákon pak vůbec nezakotvuje pojem šiřitel obchodního sdělení, nýbrž odpovědnou za porušení povinností stanovených v § 7 dotčeného zákona shledává obecně jakoukoli právnickou osobu, která šíří elektronickými prostředky obchodní sdělení. [41]

Z důvodů absence bližšího vymezení pojmů šíření a šiřitel obchodního sdělení elektronickými prostředky v zákoně o některých službách informační společnosti je tudíž nezbytné jejich význam vykládat v souladu s obecnými principy, na nichž je zákon o některých službách informační společnosti vystaven, a s obecnou právní úpravou obsaženou

v zákoně o ochraně osobních údajů [1] [42], který v době posuzované kontroly platil.

Zákonem o některých službách informační společnosti byla do právního řádu ČR transponována směrnice č. 2000/31/ES a směrnice č. 2002/58/ES. Směrnice č. 2000/31/ES vymezila základní pravidla týkající se zasílání nevyžádaných obchodních sdělení, směrnice č. 2002/58/ES pak v souvislosti s elektronickými komunikacemi zakotvila ochranu osobních údajů fyzických osob, jakož i oprávněných zájmů právnických osob. Stejně tak je i základním ideovým východiskem zákona o některých službách informační společnosti posílení ochrany soukromí uživatele služby informační společnosti, kterým může být každá fyzická nebo právnická osoba. Je přitom zřejmá snaha zákonodárce docílit, aby uživatel nemusel vydávat žádné náklady na jemu doručená obchodní sdělení posílaná elektronickou poštou, která si nevyžádal a která jej ve svém důsledku obtěžují. Základním smyslem přijetí (nejen § 7) zákona o některých službách informační společnosti tedy byla ochrana adresáta před zasíláním nevyžádaných obchodních sdělení (včetně náležité identifikace těchto sdělení a jejich původce), zamezení vzniku nákladů souvisejících s nevyžádaným obchodním sdělením a zároveň přenos povinností na jejich šiřitele (to vše při zachování možnosti elektronické kontraktace). [43]

Tyto důvody musí vytvářet interpretační východiska při výkladu § 7 a § 11 zákona o některých službách informační společnosti, neboť nelze připustit výklad, který by popíral jejich smysl a účel. [44]

A takto soud musí souhlasit se žalovaným, že za osobu, jež šíří obchodní sdělení elektronickými prostředky, nelze považovat pouze jejich přímého odesílatele, nýbrž též osobu, která jejich odeslání iniciovala, dala k němu příkaz či z něj také profitovala. Jestliže cílem zákonodárce byla především ochrana adresátů obchodních sdělení před obtěžujícími marketingovými akcemi, musí výklad dotčených právních norem odpovídat tomuto záměru. Opačný výklad, tedy že za šíření odpovídá pouze faktický odesílatel, by činila předmětné právní normy ve své podstatě neúčinnými, neboť v současném digitálním světě by se skutečný šiřitel obchodního sdělení mohl velmi snadno zbavit své odpovědnosti tím, že by odesláním obchodních sdělení pověřil jinou osobu, typicky tu, která by se nacházela mimo dosah českých orgánů veřejné moci. Navíc nelze odhlédnout od faktu, že zákon o některých službách informační společnosti nehovoří o povinnostech toho, kdo rozesílá obchodní sdělení, nýbrž toho, kdo jej šíří. A takto je nezbytné považovat za šiřitele obchodních sdělení elektronickými prostředky nikoli jen subjekt, který fakticky „klikem na myš" rozešle daná obchodní sdělení, nýbrž subjekt, který dal podnět k jejich šíření ke konečným adresátům. [45]

Tomuto výkladu ostatně odpovídá také text směrnice č. 2002/58/ES, která v čl. 13 odst. 4 uvádí, že „v každém případě je nutno zakázat

praxi posílat elektronickou poštu pro účely přímého marketingu, pokud tato skrývá nebo utajuje totožnost odesílatele, jehož jménem se sdělení přenáší, anebo ji posílat bez platné adresy, na kterou by příjemce mohl odeslat žádost o ukončení zasílání takových sdělení." Z citované právní normy zjevně vyplývá, že klíčovým subjektem není odesílatel, nýbrž subjekt, jehož jménem se sdělení přenáší. A takto v daném případě zjevně vystupoval žalobce, neboť jménem žalobce bylo nabízeno předmětné zboží a partner žalobce zde vystupoval pouze jako přímý odesílatel obchodních sdělení. Nadto žalovaný správně upozornil na fakt, že předmětný článek směrnice v originálním znění hovoří dokonce o odesílateli, v jehož zastoupení či v jehož prospěch probíhá komunikace („identity of the sender on whose behalf the communication is made"). V tomto smyslu pak již vůbec nelze pochybovat o tom, že lze žalobce považovat za osobu, jež šířila obchodní sdělení ve smyslu čl. 13 odst. 4 směrnice č. 2002/58/ES a potažmo tedy též § 7 zákona o některých službách informační společnosti, který představuje transpozici předmětného článku směrnice. [46]

Na základě shora uvedeného lze tedy uzavřít, že ze smyslu § 7 zákona o některých službách informační společnosti vyplývá, že za subjekt, který šíří obchodní sdělení, nelze považovat pouze přímého odesílatele tohoto sdělení, nýbrž subjekt, který jeho odeslání inicioval a jehož jménem došlo k jejich šíření. [49]

Ze všech shora uvedených důvodů tedy soud uzavírá, že žalobce šířil předmětná obchodní sdělení elektronickými prostředky ve smyslu § 7 zákona o některých službách informační společnosti. Uvedený výklad přitom dle soudu nelze považovat za nepřípustně rozšiřující, neboť pouze sleduje hlavní cíl a účel aplikovaného zákona, aniž by nad rámec jeho znění rozšiřoval okruh subjektů, jež mohou být za dané přestupky postiženi. A na vyřčených závěrech nic nemění ani poukazy žalobce na znění komentářové literatury, neboť ta není pro soud nikterak závazná. [55]

Uvedený výklad pak není založen výhradně na stanovisku publikovaném žalovaným na jeho webových stránkách, nýbrž vychází ze zákonné úpravy ochrany soukromí před zasíláním nevyžádaných obchodních sdělení. Soud souhlasí se žalobcem, že publikovaným stanoviskům žalovaného nelze připisovat obecnou právní závaznost. Zároveň však nelze pominout, že vydání uvedeného stanoviska nemohlo u žalobce založit legitimní očekávání, že jím zastávaný výklad právní normy je správný, a proto ani tato jeho námitka neobstojí. [56]

Žalobce je tedy odpovědný za nedodržení povinností vztahujících se k šíření obchodních sdělení elektronickými prostředky v posuzovaných případech, přičemž jeho odpovědnost za nedodržení zákonných povinností nelze vztahovat pouze k uzavření smlouvy, nýbrž k celému procesu šíření obchodních sdělení elektronickými prostředky. Bylo povinností žalobce zajistit, aby obchodní sdělení elektronickými prostředky byla šířena pouze s předchozím souhlasem adresátů a zároveň byla jasně a zřetelně označena jako obchodní sdělení, a pokud tak neučinil, je odpovědný za porušení povinností vyplývajících ze zákona o některých službách informační společnosti. [57]

A svou odpovědnost žalobce nemůže přenášet na svého smluvního partnera. K tomu soud dodává, že odpovědnost právnických osob za přestupek dle § 11 zákona o některých službách informační společnosti je odpovědností objektivní. Jestliže tedy bylo objektivně zjištěno, že došlo k porušení zákonných povinností, nemůže se žalobce odpovědnosti za jejich porušení zprostit odkazem na smluvní ujednání či odkazem na porušení povinností ze strany smluvního partnera. Soud je srozuměn s omezenými možnostmi žalobce zajistit, aby skutečný odesílatel obchodních sdělení dodržel zákonem daná pravidla. Tato skutečnost však nic nemění na odpovědnosti žalobce za případné nedodržení zákonných povinností, neboť to byl stále on, kdo byl šiřitelem předmětných obchodních sdělení. Případné uplatnění regresního nároku vůči smluvní straně, jež nedodržela smluvní podmínky a porušila zákonná ustanovení, nepředstavuje hledisko, jež by bylo určující pro správní orgány při rozhodování o odpovědnosti a spáchaný přestupek. [58]

Zpracovala Eva Janečková

1) Zákon platný v době posuzované kontroly

Předávání osobních údajů do USA: Je to stále problém?

Od účinnosti obecného nařízení o ochraně osobních údajů prošla oblast předávání osobních údajů do USA řadou změn. Ve stručnosti si připomeňme rozsudek Soudního dvora EU ve věci Schrems II (věc C-311/18), který v roce 2020 zneplatnil možnost předávat osobní údaje subjektů údajů do USA na základě rozhodnutí o odpovídající úrovni ochrany soukromí, jež bylo v USA zajištěno tzv. Privacy Shieldem, ke kterému se mohly dobrovolně zavázat ty společnosti, jež chtěly touto cestou zpracovávat osobní údaje z EU, resp. EHP.[1] V praxi jsme se jako pověřenci pro ochranu osobních údajů setkávali především s tím, že jsme před začátkem spolupráce z pohledu správců osobních údajů posuzovali, zda je dovozce údajů zavázán k Privacy Shieldu, což ovšem nebylo nijak procesně složité. De facto tak učinily samy americké společnosti, které se jednoduchým prohlášením na svých webových stránkách zavázaly k dodržování pravidel z Privacy Shieldu s tím, že navíc musely svůj závazek oznámit ministerstvu obchodu USA.

Otázku reálného souladu s Privacy Shieldem bych nechala otevřenou. V současné době, kdy je prováděcí rozhodnutí Komise (EU) o odpovídající úrovni ochrany poskytované Privacy Shieldem prohlášeno za neplatné, je možné, aby správce či zpracovatel předával osobní údaje do USA, pokud mu spolupracující správce nebo zpracovatel poskytne vhodné záruky dle článku 46 GDPR, kterými jsou buďto závazná podniková pravidla, která ale platí jen pro členy skupiny, nebo standardní smluvní doložky, kde je však na vývozce údajů naložena nesnadná povinnost posoudit konkrétní třetí zemi, zda nesnižuje účinnost vhodných záruk, a dle výsledku případně nastavit další vhodná opatření. Veškeré kroky v této oblasti musí provádět vývozce s náležitou péčí a rovněž je dokumentovat.

Od roku 2021 máme k dispozici upravené znění standardních smluvních doložek, jež nahrazuje původní verzi s cílem zohlednit rozsudek Soudního dvora EU ve věci Schrems II, kde Soudní dvůr rozhodl, že článek 46 GDPR musí být vykládán v tom smyslu, že vhodné záruky a práva poskytovaná na základě standardních smluvních doložek (SSD) poskytnou takovou úroveň ochrany, která bude shodná s úrovní ochrany v EU poskytovanou skrze GDPR ve spojení s Chartou základních práv Evropské unie.

Nové SSD poskytují evropským vývozcům *(vývozcem je dle nových SSD jak správce, tak zpracovatel předávající osobní údaje do třetí země)*[2] údajů jasné požadavky týkající se mezinárodního předávání údajů, a tedy více než dva roky po rozhodnutí ve věci Schrems II mají evropští správci a zpracovatelé údajů konečně poměrně stabilní právní pokyny, pokud jde o mezinárodní předávání údajů, a to jak obecně, tak zejména pro USA. Vzhledem k tomu, že většina správců a zpracovatelů osobních údajů má nějaké obchodní partnery se sídlem v USA a takové obchodní vztahy často vyžadují výměnu osobních údajů, byl vývoj v oblasti ochrany osobních údajů do USA v posledních dvou letech více než vítán. Ačkoliv mnoho příjemců údajů v USA, zejména větších poskytovatelů služeb působících dříve na základě Privacy Shieldu, okamžitě po rozsudku ve věci Schrems II přešlo na tehdy platné SSD, právní nejistota přetrvávala kvůli vágně formulovaným požadavkům Soudního dvora EU na další ochranná opatření. Tyto požadavky byly vyjasněny, když Evropská komise v červnu 2021 vydala nové SSD, které musely nejpozději od 27. prosince 2022 nahradit původní SSD.

Níže je stručně uvedena struktura nových SSD a požadavek na posouzení vlivu předávání údajů a také výhled pro nový transatlantický rámec ochrany osobních údajů mezi USA a EU, který snad již brzy nahradí zrušený Privacy Shield.

Nové SSD a struktura:

Jak bylo uvedeno výše, Komise (EU) v červnu 2021 zveřejnila nové standardní smluvní doložky pro předávání osobních údajů mezi Evropskou unií a třetími zeměmi.

Struktura nových SSD se řídí čtyřmi scénáři předávání[3]:

1. **Správce – správce (první modul)**
2. **Správce – zpracovatel (druhý modul)**
3. **Zpracovatel – subzpracovatel (třetí modul)**
4. **Zpracovatel – správce (čtvrtý modul)**

V souladu s čl. 3 odst. 2 obecného nařízení nové SSD výslovně stanoví, že vývozce údajů může být usazen mimo EU. To znamená, že správce nebo zpracovatel osobních údajů se sídlem mimo EU může uzavřít nové SSD se svým zpracovatelem nebo subzpracovatelem. Dále může nové dohody o spolupráci uzavírat více stran, které obsahují mechanismus, jenž umožňuje pozdější přidání nových stran. Rovněž pokud strany uzavřou druhý nebo třetí modul nových SSD, není třeba uzavírat samostatnou smlouvu o zpracování osobních údajů podle čl. 28 GDPR, neboť tyto doložky již obsahují všechna ustanovení požadovaná podle čl. 28 GDPR.

Doložka 14 SSD[4] je nová a pravděpodobně povede k dalšímu papírování. Při předávání osobních údajů do třetí země jsou strany povinny **posoudit právní předpisy** a postupy této **země, které se vztahují na zpracování osobních údajů dovozcem údajů**, včetně případných požadavků na zveřejnění osobních údajů nebo opatření umožňujících přístup orgánů veřejné moci a bránících dovozci údajů v plnění jeho povinností podle nových SSD.

Toto posouzení je posouzením vlivu na předávání údajů **(DTIA)**, které by nemělo být zaměňováno s posouzením vlivu na ochranu údajů (DPIA) podle čl. 35 GDPR. DTIA vyžaduje, aby strany posoudily zejména následující

1) Rozsudkem Soudního dvora Evropské unie ve věci C-311/18 Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems (tzv. Schrems II) ze dne 16. července 2020
2) Prováděcí rozhodnutí Komise (EU) 2021/914 ze dne 4. června 2021 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle nařízení Evropského parlamentu a Rady (EU) 2016/679)
3) https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32021D0914&from=EN
4) Doložka 14 PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2021/914

skutečnosti: konkrétní okolnosti předání, počtu zúčastněných subjektů a použitých přenosových kanálů, zamýšlená další předání, typ příjemce, účel zpracování, kategorie a formát předávaných osobních údajů, hospodářské odvětví, v němž k předání dochází, místo uložení předaných údajů, zákony a postupy cílové třetí země.

Souhrnně řečeno, evropští vývozci údajů (včetně těch, kteří nemají sídlo v EU, ale podléhají GDPR podle čl. 3 odst. 2), musí analyzovat role stran (včetně možných dalších předání) a určit příslušné moduly včetně případných požadovaných záruk a dalších posouzení, jak bylo uvedeno výše.

V praxi je tak DTIA s největší pravděpodobností největší výzvou nových SSD, protože strany budou muset posuzovat rizika nejen s ohledem na prvního příjemce údajů (a skutečného smluvního partnera), ale také s ohledem na následné všechny zpracovatele osobních údajů, kteří nemusí být tak ochotní odpovídat na komplexní dotazníky, jež se týkají jejich procesů zpracování, technických a organizačních opatření atd.

Evropský sbor pro ochranu osobních údajů (EDPB) se již pokusil konkretizovat povinnost uvedenou v doložce 14 nových SSD ve svých rozsáhlých doporučeních 01/2020, o opatřeních, která doplňují nástroje předávání k zajištění souladu s úrovní ochrany osobních údajů v EU ze dne 18. června 2021.[5)]

Ať už někdo považuje tato doporučení za užitečná, nebo ne, vývozci údajů jsou při analýze práva USA stále odkázáni sami na sebe. Na začátku roku 2022 zveřejnila německá konference o ochraně údajů odborné stanovisko právního experta Stevena Vladecka, který působil také jako soudní znalec v řízení Schrems II před irským soudem. Toto stanovisko může být užitečné pro evropské vývozce údajů při analýze právní situace v USA obecně. Přesto však konkrétní posouzení s ohledem na skutečná rizika konkrétního předávání údajů musí provést samotné strany.

Je nový transatlantický rámec ochrany osobních údajů mezi EU a USA na dohled?

V březnu roku 2022 USA a EU oznámily, že se v zásadě dohodly na novém transatlantickém rámci ochrany osobních údajů (TADP), který má nahradit štít na ochranu soukromí. Nový rámec se zabývá zejména obavami Soudního dvora EU ohledně stupňujících se pravomocí amerických sledovacích agentur a na straně USA se zavazuje k provedení reforem, které posílí ochranu soukromí a občanských svobod vztahující se na zpravodajské činnosti USA. V říjnu 2022 podepsal americký prezident Joe Biden v rámci rámce TADP exekutivní příkaz, který omezuje možnosti amerických národních bezpečnostních agentur přistupovat k osobním údajům lidí.

Rámec TADP předpokládá například tyto klíčové zásady: nový soubor pravidel a závazných záruk, které omezí přístup zpravodajských orgánů USA k údajům na míru nezbytnou a přiměřenou ochraně národní bezpečnosti, nový dvoustupňový systém pro vyšetřování a řešení stížností Evropanů týkajících se přístupu zpravodajských orgánů USA k údajům, jehož součástí bude soud pro přezkum ochrany údajů, přísné povinnosti pro společnosti zpracovávající údaje předávané z EU a požadavek, aby samy prostřednictvím amerického ministerstva obchodu certifikovaly dodržování zásad.

Jakmile bude rámec TADP platit, mohou evropští vývozci údajů zjistit, že se jedná o méně komplikovaný právní nástroj pro předávání údajů do USA, protože břemeno dokumentace a dodržování předpisů bude částečně přeneseno na zúčastněné dovozce údajů do USA. Na začátku roku 2023 dle tiskové zprávy Komise (EU) tak máme k dispozici informace, že byl návrh TADP předán Evropskému sboru pro ochranu osobních údajů (EDPB).[6)]

Bude nový transatlantický rámec ochrany osobních údajů jednodušším řešením pro předávání údajů do USA? Doufám, že ano. A vy? V mezičase, než se dořeší nový transatlantický rámec ochrany osobních údajů, může čtenářům časopisu DPO PRO pomoci dokument Otázky a odpovědi k novým SSD, který je k dispozici na webu Komise (EU).[7)]

Monika Kovář Staňková
Senior Compliance Advisor ČSOB

5) https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_cs
6) https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632
7) Questions and Answers for the two sets of Standard Contractual Clauses. K dispozici na: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Bankovní identita a zpracování osobních údajů

Bankovní identita je metoda digitálního ověření totožnosti osob poskytovaná bankami. Funguje v celé řadě zemí (Dánsko, Holansko, Švédsko), u nás pod značkou BankID. Využití bankovní identity zjednodušuje přístup uživatelů jak ke službám, které poskytuje stát, tak ke službám některých soukromých společností. Tato metoda funguje stejně jednoduše jako přihlášení do internetového bankovnictví. Společnost Bankovní identita, a.s., která tuto metodu zaštiťuje, byla založena v září 2020. Jejími akcionáři je devět českých bank. Konkrétně pak Air Bank, Česká spořitelna, ČSOB, Fio banka, Komerční banka, mBank, MONETA Money Bank, Raiffeisenbank a UniCredit Bank.

Vývoj právní úpravy

Digitální identitu občana lze nalézt již v zákoně č. 111/2009 Sb., o základních registrech, kdy dle § 4 odst. 1 základní registr obsahuje mj. identifikátory fyzických osob. Elektronickou identifikaci osob pak představuje právní úprava zákona č. 250/2017 Sb., o elektronické identifikaci, který zakotvuje možnost prokázat totožnost využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace, a to přes národní bod pro identifikaci a autentizaci (NIA). NIA přitom fungovala jako prostředník pro výměnu informací mezi kvalifikovaným správcem (státní orgán nebo akreditovaná osoba) a kvalifikovaným poskytovatelem, kterým je státní orgán nebo soukromoprávní subjekt, jenž provozuje online službu nebo jinou činnost, při nichž je vyžadováno prokázání totožnosti prostřednictvím NIA s využi-

tím elektronické identifikace v souladu se zákonem o elektronické identifikaci. Seznam kvalifikovaných poskytovatelů vede ministerstvo vnitra [1].

Právní úprava a její důsledky

Právní úpravu bankovní identity lze najít v zákoně č. 49/2020. Nejedná se však o právní úpravu, která by bankovní identitu zakotvovala, ale o novelizaci čtyř právních předpisů [2]. Pro banky ve smyslu § 1 zákona č. 21/1992 Sb., o bankách, obecně platí, že mohou vykonávat pouze ty činnosti, které jsou uvedeny v bankovní licenci, o jejímž vydání dle § 4 odst. 2 zákona o bankách rozhoduje Česká národní banka. Novela zákona o bankách rozšířila úpravou § 1 odst. 4 písm. c) okruh činností, které může banka vykonávat. Banka tedy může vykonávat *„podnikatelskou činnost spočívající v poskytování elektronické identifikace, autentizace a služeb vytvářejících důvěru, jak jsou definovány přímo použitelným předpisem Evropské unie upravujícím elektronickou identifikaci a služby vytvářející důvěru pro elektronické transakce na vnitřním trhu, jakož i souvisejících služeb, zejména poskytování nebo potvrzování osobních identifikačních údajů klienta, informací o klientovi souvisejících s jeho osobními identifikačními údaji, informací o bankovních obchodech klienta a vytváření a uchování elektronických dokumentů (dále jen „identifikační služby"), je-li držitelem příslušného oprávnění, pokud je právními předpisy vyžadováno"*.

Na základě této novelizace tak mají klienti bank možnost přistupovat ke službám státu za použití svých přihlašovacích údajů do svého online bankovnictví (bankovní identita) a hledí se na ně jako na ověřené uživatele [3]. Předpokladem pro to je zákonné zmocnění v § 38aa odst. 1 zákona o bankách, na jehož základě mohou banky nabízet, poskytovat nebo zprostředkovat identifikační služby a uzavírat smlouvy o nich též jménem a na účet poskytovatele identifikačních služeb.

Poskytovatelem identifikačních služeb je momentálně společnost Bankovní identita, a. s., která byla založena v září 2020 a jejímiž akcionáři je devět českých bank [4].

Co to znamená pro běžného uživatele?

Pro běžného uživatele to tedy znamená, že při komunikaci se státem (např. při podání daňového přiznání) může využít běžně využívaných přihlašovacích údajů do svého elektronického bankovnictví, aby se prostřednictvím poskytovatele identifikačních služeb (Bankovní identita, a. s.) s daným státním orgánem elektronicky spojil a tento státní orgán aby věděl, že se jedná o ověřenou fyzickou osobu, kterou není nutné dalším způsobem ztotožňovat za účelem ověření její identity. Jedná se tedy o zjednodušení přístupu občanů ke službám státu, kdy uživateli postačí znát přihlašovací údaje ke svému elektronickému bankovnictví a díky tomuto jednomu přihlašovacímu údaji má možnost vzdáleně přistoupit ke službám státu a stát na tohoto uživatele hledí jako na ověřeného. K tomu je třeba dodat, že definici poskytovatele identifikačních služeb obsahuje § 38a a odst. 2 zákona o bankách a dle tohoto ustanovení jím může být *„osoba, která není bankou, je na základě jiného právního předpisu oprávněna poskytovat identifikační služby a ve které mají podíl pouze banky nebo pobočky zahraničních bank; tyto banky nebo pobočky zahraničních bank jsou povinny zajistit, že poskytovatel identifikačních služeb bude zachovávat získané údaje v tajnosti a chránit je před zneužitím"*.

Když si to shrneme…

Výše uvedené můžeme shrnout tak, že bankovní identita je metoda digitálního ověření totožnosti uživatele a tento uživatel se pomocí jednoho přihlašovacího údaje může spojit s některým státními institucemi a komunikovat s nimi na dálku. Obdobné platí rovněž pro využití služeb některých společností ze soukromého sektoru. Vychází se přitom z předpokladu, že subjekty poskytující bankovní služby, které jsou regulovány poměrně přísnou legislativou, mají o svých klientech ty nejaktuálnější informace.

Technický aspekt bankovní identity

Při zvoleném způsobu přihlášení do určité služby za pomocí BankID prochází uživatel standardním přihlášením u své banky. Po dokončení procesu přihlášení je zobrazena výzva k potvrzení předání údajů pro toto jedno konkrétní přihlášení. Toto rozhodnutí nelze nijak uložit za účelem budoucího automatického souhlasu, ale je třeba ho udělit při každém přihlášení znovu. Po udělení souhlasu ohledně předání údajů dochází k přesměrování do cílové služby skrze ověřovací požadavky do služby NIA.

Společnost Bankovní identita, a.s., funguje jako agregátor bankovních API [5] **a poskytuje služby komerčním subjektům**. Připojením na bankovní identitu získá společnost možnost online ověřovat a komunikovat se svými klienty. V roce 2023 by se měly připojit také další banky.

Společnost Bankovní identita, a. s., vůbec nevstupuje do datové komunikace při procesu ověřování identity uživatele (mezi státem a bankou). Banky jsou totiž přímo napojeny do služby NIA ID. To je identifikační prostředek, který umožní zaručené ověření totožnosti při přihlašování k některým online službám. Jedná se soubor identifikátorů dané osoby, kterými jsou například jméno osoby, datum narození, rodné číslo, číslo dokladu apod. Konkrétní identifikátory předávané při daném procesu přihlášení ze strany banky do cílové služby se pak liší a záleží primárně na nastavení a potřebách cílové služby.

Komerční využití

Jak už jsme popsali v úvodu, služba BankID není určena pouze pro přihlašování do služeb zřízených či spravovaných státem, ale může sloužit i pro soukromé subjekty, které tento způsob přihlášení do svých služeb nabízejí. Tuto metodu využívá například firma **Seznam.cz, a.s.**, pro svůj online inzertní portál sbazar.cz, díky čemuž svítí takto přihlášeným uživatelům štítek s ověřením a ostatní uživatelé se tak nemusí obávat podvodů.

1) https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx
2) zákon č. 21/1992 Sb., o bankách, zákon č. 277/2009 Sb., o pojišťovnictví, zákon č. 168/1999 Sb., o pojištění odpovědnosti za škodu způsobenou provozem vozidla a zákon č. 253/2008 Sb., o některých opatření proti legalizaci výnosů z trestné činnosti a financování terorismu.
3) Zákon ale pojem bankovní identita výslovně neuvádí, a proto je třeba ho vnímat jako záznam, který o svém klientovi vede banka.
4) https://www.bankid.cz/o-nas
5) API neboli **aplikační programové rozhraní**, slouží k datové komunikaci mezi softwarovými aplikacemi.

Do budoucna bude jistě přibývat soukromých subjektů, které tento způsob přihlášení svým uživatelům umožní. Pro firmy je samotná implementace BankID jednoduchá a zároveň je to příležitost k rozsáhlejší změně a **digitalizaci zákaznických procesů**. Pro Česko je to šance, jak se posunout mezi digitální šampiony. Nutno však dodat, že soukromé firmy musí za používání BankID platit. Nejedná se přitom jen o tzv. zřizovací poplatek, ale i o další platby za každý ověřený kontakt, který je účtován ve více variantách.

Míra používání

Poslední čísla ukazují[6], že bankovní identitu využívá celkem cca 5,5 mil. klientů jednotlivých bank. Od poloviny roku 2023 by mělo být možné přes bankovní identitu ztotožňovat i cizince, kteří mají v ČR trvalý nebo přechodný pobyt. I těm se tak výrazně zjednoduší některé úkony.

Použití BankID v praxi

Bankovní identita zaručuje snazší přihlášení do služeb zřízených nebo spravovaných státem. U některých z těchto služeb si proto vůbec nemusíme pamatovat unikátní přihlašovací jména a hesla a můžeme se do nich přihlásit pouze tímto jedním univerzálním přístupem. Například u služby Datové schránky je tato možnost k nezaplacení.

Situace, kdy má jedna osoba zřízené celkem tři datové schránky, není vůbec nestandardní. Představme si, že daná osoba je jednatelem podnikatelského subjektu a k tomu sama provozuje určitou činnost jako OSVČ. A jelikož si chce maximálně zjednodušit komunikaci se státní správou, založí si schránku také jako fyzická nepodnikající osoba. Pro každou z těchto tří uvedených rolí má pak osoba samostatně fungující datovou schránku a bohužel se zcela rozdílnými přihlašovacími údaji. Zda je to správný postup ze strany zřizovatele datových schránek, je ale už na jinou debatu. Výhodou je však to, že si tato osoba nemusí pamatovat současně všechny tři přístupy. Přihlášením skrze službu bankovní identity a po úspěšném procesu ověření si už pak snadno vybere, do které z přístupných datových schránek chce nahlížet.

Ochrana osobních údajů

Z logiky celého fungování bankovní identity je zřejmé, že její esenciální podstatou je zpracování osobních údajů, a to na všech stranách, tj. na straně banky, společnosti Bankovní identita, a. s., a u cílového poskytovatele služby. Otázkou však je, jaké je postavení těchto subjektů, které digitální ověření totožnosti poskytují, zda je třeba mít uzavřenou smlouvu o zpracování osobních údajů a jaká jsou potenciální rizika této služby.

Banka

Banka bude v postavení správce osobních údajů ve smyslu čl. 4 bod 7 obecného nařízení, kdy osobní údaje svých klientů banka zpracovává za účelem plnění smlouvy mezi subjektem údajů a bankou, přičemž využívá svých technických prostředků, aby splnila, co je předmětem smlouvy mezi ní a subjektem údajů. Nejedná se však o smlouvu zakládající základní vztah mezi bankou a fyzickou osobou, ale o další smlouvu, kterou může klient banky s bankou uzavřít a jejímž předmětem je poskytování bankovní identity. Např. v případě České spořitelny, a. s., se smlouva o bankovní identitě dále odkazuje na všeobecné obchodní podmínky[7], které v bodě 2.5 bankovní identitu dále popisují a odkazují se rovněž na dokument s výčtem podporovaných aplikací[8]. Banka však v rozsahu zákonného zmocnění v § 4 odst. 1 písm. c) zákona o bankách na základě smlouvy mezi ní a subjektem údajů při přihlášení subjektu údajů do svého elektronického bankovnictví subjekt údajů ověří, deklaruje, že se skutečně jedná o konkrétně ověřenou fyzickou osobu, a tyto informace (informaci o ověření) předá dalšímu „hráči". Vždy se tak ale děje pouze na pokyn klienta banky (subjektu, který chce využít možností bankovní identity).

Bankovní identita, a. s.

Výše uvedeným „hráčem" je společnost Bankovní identita, a. s., která je v postavení poskytovatele identifikačních služeb ve smyslu § 38aa odst. 2 zákona o bankách. Při využití bankovní identity tedy subjekt údajů své bance vydává pokyn k tomu, aby banka předala osobní údaje Bankovní identitě, a. s., která je následně předává koncovému subjektu, jenž klientovi banky poskytne online službu, o níž žádá. Rozsah zpracovávaných osobních údajů odpovídá rozsahu, k jakému dal uživatel služby bankovní identita pokyn, především se bude jednat o jméno, příjmení, datum narození, adresu pobytu, kontaktní a platební údaje a informace o tom, kdo údaje Bankovní identitě, a. s., předává (jaká banka) a komu mají být předány (koncový subjekt – poskytovatel online služby). Poskytovatel identifikačních služeb tak je rovněž v postavení správce osobních údajů ve smyslu čl. 4 bod 7 GDPR.

Doba trvání uložení pak odpovídá době, která je nutná pro předání osobních údajů. Po této době se osobní údaje uchovávají v pseudonymizované podobě po dobu, po kterou trvají promlčecí nároky.

Koncový subjekt

Pod pojmem koncový subjekt je možné si představit jak orgány státu, tak soukromoprávní subjekty, které s Bankovní identitou, a. s., uzavřou smlouvu. Některé z těchto smluv je možné nalézt také v registru smluv[9]. Z náhledu do těchto smluv je zřejmé, že obě smluvní strany se identifikují jako správci osobních údajů. Je to logický závěr, neboť obě smluvní strany samy určují své účely a prostředky zpracování osobních údajů. Koncovým subjektem však může být rovněž místní samospráva, kdy prostřednictvím bankovní identity je možné hradit místní poplatky. Jejich seznam je možné nalézt na portálu identity občana[10].

Ukázka

Službu BankID si může každý prakticky vyzkoušet pod odkazem https://demo.bankid.cz/

Evropský rozměr

V souvislosti s využíváním služby bankovní identity lze poukázat rovněž na činnost Komise, která v červnu 2021 navrhla rámec pro evropskou digitální identitu, která by byla dostupná formou evropské peněženky digitální identity. Tento navrhovaný rámec mění

6) Zmiňuje sám poskytovatel BankID na https://www.bankid.cz/cenik
7) https://www.csas.cz/static_internet/cs/Redakce/Ostatni/Ostatni_IE/Prilohy/vseobecne-obchodni-podminky-ceske-sporitelny-soukroma-klientela-31-10-2018.pdf
8) https://www.csas.cz/content/dam/cz/csas/www_csas_cz/dokumenty/obecne/podporovane_aplikace.pdf
9) https://smlouvy.gov.cz/vyhledavani
10) https://info.identitaobcana.cz/sep/

nařízení eIDAS[11]. Cílem úpravy je povinnost členských států vydávat digitální peněženku na základě společných technických norem a v návaznosti na povinnou certifikaci v rámci oznámeného systému elektronické identifikace.

Tato identita by měla sloužit k online i offline prokazování nebo ověřování totožnosti. O digitální peněženku bude moci požádat každý občan EU a rezident s trvalým pobytem v EU. Cílem je vytvořit e-identitu každého občana EU, tak, aby při využívání různých služeb (objednávka jídla, půjčení kola, komunikace se státem apod.) nebylo nutné vždy zakládat novou identitu pro každou z těchto služeb, ale aby bylo možné využít jednu již existující identitu, kdy každý bude moci rozhodnout, jaký rozsah osobních údajů poskytne. Předsedkyně EU Ursula von den Leyen k tomu řekla:

„Pokaždé, když nás aplikace nebo webové stránky požádají o vytvoření nové digitální identity nebo o snadné přihlášení přes velkou platformu, nemáme ponětí, co se stane s našimi údaji ve skutečnosti. Komise proto navrhne vytvořit bezpečnou evropskou e-identitu. Takovou, které věříme a kterou může každý občan využít kdekoli v Evropě k čemukoli, od placení daní až po půjčení jízdního kola. Půjde o technologii, díky níž si můžeme sami kontrolovat, která data se používají a jak.“

Evropská digitální identita má být využitelná různými způsoby – pro otevření bankovního účtu, k podání daňového přiznání, pro prokázání věku, pronájem vozidla prostřednictvím digitálního řidičského průkazu apod.

Otázkou dle našeho názoru zůstává, jak by v praktickém měřítku měla digitální peněženka vypadat, a to především s ohledem na zajištění bezpečnosti údajů, které by měla obsahovat. V tuto chvíli se jeví jako vysoce pravděpodobné, že by se jednalo o mobilní aplikaci, ve které by uživatel spravoval své osobní údaje a další informace. Mobilní telefon jako zařízení, které se stalo běžnou součástí našich životů, se na jednu stranu může jevit jako vhodný prostředek, ale je třeba upozornit i na rizika, která jsou s tím spojena – ztráta signálu (ano, ještě dnes taková místa existují, byť je otázka, zda právě v nich by bylo nutné prokázat svoji totožnost), odcizení nebo ztráta mobilního telefonu, ale rovněž možnost vybití baterie nebo mechanické poškození mobilního telefonu.

Sečteno a podtrženo

Je skvělé, že doba a stav digitalizace na území našeho státu pokročila a máme k dispozici další velmi užitečný nástroj, kterým BankID zajisté je. I výše uvedený evropský záměr ukazuje, že trend je patrně již nastaven a je pouhou otázkou času, kdy se více a více služeb včetně těch poskytovaných státem přesune do online prostoru. Tato cesta s sebou nese celou řadu pozitiv, avšak zároveň nese i nároky jak na jednotlivé koncové subjekty poskytující své služby, tak především na nás uživatele. A stále je třeba pamatovat na to, že ne všichni chtějí své záležitosti vyřizovat digitálně nebo že je pro některé tento způsob příliš náročný, protože rychlost, s jakou se technologie prolínají běžným lidským životem, se neustále zvyšuje a každý nemusí zvládat toto tempo udržet. Kromě toho je třeba mít také na paměti rizika, která jsou s digitalizací spojena. Ať už se jedná o snazší cestu k odcizení identity člověka nebo o situaci, kdy našemu mobilnímu zařízení jednoduše „dojde šťáva“ a nebude po ruce nabíječka nebo přímo nebude „šťáva“ (riziko blackoutu).

David Musil
Autor je vedoucí vývojář v Davmo Software, s.r.o.

Vojtěch Dlouhý
Autor je právník, zabývá se ochranou osobních údajů

11) nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a o službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Osobní údaje ve zpravodajích – vybrané střípky

Zajímá vás téma ochrany osobních údajů v obecních či městských zpravodajích? A chcete vědět, co se o tom uvádí v obecném nařízení o ochraně osobních údajů? Vybrali jsme pro vás několik důležitých střípků, které se vztahují k nejčastějším dotazům, s nimiž se ve zmíněných souvislostech pověřenci setkávají.

Nejprve je nutné podotknout, že se následující právní předpisy uplatní v případech, kdy se v daném obecním zpravodaji vyskytují osobní údaje fyzických osob, jako jsou např. přistěhovalí, nově narození občané, jubilanti, výherci soutěží, také údaje osob zdokumentovaných v popiscích pod fotografiemi apod. Obec sama rozhoduje o tom, jaké osobní údaje se ve zpravodaji objeví. Žádný právní předpis nestanovuje povinnost místní periodikum vydávat, natož pak konkrétní specifikace možných osobních údajů zveřejněných v takovém periodiku. Jak se na tuto problematiku dívat z pohledu ochrany osobních údajů a soukromí?

Nejtypičtější příklady zveřejňování osobních údajů v obecních zpravodajích

V rámci transparentnosti a dostatečného informování veřejnosti obec zveřejňuje ve zpravodaji zápisy ze zasedání zastupitelstva, rady a komisí. Je toto zveřejnění možné?

K tématu zápisů ze zastupitelstva uvádí zákon č. 128/2000 Sb., o obcích (dále jen „obecní zřízení“), pouze to, že *„zápis, který je nutno pořídit do 10 dnů po skončení zasedání, musí být uložen na obecním úřadu k nahlédnutí“* (§ 95 obecního zřízení). O zveřejnění zápisů ze zastupitelstva obce se pak v zákoně vůbec nepíše, tudíž jakékoliv zveřejnění zápisů ze zastupitelstva je **dobrovolné, nikoliv nemožné.** V případě takového zveřejňování by zápis neměl obsahovat nadbytek osobních údajů. Při dobrovolném zveřejňování je možné ponechat osobní údaje veřejných představitelů, zaměstnanců a příjemců veřejných prostředků nejvýše v rozsahu dle § 8b Infozákona. Je důležité si uvědomit, že § 8b hovoří o maximálním možném rozsahu.

Zveřejňování zápisů ze zastupitelstva, usnesení zastupitelstva, zápisů z rady, výborů či komisí je bezpochyby možné, je však třeba dbát na ochranu osobních údajů a nezveřejňovat osobní údaje s výjimkou základních údajů veřejných představitelů, zaměstnanců a příjemců veřejných prostředků.

Významná životní jubilea nebo nově narození: Zástupci obce chodí gratulovat k takovým událostem, obec by však ráda k takovým jubileím pogratulovala i v obecním zpravodaji. Může?

Ve zpravodajích obce se často objevují osobní údaje žijících fyzických osob, a to zejména ve čtenáři velmi oblíbených rubrikách věnovaných jubilantům či nově narozeným dětem, novomanželům, osobám, které se odstěhovaly nebo přistěhovaly atd. Vyjádření Úřadu pro ochranu osobních údajů (dále jen jako „ÚOOÚ“) upřesňuje, co umožňuje § 36a obecního zřízení, který stanovuje, že *obec může ocenit významné životní události svých občanů. Nezbytné osobní údaje jubilantů může obec za tímto účelem získávat z evidence obyvatel, v souladu s § 4 odst.* Při zveřejnění takových osobních údajů v obecním zpravodaji je ale třeba mít na paměti, že lze použít jen takové údaje, které jsou nezbytné ke splnění daného účelu. V případě zveřejnění osobních údajů jubilantů v regionálním tisku je dle ÚOOÚ přípustné, aby se osobní údaje objevovaly pouze v rozsahu jméno a příjmení.

V případě, že se v tisku objeví i další osobní údaje (např. rok narození, věk, bydliště, místní část), je nutné k tomu získat souhlas od subjektů údajů. Možná je například následující textace: *„V měsíci květnu oslaví životní jubileum Jan Novák, Vladimíra Koutná,…“* Pokud jsme si na základě osobní znalosti jisti, že jubilant/ka souhlasí a bude potěšen/a podrobnějším údajem, bylo by ještě přijatelné např. sdělení *„V květnu oslaví krásných 90 let Božena Zmatlíková.“* Takovéto zveřejnění pak není zpracováním osobních údajů.

Za určitých podmínek tedy není problém zveřejnit ocenění životních jubileí občanů např. v místním periodiku. Nade vše se však staví vůle daného občana. Pokud si takové zveřejnění občan nepřeje, měla by to obec respektovat a ocenění nezveřejňovat.

Obec pořádá velké množství akcí, kde pořizuje fotografie. Mezi nejoblíbenější patří např. dětský den. Je možné publikovat fotografie z těchto akcí v obecním zpravodaji?

V případě fotografie, která bude přílohou reportážního článku ze společenské, kulturní či sportovní akce, a která nebude zahrnovat osobní údaje v článku či v popisku, bude tedy zveřejněna pouze s reportážním článkem bez dalšího, nejde o zachycení podoby ve smyslu § 84 občanského zákoníku ani o zpracování osobních údajů, a tudíž je možné ji bez dalších komplikací zveřejnit. Z takové fotografie nelze určit totožnost osoby, která je na fotografii zobrazena, a nelze ji tudíž identifikovat. I v případě portrétu, kde místní identifikují svého souseda, se uplatní zpravodajská licence, jak uvádíme dále. K pořízení a zveřejnění takové fotografie není třeba získávat svolení ani souhlas se zpracováním osobních údajů.

O zpracování osobních údajů nejde ani ve chvíli, kdy se k fotografii připojí jméno a příjmení osoby, která je na fotografii zachycena. Se samotným zveřejněním takové fotografie včetně osobních údajů v rozsahu jméno a příjmení pak počítá § 89 občanského zákoníku, který stanovuje, že *„Podobizna nebo zvukový či obrazový záznam se mohou bez svolení člověka také pořídit nebo použít přiměřeným způsobem též k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství.“* V tomto případě mluvíme o tzv. zpravodajské nebo umělecké licenci. Jedná-li se tedy o reportážní fotografii s uvedením jména a příjmení osoby (či více osob) na ní, která bude zveřejněna ve zpravodaji obce, není vyžadováno ani svolení dle občanského zákoníku, jelikož se jedná o již zmíněnou zpravodajskou licenci. Podmínkou je, že se neuvedou další identifikační údaje (např. bydliště, věk, místní část, kde občan bydlí, atd.). V takovém případě pak stále nejde o zpracování osobních údajů, a tudíž je možné fotografii bez obav zveřejnit.

O zpracování osobních údajů ve spojitosti s fotografií, a tudíž i nutnost získat souhlas se zpracováním osobních údajů, by šlo až v případě, že se zveřejní systematicky řazené osobní údaje. Jako příklad takového zveřejnění lze uvést situaci, kdy je zveřejněna fotografie výherců soutěže, jež se v rámci dětského dne pořádá a ke které jsou připojeny další údaje nad rámec jména a příjmení, které lze zveřejnit v rámci tzv. zpravodajské licence. O zpracování by se jednalo tedy v případě, že by k fotografii kromě jména a příjmení byl přiřazen např. i věk, datum narození, místní část obce, kde osoba žije, bydliště apod.

Z výše uvedeného je zřejmé, že ne každé získání a zveřejnění fotografií podléhá pravidlům zpracování, a tudíž i obecnému nařízení, respektive zákonu o zpracování. V případě, že se spolu s fotografií nezveřejňují další systematicky přiřazené osobní údaje, nejedná se o zpracování osobních údajů. Uplatní se jen některé aspekty občanského zákoníku, včetně zpravodajské licence.

Zpracovali
Michal Hinda a Kristýna Vodrážková
Pověřenci pro ochranu osobních údajů

DPO PRO. Ročník III, číslo 2. 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. 2. 2023.