

Cookies využívané orgány veřejné správy

Úprava čl. 5 odst. 3 směrnice ePrivacy a § 89 odst. 3 ZEK dopadá na **každý** subjekt, který hodlá používat nebo používá síť elektronických komunikací k ukládání údajů nebo k získávání přístupu k údajům uloženým v koncových zařízeních. Tato úprava tedy plně dopadá i na orgány veřejné správy a jimi provozované webové stránky či mobilní aplikace, prostřednictvím kterých dochází ke zpracování cookies (a dalších online identifikátorů).

Spolek pro ochranu osobních údajů

www.epravo.cz; 21. prosince 2021

Postavení poskytovatelů služeb při zpracování osobních údajů

Nařízení EU o ochraně osobních údajů („GDPR“)[1], které upravuje pravidla při zpracování osobních údajů, primárně vychází ze zdánlivě jednoduchého rozlišení účastníků zpracování na tzv. správce (anglicky controllers) a zpracovatele (anglicky processors).

Naším cílem v tomto článku není podat detailní definice toho, kdo je správce a kdo zpracovatel osobních údajů. K tomu ostatně můžeme odkázat například na Pokyny Evropského sboru pro ochranu osobních (EDPB) č. 07/2020 k pojmu správce a zpracovatele podle GDPR.

Rádi bychom se ale zaměřili na jeden praktický případ, se kterým se opakovaně setkáváme a který vyvolává často neshody mezi zúčastněnými stranami. Jde o určení postavení a povinností při zpracování osobních údajů v případě poskytovatelů služeb v obchodních vztazích, ve kterých vystupují zpravidla dvě obchodní společnosti a dochází ke zpracování údajů klientů, případně zaměstnanců jedné z nich. Typicky může jít např. o dopravce zboží, který přijímá zakázku od e-shopu na dodání zboží jeho zákazníkovi, nebo poskytovatele služeb, které jsou využívány zaměstnanci jiné společnost (např. správa služebních platebních karet).

V praxi se často setkáváme s tím, že společnost poskytující údaje svých zákazníků nebo zaměstnanců automaticky předpokládá, že poskytovatel, jehož služby si pořizuje, je zpracovatelem osobních údajů. Tento přístup nicméně v mnoha případech považujeme za nesprávný.

Kdo je zpracovatelem?

Podle čl. 4/8 GDPR je „zpracovatelem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Přesněji řečeno, zpracovatel provádí zpracování za správce (viz oficiální *corrigendum* k obecnému nařízení čl. 28). Ještě jasněji je to pak uvedeno v anglické verzi GDPR, která používá spojení *on behalf of* (jménem, jako zástupce).

Toto vymezení jinými slovy určuje, že zpracovatel nemůže osobní údaje zpracovávat pro své vlastní účely[2], a zároveň to také znamená, že zpracovatel může zpracovávat osobní údaje pouze na základě pokynů správce a v jejich mezích (viz čl. 28/3/a GDPR). Jde tedy o jakousi formu delegace zpracování ze správce na zpracovatele.[3] Na tom nic nemění ani určitá míra autonomie při volbě prostředků zpracování, kterou zpracovatelé GDPR umožňuje. Nesmí nicméně jít o podstatné aspekty zpracování.

Zpracovatel nesmí zpracovávat údaje pro vlastní účely – opravdu?

Požadavek na pouhopouhé robotické plnění pokynů je sám o sobě velmi problematický, nakolik i typičtí zpracovatelé (podle příkladů uvedených v pokynech, stanoviscích, rozhodnutích a dalších podobných dokumentech regulátorů nebo soudů) v mnoha případech určité zpracování pro vlastní účely provádět musí (např. z důvodu interní kontroly nebo obrany a vymáhání smluvních podmínek dohodnutých se správcem, případně pro plnění svých zákonných povinností). Idea čistého zpracovatele je tak v současném právním prostředí EU spíše iluzorní. V tomto smyslu je realističtější přístup kalifornského

[1] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 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)

[2] Pokyny EDPB č. 07/2020 k pojmu správce a zpracovatele, bod 80.

[3] Pokyny EDPB č. 07/2020 k pojmu správce a zpracovatele, bod 80.

zákona o soukromí spotřebitelů („CCPA“)[4], který dává podnikům (*businesses*) určité úlevy z regulace při využití tzv. poskytovatelů služeb (*service providers*). Tito poskytovatelé jsou nicméně podle §999.314 prováděcích nařízení k CCPA oprávněni nad rámec zpracování nutného pro splnění smlouvy s podnikem zpracovávat údaje pro zákonem vymezené účely zahrnující:

- najmutí a zaměstnání jiného poskytovatele služeb jako subdodavatele;
- interní použití údajů poskytovatelem služeb k vybudování služeb nebo zlepšení jejich kvality za předpokladu, že toto použití nezahrnuje vytvoření nebo úpravu profilů domácností nebo spotřebitelů ani čištění nebo obohacování údajů získaných z jiného zdroje;
- odhalování bezpečnostních incidentů s údaji nebo ochranu před podvodnou nebo nezákonnou činností a
- k plnění právních povinností, jako je spolupráce s orgány činnými v trestním řízení a uplatňování nebo obhajoba právních nároků.

Tento přístup považujeme za lepší z hlediska reálného fungování dodavatelských vztahů. *De lege ferenda* jde podle našeho názoru o přístup, který by měla EU, potažmo členské státy zvážit.

Kdy jsou poskytovatelé služeb správci?

Pokud výše uvedená pravidla podle GDPR aplikujeme na námi vymezené vztahy, je zřejmé, že u řady poskytovatelů služeb nemůže v žádném případě jít o zpracovatele. V rámci jejich služeb dochází ke zpracování osobních údajů, které si sami určují jak co do jeho účelu, tak co do prostředků zpracování. Relevantní informace o zpracování osobních údajů v souladu s čl. 13 (případně 14) GDPR pak mají poskytovatelé popsány ve svých zásadách ochrany osobních údajů.

Tento přístup je podpořen aktuálními pokyny EDPB č. 07/2020 k pojmu správce a zpracovatele. Podle bodu 82. těchto pokynů je klíčovým faktorem pro posouzení postavení při zpracování povaha zpracování v kontextu specifických aktivit poskytovatele služeb, nikoli typ entity (myšleno zřejmě ve vztahu k poskytovateli služeb). Nelze tedy izolovaně hodnotit postavení jen podle typu vztahu, povahy osobních údajů ani kategorií subjektů údajů, kterých se zpracování týká. Vždy je nutné hodnotit celkový kontext zpracování.

EDPB v tomto smyslu uvádí, že tam, kde poskytované služby nejsou specificky zaměřené na zpracování osobních údajů nebo kde zpracování osobních údajů není klíčovým elementem služby, může být poskytovatel služby v pozici, kdy samostatně určuje účely a prostředky zpracování nutného k zajištění své služby. V takové situaci pak podle EDPB bude poskytovatel služeb samostatným správcem a nikoli zpracovatelem.

Tato poněkud krkolomná definice se podle našeho názoru dá zjednodušit tak, že osoba, která poskytuje vlastní služby, jejichž předmět a rozsah sama definuje, bude zpravidla správcem osobních údajů. To platí zejména tam, kde daná služba zahrnuje vysokou přidanou hodnotu, odbornost, autonomii rozhodování, nebo dokonce spadá do specifické právní regulace s pevně danými pravidly a povinnostmi (např. platební služby, nezávislé zprostředkování finančních služeb apod.).[5] V těchto případech si lze jen stěží představit situaci, kdy by objednatel služeb určoval, jak mají být takové služby poskytovány, eventuálně že by se služby poskytovaly pro každého objednatele jiným způsobem v závislosti na jeho pokynech.

Příklady

- Taxislužba nabízí online platformu, která firmám umožňuje objednat si taxi pro přepravu zaměstnanců nebo hostů na letiště a z letiště. Taxislužba nabízí své vlastní služby, zpracování osobních údajů není specifickým záměrem jejich činnosti, ale jen z ní vyplývá. Taxislužba se neřídí pokyny zákazníků ve vztahu ke zpracování osobních údajů, přestože své služby poskytuje na základě jejich požadavků. Taxislužba je správcem osobních údajů.[6]
- Firma používá účetního k vedení účetnictví. Účetní zpracovává údaje pro svého klienta, ale je sám správcem osobních údajů v rámci své činnosti (účetnictví). Je tomu tak proto, že účetní a podobní poskytovatelé odborných služeb pracují na základě řady profesních povinností, které je zavazují k odpovědnosti za osobní údaje, které zpracovávají.[7]
- Doručovací společnost obdrží od původního správce (např. od e-shopu) doručovací adresy (osobní údaje) adresátů pro účely doručení a zajistí doručení zásilek. Doručovatel zásilek jedná na vlastní odpovědnost, jde o samostatnou činnost dodavatele těchto služeb, tedy správce údajů, který provádí zpracování nebytné pro jím stanovený účel doručování. Doručovací společnost neprovádí zpracování údajů jako zpracovatel.[8]

[4] Dostupné >>> [zde](#).

[5] Viz například také stanovisko britského ICO ohledně postavení specializovaných poskytovatelů služeb: Pokud specializovaní poskytovatelé služeb zpracovávají údaje v souladu se svými profesními povinnostmi, vystupují vždy jako správce (viz >>> [zde](#)).

[6] Pokyny EDPB č. 07/2020 k pojmu správce a zpracovatele, bod 82.

[7] Viz >>> [zde](#).

[8] Viz stanovisko UOOU k dispozici >>> [zde](#).

Kdy budou poskytovatelé přece jen zpracovateli?

Pouhým zpracovatelem a nikoli správcem naopak zpravidla bude osoba, která provádí triviální operace s osobními údaji (např. rozeslání dopisů na adresy určeném zadavatelem), nebo postupuje výlučně podle pokynů správce a nemá prostor pro vlastní rozhodování ohledně předmětu a rozsahu svých služeb.

Příklad

- Provedení marketingové analýzy podle jasně daných instrukcí na datech poskytnutých zadavatelem.
- Zajištění služeb call centra na základě a v mezích pokynů objednatele a ve vztahu k objednatelovým klientům.
- Zajištění IT podpory na základě a v mezích pokynů objednatele, při níž dochází nevyhnutelně i k práci s osobními údaji, přestože nejde o primární smysl činnosti.
- Doručovatel provádí doplňkové činnosti podle pokynů objednatele, např. kompletaci zásilek, vč. tisku oznámení obsahující osobní údaje a jejich vkládání do obálek. V tomto případě se jedná o činnost zpracovatele.

Relativně samostatnou kapitolou jsou pak poskytovatelé cloudových služeb nebo jiných úložišť, kteří se zpravidla také považují jen za zpracovatele osobních údajů, a to přestože nabízejí své služby široké veřejnosti a podle jimi definovaných pravidel. Důvodem je podle EDPB skutečnost, že konečné rozhodnutí o účelech a o tom, jak takové předem definované nástroje využije, dělá zákazník (původní správce údajů), a to včetně všech povinností a nutnosti zajistit, že poskytovatel cloudových služeb respektuje jeho pokyny.[9] Tento přístup nám nepřijde zcela konzistentní s výše uvedenými kritérii a pro praxi navíc velmi problematický, nakolik požadavek donutit některé poskytovatele cloudových služeb respektovat specifické pokyny jednotlivých zákazníků/správců je mimo jejich reálné možnosti.

Kdy nebude poskytovatel služeb ani správcem, ani zpracovatelem?

Specifickým případem jsou situace, kdy osoba vůbec ke své činnosti osobní údaje nepotřebuje, ale může se k nim za určitých podmínek dostat (ať už náhodou, nebo i vědomě). V těchto případech je na místě primárně zajistit takové smluvní podmínky a záruky, aby nedošlo k ohrožení osobních údajů, případně si ujednat postup pro případ, že k tomu i přes tyto záruky dojde (např. ve smyslu ohlášení situace, zajištění bezpečnosti osobních údajů a zamezení dalšímu opakování nebo zhoršení situace).

Příklad

- Firma zajišťující úklid kanceláří, která se náhodou nebo nedbalostí zaměstnanců může dostat k dokumentům, počítačům apod.
- IT firma najatá na vývoj nebo opravu softwaru, ke kterým nepotřebuje žádné osobní údaje, ale může náhodou nebo nedbalostí k takovým údajům získat přístup.
- Doručovatelé poštovních zásilek ve vztahu k osobním údajům obsaženým uvnitř zásilek, které nesmějí otevřít.

Závěrem

Jak jsme v předchozím textu naznačili, zjednodušený přístup k poskytovatelům služeb, který jim automaticky přisuzuje postavení zpracovatelů, není v mnoha případech správný. Vždy bude záležet na konkrétním kontextu zpracování osobních údajů. Z uvedených příkladů a stanovisek dozorových úřadů se nicméně dá usuzovat, že poskytovatelů služeb, kteří budou jen zpracovateli, je podstatně méně, než by se na první pohled mohlo zdát. V řadě oblastí bude dokonce podle nás potřeba vztahy znovu revidovat a posoudit, zda skutečně v daných případech jsou poskytovatelé služeb pouhými zpracovateli ve smyslu GDPR.

Jinou možností je pak přehodnotit extrémně úzké vymezení zpracovatele podle GDPR jako takového. V tomto ohledu hodnotíme jako lepší přístup kalifornského zákona o soukromí spotřebitelů a jeho definici poskytovatelů služeb, která jim nad rámec zpracování nezbytného pro plnění smlouvy umožňuje zpracovávat osobní údaje i pro další zákonem vymezené účely, aniž by ztratili postavení poskytovatele služeb.

Autor: Ing. Mgr. Jakub Hruška, CIPP/E

www.epravo.cz; 7. ledna 2022

[9] Pokyny EDPB č. 07/2020 k pojmu správce a zpracovatele, bod 84.

Bankovní tajemství a GDPR

Nové stanovisko České národní banky k bankovnímu tajemství Institut bankovního tajemství chrání informace o klientech banky, jejich majetku, využívaných produktech a bankovních obchodech. Samotná definice bankovního tajemství a souvisejících povinností banky v § 37-38 a § 38b zákona č. 21/1992 Sb., o bankách, je poměrně stručná. Uvedený zákon věnuje daleko více prostoru jednotlivým výlukám ze zákazu poskytovat informace chráněné bankovním tajemstvím dalším osobám bez souhlasu klienta.

Oč jsou daná ustanovení zákona stručnější, o to více praktických otázek nabízejí. Otázek týkajících se jak okruhu chráněných osob, informací, které institutu bankovního tajemství podléhají, a rovněž aplikací jednotlivých výluk.

Česká národní banka dne 1. listopadu 2021 zveřejnila komplexní stanovisko k některých otázkám týkajícím se praktické aplikace bankovního tajemství. Toto stanovisko na řadu otázek či praktických nejasností odpovídá.[1] V následujícím článku toto stanovisko stručně shrnu a pokusím se odpovědět i některé další otázky či nejasnosti, které jsou pro praxi rovněž důležité.

Osobní údaje vs. bankovní tajemství

Neméně zajímavý aspektem je vztah úpravy bankovního tajemství a obecné regulace zpracování osobních údajů. Pojem osobní údaj je v čl. 4 bod 1 obecného nařízení o ochraně osobních údajů (GDPR)[2] definován jako jakákoliv informace, která se týká identifikované nebo přímo či nepřímo identifikovatelné fyzické osoby. Informace chráněné bankovním tajemstvím jsou pak v zásadě veškeré údaje týkající se klientů či bývalých klientů využívajících nebo majících zájem využít některou platební službu poskytovanou bankou.

Je zjevné, že v případě klientů, fyzických osob, se tyto dvě množiny informací do velké míry překrývají. Stanovisko ČNB se vztahem příslušné úpravy v zákoně o bankách a v GDPR částečně zabývá, nicméně i zde podle mého názoru stojí několik dalších bodů za vyjasnění. Nebo alespoň za formulování klíčových otázek, které si zaslouží další diskusi.

Úprava bankovního tajemství v zákoně o bankách

Rozsah bankovního tajemství je fakticky upraven jedinou větou v § 38 odst. 1 zákona o bankách: „Na všechny bankovní obchody, peněžní služby bank, včetně stavů na účtech a depozit, se vztahuje bankovní tajemství.“ Zákon kromě toho v obecném rozsahu zakládá oprávnění bank shromažďovat a dále zpracovávat osobní údaje včetně rodného čísla nezbytné pro poskytování obchodů bez nepřiměřených rizik pro banku (§ 38).

Zákon o bankách dále obsahuje detailní a uzavřený (taxativní) výčet případů, kdy lze osobní údaje poskytnout dalším osobám. V principu jde o čtyři kategorie situací:

Zpřístupnění nezbytné pro poskytnutí služby klientovi (např. poskytnutí informací bance, která vede účet příjemci platby)

- zpřístupnění orgánu dohledu (Česká národní banka) nebo některým dalším úřadům při výkonu jejich kompetencí (například Finančnímu analytickému úřadu, Úřadu pro dohled nad politickými stranami, soudnímu exekutorovi atd.)
- zpřístupnění nebo i zveřejnění nezbytné k ochraně práv banky či dalších subjektů (sdílení dat o bonitě klientů v bankovním registru, podání trestního oznámení nebo občanskoprávní žaloby, možnost, v praxi příliš nevyužívaná, zveřejnit informace o dlužníkovi banky)
- zpřístupnění těchto informací se souhlasem klienta, tedy osoby, které bankovní tajemství svědčí

Jaké informace podléhají bankovnímu tajemství?

První z otázek, kterou se komentované stanovisko České národní banky zabývá, je rozsah informací, které podléhají ochraně dle bankovního tajemství.

Česká národní banka k tomuto bodu upřesňuje, že bankovnímu tajemství podléhají informace o všech bankovních obchodech a peněžních službách bank. Těmito pojmy je, stručně řečeno, nutno rozumět veškeré informace o obchodních vztazích banky a konkrétní (fyzické či právnické osoby), stejně jako o poskytnutí jednorázové platební služby, např. umožnění vložení peněz na účet či výběru hotovosti z bankomatu. K této otázce ČNB upřesňuje, že i záznam z kamer zachycující identifikovatelnou osobu, jak využívá službu banky, např. vybírá z bankomatu, tudíž nutně obsahuje informace charakteru bankovního tajemství.

[1] K dispozici >>> [zde](#).

[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).

Nabízí se tudíž otázka, zda mohou existovat situace, kdy banka někomu poskytuje službu, ale informace o poskytování této služby a jejím příjemci bankovnímu tajemství nepodléhají. Zákon o bankách vymezuje možný okruh služeb nabízených bankou uzavřeným výčtem. Velkou většinu z možných činností je možné podřadit pod uzavírání bankovních obchodů nebo poskytování peněžních služeb, tedy nejen přijímání vkladů od veřejnosti a poskytování úvěrů, ale i např. vydávání elektronických peněz, poskytování záruk či investičních služeb, poskytování směnářenské činnosti nebo pronájem bezpečnostních schránek.[3]

Služby, které podle mého názoru naopak do vymezené kategorie nespádají, jsou především služby, řekněme, nefinančního charakteru. Jedná se především o činnost spočívající v poskytování identifikačních služeb, tedy poskytování elektronické identifikace, autentizace a služeb vytvářejících důvěru i poskytování nebo potvrzování osobních identifikačních údajů klienta. Druhou takovou službou pak může být výkon působnosti kontaktního místa veřejné správy.

Informace o poskytování služeb uvedených v předchozím odstavci ochraně dle bankovního tajemství nepodléhají. To však neznamená, že s nimi banka může nakládat libovolně, například využívat je k profilování či marketingovému oslovování klienta. Pokud klientem bude fyzická osoba, pak je vždy rovněž nutno aplikovat GDPR, které pro zpracování těchto informací, osobních údajů, stanovuje detailní pravidla.

Není souhlas jako souhlas

Stanovisko České národní banky se zabývá i tím, jaké náležitosti musí splňovat souhlas klienta s poskytnutím informací charakteru bankovního tajemství dalšímu subjektu. V praxi se typicky jedná o souhlas klienta se sdílením informací podléhajících bankovnímu tajemství podnikům spřízněným s bankou, resp. tvořící s ní skupinu. K takovému sdílení pro některé účely, např. obsluhu klienta, by obvykle nebyl nutný souhlas se zpracováním osobních údajů podle GDPR, protože by toto zpracování bylo možné považovat za jednání v oprávněném zájmu banky či dalšímu člena skupiny podniků. Zákon o bankách však tento důvod ke sdílení informací podléhajících bankovnímu tajemství, tedy oprávněný zájem, nezná, proto v těchto případech může banka data předávat jen se souhlasem klienta.

Česká národní banka k tomu uvádí, že takovýto souhlas musí především splňovat náležitosti pro právní jednání stanovené občanským právem. Musí tedy být projevem svobodné vůle, být učiněn vážně a vyjádřen určitě a srozumitelně. ČNB k tomu dodává, že jako jednostranné právní jednání může být tento souhlas uveden například ve smlouvě nebo obchodních podmínkách.

V tom je nutno rovněž spatřovat jistý rozdíl oproti souhlasu se zpracováním osobních údajů. U něj GDPR výslovně vyžaduje, aby v případě, kdy je udělován písemným prohlášením, které se týká rovněž dalších skutečností, byl souhlas od těchto jasně odlišen.[4] Na druhé straně, i v případě souhlasu se zpřístupněním informací bankovního tajemství, které je součástí komplexnějšího dokumentu, nesmí být tento souhlas pro klienta překvapivý či nejasný.

Pokud bychom tuto část měli shrnout, tak byť se v případě souhlasu se zpřístupněním informací podléhajících bankovnímu tajemství a souhlasu se zpracováním osobních údajů jedná o postup podle dvou odlišných právních předpisů, zákona o bankách a GDPR, fakticky si jsou tyto dva úkony velmi blízké. Pokud bude souhlasy udělovat fyzická osoba, pak je jistě možné, aby bylo vyjádřeno jedním jednáním, např. prostřednictvím jednoho formuláře. V takovém případě je důležité, aby toto jednání splňovalo náležitosti vyžadované oběma předpisy a aby bylo transparentní. Jinými slovy, klientovi musí být zřejmé, ke zpřístupnění jakých informací dává souhlas a že se jedná jak o jeho osobní údaj, tak o informace charakteru bankovního tajemství.

Kdo je vlastně klientem banky?

Česká národní banka vykládá shora uvedené ustanovení zákona po bankách tak, že za klienta banky je při posuzování institutu bankovního tajemství nutno považovat každého, kdo má nebo v minulosti měl s bankou obchodní vztah, a stejně tak každého, kdo s bankou vedl nebo vede jednání o uzavření bankovního vztahu bez ohledu na to, jak jednání dopadlo. ČNB tedy aplikuje extenzivní výklad, kdy každá osoba, která čerpala nebo čerpá některou výše vymezenou bankovní službu, ať už na základě písemné smlouvy či jednorázově, nebo která banku o poskytnutí některé produktu, typicky úvěru, požádala, je osobou, již svédčí bankovní tajemství.

I tato část komentovaného stanoviska může přinést dílčí výkladové problémy. Zejména u osob, které jednorázově využijí platební službu, u které se nemusí identifikovat, může být komplikované získat jejich souhlas s využitím informací podléhajících bankovnímu tajemství. Pokud by banka hodlala tyto informace využít, aniž by jí k tomu svédčil některý z právních titulů uvedených v zákoně o bankách, bylo by prakticky velmi obtížné získávat prokazatelný souhlas takovýchto klientů.

[3] Srov. § 1 zákona o bankách.

[4] Srov. rovněž pokyny Evropského sboru pro ochranu osobních údajů č. 5/2020 k souhlasu se zpracováním osobních údajů, konkrétně bod 71 těchto pokynů. K dispozici >>> [zde](#).

Outsourcing a postoupení pohledávky není porušením bankovního tajemství

Komentované stanovisko se vyjadřuje i ke dvěma velmi častým situacím, kdy v praxi dochází nebo může docházet ke zpřístupnění informací o konkrétních klientech banky další osobě.

Prvním z nich je outsourcing čili zajištění určité činnosti, kterou by jinak dělala banka, prostřednictvím další osoby.[5] Česká národní banka k tomu uvádí, že v takovém případě dodavatel, poskytovatel outsourcingu, pro banku vykonává činnosti, které by jinak banka vykonávala sama. Informace mu tedy nejsou předány pro využití za jeho vlastním cílem, ale pouze pro zajištění outsourcované služby. Z toho důvodu se nejedná o průlom do bankovního tajemství a k využití poskytovatele outsourcingu není nutné hledat některý z právních titulů pro zpřístupnění těchto informací, tím méně souhlas klienta.

Podle mého názoru je nutné tento výklad vztáhnout i na další situace, kdy banka určitou činnost řeší dodavatelsky, nicméně se nejedná o outsourcing ve smyslu příslušné regulace. Takovým případem může být např. využití služeb advokátní kanceláře pro zastupování banky ve sporu s klienty.[6] Ač se rovněž jedná o zpřístupnění osobních údajů další osobě odlišné od banky, opět půjde o situaci, kdy tato třetí osoba informace zpracovává pro banku a v jejím zájmu. Navíc, pokud podle ČNB není důvodné považovat za prolomení bankovního tajemství zpřístupnění informací o klientovi poskytovateli outsourcingu, tím méně důvodné by to bylo u poskytovatele méně rizikové a méně regulované služby.

Česká národní banka rovněž dovozuje, že bez souhlasu klienta lze sdělit informace podléhající bankovnímu tajemství v situaci, kdy banka postupuje pohledávky za svými klienty dalším osobám. V této části však nejsou možnosti banky neomezené. S ohledem na uzavřený výčet právních titulů ke zpřístupnění těchto informací lze aplikovat jen důvod uvedený v § 38b zákona o bankách, podle kterého lze tyto informace další osobě předat jen tehdy, je-li to potřebné pro účely plnění pravidel obezřetného podnikání. Tento právní důvod v sám sobě obsahuje jisté omezení: Aby postoupení pohledávek, resp. související zpřístupnění informací podléhajících bankovnímu tajemství, mohlo proběhnout bez souhlasu klienta, je nutné, aby banka byla schopna doložit, že postoupení pohledávky bylo součástí jejího obezřetného podnikání. Typicky se jedná o případy, kdy je z pohledu banky efektivnější problematiku pohledávku postoupit (prodat) nebo je hospodárnější zvýšit si likviditu prodejem určitého portfolia než například úvěrem od jiné instituce.

Poskytování informací úřadům

Stanovisko upřesňuje některé spíše formální nebo procesní aspekty poskytování informací oprávněným úřadům, např. rozsah či lhůtu pro zpřístupnění požadovaných dat. Tato část komentovaného stanoviska podle mého názoru žádné další otázky nepřináší, proto si zájemce dovoluji odkázat na stanovisko samotné.

Shrnutí vztahu bankovního tajemství a GDPR

Pokud je klientem banky nebo zájemcem o produkt banky fyzická osoba, pak informace o jeho využívání bankovních produktů a související skutečnosti můžeme ve velké většině podřadit jak pod pojem osobní údaje, tak informace chráněné bankovním tajemstvím.

Na druhou stranu, osobními údaji jsou i data o neklitech banky, které má banka k dispozici, nebo data klientech, kteří využívají některé specifické služby, zejména identifikaci či služby kontaktního místa veřejné správy. Z opačného úhlu pohledu pak můžeme konstatovat, že informace o právnických osobách jako o (současných či bývalých) klientech banky nebo zájemcích o bankovní produkty jsou informacemi charakteru bankovního tajemství, nikoliv však osobními údaji v režimu GDPR. GDPR totiž dopadá pouze na informace týkající se fyzických osob.

V praxi je proto nutné při každém procesu, který zahrnuje zpřístupnění informací o klientech banky dalším subjektům, na prvním místě posoudit, zda se jedná o informace podléhající bankovnímu tajemství nebo o osobní údaje. Následně je nutné uplatnit některý, či případně oba, z dotčených předpisů. Zákon o bankách, který obsahuje především výčet právních titulů pro zpřístupnění chráněných informací, pro bankovní tajemství a GDPR s jeho detailními pravidly pro zpracování osobních údajů.

Autor: Mgr. František Nonnemann

www.epravo.cz; 3. prosince 2021

[5] Outsourcing v bankovníctví, resp. při poskytování platebních služeb, je velmi detailně upraven především v obecných pokynech EBA k outsourcingu, k dispozici >>> [zde](#).

[6] To, že takováto činnost není outsourcingem, je výslovně uvedeno v bodu 28 písm. g) obecných pokynů EBA k outsourcingu.