ČESKÁ CZECH
BANKOVNÍ BANKING
ASOCIACE ASSOCIATION

# RÁMCOVÝ VÝKLAD NĚKTERÝCH USTANOVENÍ GDPR V BANKOVNÍM SEKTORU

Praha I březen 2019

*Aktualizace: červen 2022*

# Obsah

Tímto dokumentem je dán rámcový výklad některých ustanovení nařízení EU č. 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, dále jen „GDPR“) v procesech poskytování bankovních produktů a služeb, a to s ohledem na specifika bankovního sektoru a jeho závislosti na zpracování osobních údajů ve velkém rozsahu. Cílem tohoto dokumentu je proto stanovit výkladový rámec bankovního sektoru využívaný při aplikaci GDPR tak, aby byl zároveň zajištěn soulad s ostatní regulací finančního trhu a výklad jednotlivých ustanovení GDPR zohledňoval jeho specifika.

Tyto doporučené postupy nepředstavují závazný výklad příslušných ustanovení, je na každé bance zvážit, jak GDPR bude interpretovat. S dále uvedenou interpretací jsou nicméně srozuměni všichni členové České bankovní asociace, kteří se k tomuto dokumentu přihlásí. Dokument představuje obecně pojatou minimální míru ochrany subjektů osobních údajů, kdy není bráněno jednotlivým členským bankám zvolit v konkrétních případech vyšší míru ochrany zpracování osobních údajů na základě jejich specifických potřeb a postupů.

Banky jsou ve své činnosti vázány rozsáhlou regulací, a to ve všech oblastech poskytování bankovních produktů a finančních služeb. Ve vztahu k fyzickým osobám se jedná především o plnění požadavků přímo účinných evropských nařízení nebo směrnic transponovaných do právního řádu České republiky například zákonem o bankách, zákonem o spotřebitelském úvěru, zákonem o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, zákonem o platebním styku atd. Nařízení GDPR stanovuje základní rámec pro nakládání s osobními údaji, který banky musí skloubit se svými ostatními regulatorními povinnostmi.

Banky zpracovávají osobní údaje svých klientů a zájemců o bankovní produkty či služby, zaměstnanců, dodavatelů a jiných osob (např. členů dozorčí rady) v souladu s požadavkem zákonného zpracování (čl. 6 GDPR) převážně na následujících právních základech:

- zpracování osobních údajů je nezbytné pro uzavření smlouvy a její následné plnění (čl. 6 GDPR, odst. 1, písm. b); jedná se například o zpracování identifikačních, kontaktních údajů před uzavřením smlouvy, nebo o doplňování dat v průběhu smluvního vztahu, jako je změna příjmení, aktualizace kontaktních údajů apod.;
- osobní údaje jsou zpracovávány na základě právní povinnosti dané bankám závazným právním předpisem (čl. 6 GDPR, odst. 1, písm. c); například se jedná o údaje získávané od klientů bank v souvislosti s povinnými opatřeními proti legalizaci výnosů z trestné činnosti nebo údajů týkajících se úvěrové zatíženosti a platební morálky při sjednávání spotřebitelského úvěru apod.[1];
- banky mohou zpracovávat osobní údaje na základě oprávněného zájmu – tento právní základ je vyvážen rozsáhlými právy subjektu osobních údajů (čl. 6 GDPR, odst. 1, písm. f); jedná se například o oslovování klientů bank v rámci přímého marketingu, zpracování dat pro účely řízení rizik atd.;
- osobní údaje jsou zpracovávány ke konkrétnímu účelu na základě souhlasu uděleného subjektem údajů bance (čl. 6 GDPR, odst. 1, písm. a), přičemž takový souhlas je vyjádřen v souladu s podmínkami stanovenými GDPR (čl. 7 a 4 – souhlas je doložitelný, informovaný, svobodný,

[1] V oblasti bankovnictví mnoho povinností vyplývá i ze sekundární legislativy, nebo nepřímo z výkladů či rozhodovací praxe regulátora (nejčastěji ČNB).

srozumitelný a odvolatelný); souhlas je vyžadován například v případě nabízení produktů třetích stran nijak nesouvisejících s nabídkou bankovních produktů, nebo v případě, kdy banka zpracovává osobní údaje tzv. profilováním pro marketingové účely apod.

Okrajově, ve specifických případech, může být zpracování osobních údajů nezbytné pro ochranu životně důležitých zájmů klientů (čl. 6 GDPR, odst. 1, písm. d) nebo pro splnění úkolu prováděného ve veřejném zájmu (čl. 6 GDPR, odst. 1, písm. e), např. v souvislosti s bojem proti pandemii vyhlášeným vládou.

## SPECIFIKA NĚKTERÝCH PRÁVNÍCH ZÁKLADŮ PRO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

### 1. Zpracování osobních údajů na základě oprávněného zájmu (balanční test a námitky)

Balanční test

V případě, že banka zamýšlí osobní údaje zpracovávat na základě právního titulu oprávněného zájmu banky, provede balanční test, v jehož rámci posoudí svůj oprávněný zájem na zpracování oproti základním svobodám a právům subjektů údajů a zjistí tedy, zda jí oprávněný zájem v souvislosti s daným zpracováním skutečně svědčí či nikoli. Balanční test se obecně skládá ze tří základních částí:

- definování oprávněného zájmu;
- prokázání, že předmětné zpracování osobních údajů je nezbytné pro dosažení oprávněného zájmu;
- posouzení tvrzeného oprávněného zájmu oproti zájmům a základním svobodám a právům subjektu údajů.

V případě, že výsledkem balančního testu je závěr, že zájmy, základní svobody a práva subjektů údajů převažují nad předmětným zájmem banky, nemůže banka dané zpracování osobních údajů na základě oprávněného zájmu provádět.

Za případ dobré praxe lze označit zpracování interní metodiky popisující, v jakých případech, jakým způsobem a podle jakých kritérií balanční test vypracovat, včetně stanovení pravidel jeho archivace a pravidel pro případné konzultace s pověřencem pro ochranu osobních údajů. Je na úvaze banky, zda se rozhodne pro balanční test uplatnit formu slovního nebo číselného hodnocení. Balanční test je vhodné vypracovat v písemné podobě, aby mohl sloužit jako doklad uskutečnění výše popsaného procesu.

Námitky

Proti zpracování osobních údajů na základě oprávněného zájmu[2] má subjekt údajů kdykoli právo uplatnit námitku z důvodů týkajících se jeho konkrétní situace (ledaže jde o námitku proti zpracování osobních údajů pro účely přímého marketingu na základě oprávněného zájmu, jak je blíže popsáno níže). Banka tedy může pro přijetí žádosti po subjektu údajů požadovat, aby v rámci podané námitky popsal okolnosti týkající se jeho konkrétní situace, kvůli kterým se domnívá, že banka v jeho případě nemá převažující oprávněný zájem na zpracování jeho osobních údajů.

[2] A rovněž i veřejného zájmu.

V případě řádného vznesení námitky subjektem údajů banka osobní údaje dále nezpracovává (omezí jejich zpracování), dokud neověří, zda její oprávněné důvody pro zpracování osobních údajů, které by měly být popsány v balančním testu, převažují nad zájmy či právy a svobodami daného subjektu údajů. Omezení zpracování předmětných osobních údajů se týká pouze namítaného účelu zpracování, banka je tedy může nadále zpracovávat pro jiné účely, pro které má zákonný titul. Omezení zpracování předmětných osobních údajů se rovněž netýká zpracování nutného pro určení, výkon nebo obhajobu právních nároků, přičemž v tomto případě se nemusí jednat pouze o právní nároky banky, ale může jít i o právní nároky třetích osob. Blíže k omezení zpracování osobních údajů viz také kapitola B) čl. 1 odst. 1.1 tohoto dokumentu.

Pro uplatnění námitky proti zpracování osobních údajů pro účely přímého marketingu na základě oprávněného zájmu se uplatní zvláštní pravidla – námitku subjekt údajů nemusí odůvodňovat a je účinná bez dalšího.

Na právo podat námitku proti zpracování osobních údajů na základě oprávněného zájmu (pro účely přímého marketingu i jiné účely) by subjekt údajů měl být výslovně upozorněn a toto právo by mělo být uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů. Tato povinnost se považuje za splněnou také v případě, že informace o právu podat námitku proti zpracování osobních údajů je uvedena v rámci textu, kterým banka plní svou informační povinnost vůči subjektům údajů v souladu s čl. 13, případně čl. 14 GDPR (vč. např. Informace o zpracování osobních údajů zveřejněné na webových stránkách banky), za předpokladu, že tento text je zřetelně oddělen od jiných, např. smluvních informací.

## 2. Souhlas se zpracováním osobních údajů a jeho náležitosti

Souhlas banky obecně využívají v souvislosti s marketingovým zpracováním osobních údajů, nejedná-li se o marketing na základě oprávněného zájmu. V ostatních případech využití souhlasu pro zpracování osobních údajů se jedná o konkrétní specifické potřeby jednotlivých bank.

### 2.1 GDPR souhlas

a) Základní pravidla pro sbírání souhlasů se zpracováním osobních údajů

- Poskytnutí bankovní služby nesmí být podmiňováno udělením souhlasu se zpracováním osobních údajů ze strany subjektu údajů.
- Subjekty údajů smí být pozitivně motivovány (např. poskytnutím přiměřené slevy) k tomu, aby souhlas udělily.
- Souhlas musí být jednoduše odvolatelný a subjekt údajů nesmí být sankcionován pro odvolání souhlasu.
- Od subjektů údajů nelze vyžadovat vyslovení nesouhlasu, ale jen vyslovení souhlasu, protože GDPR zná jen souhlas vyjádřený aktivním jednáním, nikoliv nesouhlas (tj. souhlas musí být založen na principu „*opt-in*“).
- Souhlas nemusí být uveden na samostatném formuláři a může být součásti jiného dokumentu, ale musí být odlišitelný od ostatního textu a subjekt údajů musí mít možnost projevit svou vůli, že souhlas uděluje (např. zaškrtne zaškrtávací políčko).

b) Minimální obsahové náležitosti souhlasu se zpracováním osobních údajů

- Účel zpracování (souhlas může obsahovat více rozdílných / neslučitelných účelů, ale tak, aby se subjekt údajů mohl svobodně vyjádřit ke každému jednotlivému účelu, tj. jednotlivé účely musí být oddělitelné).
- Rozsah zpracovávaných osobních údajů.
- Identifikace správce:
  - musí být identifikováni všichni správci, kterým je souhlas udělován (není ale nutné, aby byl souhlas udělován na formuláři každému správci zvlášť),
  - tuzemský správce by měl být identifikován názvem (obchodní firmou) a identifikačním číslem, pokud je to vhodné a přiměřené danému způsobu komunikace,
  - zahraniční správce musí být identifikován názvem (obchodní firmou), právní formou a sídlem.
- Informace o právu subjektu údajů odvolat souhlas, případně právu uplatnit námitku proti automatizovanému rozhodování (vyjádření, manuální přezkum, napadnout rozhodnutí), pokud je prováděno na základě souhlasu.

Vůči subjektu údajů musí být splněna informační povinnost. Povinnou obsahovou náležitostí souhlasu se zpracováním osobních údajů není doba, na kterou se souhlas uděluje. Informace o právech subjektu údajů nemusí být obsaženy ve formuláři souhlasu. V textu souhlasu může být odkaz na další dokument (informační memorandum) s dalšími informacemi o zpracování osobních údajů vyžadovanými GDPR, s tím, že s tímto dokumentem musí být subjekt údajů seznámen ještě před podpisem souhlasu.

## 2.2 Souhlas dle jiné legislativy a pořizování kopií OP

a) Pořizování kopií dokladů při identifikaci osob

Banky při své činnosti musejí postupovat tak, aby předcházely využívání finančního systému k praní peněz nebo financování terorismu. Za tímto účelem se řídí národní legislativou vycházející ze Směrnice Evropského parlamentu a rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU, která byla implementována do zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, (dále jen „AML zákon“), jehož aplikace je dále upřesněna metodickými pokyny Finančního analytického úřadu MF ČR (FAÚ).

Hlavním principem této činnosti je identifikace všech osob, které jsou s bankovním produktem či službou spojeny. Za tímto účelem banky (tzv. povinné osoby) provádějí identifikaci osob, k jejímuž doložení mohou pořizovat kopie nebo výpisy z předložených průkazů totožnosti a zpracovávat takto získané informace, pokud je to vyžadováno AML zákonem nebo pokud je to nezbytné k dosažení jeho účelu. Písemný souhlas klienta s pořízením kopie dokladu v tomto případě není vyžadován, o pořízení kopie však musí být klient informován. Pokud klient vyjádří nevůli k pořízení kopie, smí banka pořídit pouze výpis z dokladu totožnosti, a to pouze v rozsahu údajů nezbytných pro dosažení AML účelu. Pořízením kopie dokladu totožnosti může banka, s přihlédnutím k celkovému rizikovému profilu klienta, podmínit poskytnutí služby. Banky postupují v souladu s metodickými pokyny a doporučeními FAÚ.

Pokud doklad, z něhož je pořizována kopie, obsahuje údaje, které nejsou nezbytné pro AML účel (starší verze dokladů, údaje uváděné dobrovolně – např. rodinný stav), nejsou tyto údaje systémově

zpracovávány a jejich výskyt je nahodilý; s ohledem na integritu pořizované kopie i technickou náročnost maskování vybraných údajů (různé šablony dokladů) je ponechání těchto údajů na kopii přípustné.

Kromě identifikačních dokladů jsou banky povinny rovněž uchovávat kopie dokumentů a informací získaných v rámci kontroly klienta dle § 9 AML zákona. Kontrola klienta se provádí mimo jiné při vzniku a v průběhu obchodního vztahu, provedení transakce nad určitý finanční limit nebo při podezření na praní peněz nebo financování terorismu, při navázání obchodního vztahu s politicky exponovanou osobou nebo klientem usazeným ve vysoce rizikové třetí zemi.

V případě, že banka při své činnosti vyplývající z AML legislativy pořídí kopie dokladů předložených při identifikaci či kontrole klienta, je povinna je uchovávat po dobu 10 let od uskutečnění obchodu nebo od ukončení obchodního vztahu s klientem. S uložením těchto kopií dokladů klient souhlas neuděluje a jeho případný nesouhlas nemá na jejich uložení žádný vliv. Lhůta začíná běžet prvním dnem kalendářního měsíce následujícího po kalendářním měsíci, ve kterém byl uskutečněn poslední úkon obchodu známý povinné osobě. Po uplynutí této lhůty zajistí příslušný správce výmaz uchovávaných údajů a zničení dokladů, pokud neexistuje jiný právní titul pro uchovávání údajů a dokladů. Banka musí zajistit vhodnými technickými a organizačními opatřeními vysokou míru zabezpečení přístupu k uloženým kopiím dokladů po celou dobu jejich zpracování (řízení přístupových práv, logování přístupů).

b) Zpracování rodného čísla

Zpracování rodného čísla je upraveno zákonem č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů. Tento zákon taxativně vymezuje případy, kdy je možné rodné číslo využívat. Jedním z těchto případů je situace, kdy tak stanoví zvláštní zákon. Pro banky je tímto zákonem č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů (dále jen „ZoB“), který uvádí, že *„Banky a pobočky zahraničních bank jsou povinny pro účely bankovních obchodů zjišťovat a zpracovávat údaje o osobách včetně rodného čísla, pokud bylo přiděleno, vyjma citlivých údajů o fyzických osobách, potřebné k tomu, aby bylo možné bankovní obchod uskutečnit bez nepřiměřených právních a věcných rizik pro banku.“.* Současně i AML zákon v § 5 stanovuje povinnost získat identifikační údaje klienta, kterým se rozumí mimo jiné i rodné číslo, bylo-li přiděleno, jako jeden ze základních identifikačních údajů.

Banky od klientů ani dalších osob, jejichž údaje při bankovních obchodech zpracovávají na základě plnění svých právních povinností, nevyžadují souhlas se zpracováním rodného čísla.

## INTERNÍ POVINNOSTI BANKY

### 1. Postavení, role a činnost DPO

Základní požadavky na postavení, roli a činnosti DPO vycházejí z Oddílu 4, článků 37-39 GDPR. Banky jsou povinny jmenovat DPO zejména dle čl. 37 odst. 1 písm. b) GDPR.

Postavení DPO v rámci organizace musí být nezávislé, čehož je docíleno zejména:

- jednoznačným vymezením pozice DPO v hierarchii organizace s přímým napojením na vrchní řídící úroveň (zpravidla 1. nebo 2. úroveň řízení pod představenstvem, tzv. B-1 nebo B-2),
- zařazením do kontrolní (dohledové) struktury organizace, která se přímo nepodílí na výkonu provozních činností banky, a to až do úrovně člena nejvyššího vedení, kterému je DPO podřízen (tzv. 2nd Line of Defense).

Role DPO by měla být ustanovena jako samostatná, nikoliv sloučená s výkonem jiných činností. Pozice DPO může být ustanovena zcela samostatně jako např. „Kancelář DPO“ nebo v rámci širší struktury útvarů např. Compliance nebo Právní podpory. K zamezení konfliktu zájmů nemůže být pozice DPO vytvořena v útvarech, které se přímo podílí na realizaci opatření pro ochranu osobních údajů, popř. na jejich zpracování, jako např. oddělení IT, Lidských zdrojů, Zpracování klientských transakcí, apod.

V zájmu zajištění jednotného přístupu k subjektům údajů a efektivity činnosti DPO může DPO vykonávat svou působnost v rámci celé skupiny podniků banky, které poskytují služby zejména retailovým klientům. Činnost DPO v rámci skupiny je pak vykonávána na základě outsourcingových smluv.

S přihlédnutím k velikosti banky, resp. skupiny, a rozsahu jejích činností musí správce zajistit dostatečné prostředky pro výkon činnosti DPO, zejména pak dostatečnou a konkrétně vymezenou personální kapacitu.

V rámci své činnosti DPO:

- Poskytuje poradenství (konzultace) k výkonu činností zpracování na žádost útvarů správce, např. s ohledem na určení správných zákonných titulů zpracování dle článku 6 GDPR, apod.
- DPO může být pověřen vedením záznamů zpracování, není však odpovědný za úplnost evidence činností zpracování správce (povinnost a odpovědnost za oznámení všech prováděných zpracování DPO mají vlastníci těchto zpracování z provozních útvarů banky).
- Vydává posudek k závěrům Posouzení vlivu na ochranu osobních údajů (DPIA) vypracovaných správcem, ale Posouzení neschvaluje.
- Vyjadřuje se na vyžádání k výsledkům balančních testů, které však nevypracovává ani neschvaluje.
- Vydává stanoviska a metodické pokyny k uplatňování ochrany osobních údajů při výkonu činností správce.
- Provádí vlastní kontrolní a dohledovou činnost k ujištění se o souladu činností správce s GDPR. V rámci této kontroly nepodléhá příkazům jiných útvarů správce ani vedení banky, ale stanovuje si vlastní plán a postupy kontrolní činnosti.
- Pravidelně, minimálně 1x ročně, nebo dle aktuální potřeby, informuje nejvyšší vedení banky o souladu výkonu činností správce s GDPR a výsledcích své kontrolní činnosti. V této souvislosti může předkládat vedení souhrnnou výroční zprávu o souladu činností správce s požadavky GDPR.
- Může se podílet na hodnocení rizik a dopadů případů porušení zabezpečení osobních údajů zjištěných správcem, zejména s ohledem na posouzení výše rizika vyžadující ohlášení Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ“) nebo oznámení dotčeným subjektům údajů.
- Může se podílet na zvyšování povědomí a odborné přípravy pracovníků správce v oblasti ochrany osobních údajů, např. podílením se na přípravě vzdělávacích podkladů, poskytováním školení, apod. DPO však neodpovídá za plán vzdělávání a jeho realizaci.
- Působí jako kontaktní místo pro subjekty údajů.
- Působí jako kontaktní místo pro ÚOOÚ.

Pro zajištění udržení odborných znalostí DPO v oblasti práva a praxe ochrany osobních údajů musí správce zajistit dostatečné prostředky pro vzdělávání DPO a určených specialistů ochrany osobních

údajů, zejm. formou účasti na odborných konferencích a seminářích. Vhodnou praxí je i zajištění certifikace znalostí pro výkon funkce DPO (např. IAPP).

## 2. Záznamy o činnostech zpracování

Banka jako správce i zpracovatel osobních údajů je povinna vést záznamy o činnostech zpracování. Základní obsah záznamů o činnostech zpracování je stanoven v čl. 30 GDPR. Banka rozlišuje záznamy o činnostech zpracování v postavení správce a záznamy o činnostech zpracování, které vykonává v postavení zpracovatele.

V praxi může nastat situace, kdy banka je obecně v postavení správce osobních údajů, ale zároveň také provádí určité zpracování pro jiného správce a ve vztahu k těmto činnostem zpracování a osobním údajům je pak současně i v postavení zpracovatele (např. při poskytování outsourcingu služeb v rámci finanční skupiny). V takovém případě lze vypracovat jeden záznam o činnosti zpracování, přičemž v nástroji vedení evidence musí být obě role banky uvedené a odlišitelné.

### Forma záznamů o činnostech zpracování

Banka si individuálně stanoví jednotnou (rámcovou) strukturu záznamů o činnostech zpracování. Bankou zvolená struktura záznamů by měla být přehledná a srozumitelná. Po stránce obsahové záznamy obsahují nejméně informace specifikované v čl. 30 odst. 1 GDPR v případě, že banka je správcem, nebo v čl. 30 odst. 2 GDPR, pokud je banka zpracovatelem. Záznamy o činnostech mohou obsahovat i informace, které GDPR nevyžaduje, např. zda pro činnost zpracování byla zpracována DPIA nebo v jakých systémech jsou osobní údaje zpracovávány. Banka není povinna zahrnout do záznamů kompletní dokumentaci vztahující se k dané činnosti zpracování, může na danou dokumentaci odkázat (např. odkazem na interní předpis o technických a organizačních opatřeních). Právě tak mohou záznamy o činnostech zpracování obsahovat odkazy na příslušné normy.

### Vypracování a revize záznamů o činnostech zpracování

Záznamy o činnostech zpracování banka vypracovává před zahájením činnosti zpracování. Pokud dochází ke změně procesu již probíhajícího zpracování, banka aktualizuje záznam o činnosti zpracování nejpozději současně se zavedením změny činnosti zpracování. Banka reviduje záznamy o činnosti zpracování v pravidelných intervalech.

Za příklad dobré praxe lze označit vypracování interní metodiky, ve které budou popsána pravidla pro vypracovávání záznamů o činnosti zpracování, jejich obsah, odpovědnost pracovníků banky za vypracování a aktuálnost záznamu o činnosti zpracování a stanovena pravidla pro životní cyklus záznamů o činnostech zpracování.

### Granularita záznamů o činnostech zpracování

Podle povahy konkrétního zpracování může banka přistoupit k členění záznamů o činnostech zpracování. Banka si může interně stanovit, podle jakých kritérií bude sdružovat operace zpracování do záznamů o činnostech zpracování. Za příklad dobré praxe lze uvést členění záznamů o činnostech zpracování podle účelu zpracování, případně podle svých procesů (např. podle určitých agend), produktů nebo podle svých technických podmínek (např. s ohledem na své systémy). Pokud banka zvolí členění záznamů o činnostech zpracování podle jiného kritéria, než je účel zpracování, může jedna činnost zpracování zahrnovat více účelů zpracování.

## 3. Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů bývá často označováno také anglickou zkratkou DPIA *(„data protection impact assessment“*) a je prostředkem pro řízení rizik spojených s bankou zaváděnými procesy zpracování osobních údajů.

V souvislosti s každým novým zpracováním osobních údajů nebo změnou stávajícího zpracování by banka měla zvážit, zda je či není v daném případě nutné posouzení vlivu na ochranu osobních údajů provést, a to na základě:

a) zohlednění nutných případů zpracování Posouzení uvedených v čl. 35, odst. 3 GDPR;

b) ověření, že zpracování není uvedeno na seznamu druhů operací, které nepodléhají posouzení, zveřejněném ÚOOÚ[3];

c) vyhodnocení kritérií uvedených na seznamu druhů operací zpracování, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů, zveřejněném ÚOOÚ [4].

Provedení DPIA není nutné pokud:
a) povaha, rozsah, kontext a účel zpracování jsou velmi podobné zpracování, pro které byla DPIA bankou již provedena;

b) operaci zpracování zkontroloval ÚOOÚ před 25. květnem 2018 za konkrétních podmínek a parametrů zpracování, které se od té doby nezměnily;

c) zpracování má právní základ v právu EU nebo členského státu, pokud toto právo upravuje konkrétní operaci zpracování a pokud bylo posouzení vlivu na ochranu osobních údajů již provedeno v souvislosti s přijetím uvedeného právního základu, ledaže by členský stát prohlásil, že považuje provedení tohoto posouzení vlivu na ochranu osobních údajů před činnostmi zpracování za nezbytné;

d) právní předpis stanoví povinnost konkrétní zpracování osobních údajů Bance provést (§ 10 zákona č. 110/2019 Sb., o zpracování osobních údajů).

V případě, že bude vyhodnoceno, že DPIA je nutná, postupuje banka v souladu s metodikou vydanou ÚOOÚ[5]
nebo obdobnou metodikou a provede alespoň:

a) systematický popis zamýšlených operací zpracování, který v zásadě vychází ze záznamů o činnostech zpracování, popř. obsahující diagram (workflow) popisující zpracování (tok)

[3] Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů. Aktuální verze 1.0 je dostupná na https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940. Seznam podléhá schválení Evropským sborem pro ochranu osobních údajů a může zaznamenat určité změny.

[4] dtto

[5] Metodika obecného posouzení vlivu na ochranu osobních údajů, Verze 1.0 ze dne 11. listopadu 2020 dostupná na https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=46487

osobních údajů, včetně případných vazeb na jiná zpracování osobních údajů, a určení agend a útvarů zajišťujících zpracování osobních údajů;

b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů prostřednictvím testu proporcionality;
c) posouzení rizik pro práva a svobody subjektů údajů, při kterém banka postupuje v souladu s obecnou analýzou rizik[6] pro zajištění konzistentnosti přijatých opatření, v rámci které banka identifikuje primární a podpůrná aktiva, jejich zranitelnosti a z nich vyplývající hrozby; a
d) popis plánovaných opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k prokázání souladu s GDPR a stanovení míry zbytkového rizika po realizaci identifikovaných opatření.

Pokud se nepodaří dostatečně snížit míru zbytkového rizika (dle metodiky ÚOOÚ pod hodnotu 48), musí banka zahájit předchozí konzultaci s ÚOOÚ.

V rámci bankovního sektoru se povinnost přípravy DPIA typicky dotkne záležitostí jako např.:

- zavedení nového zpracování zahrnujícího biometrické údaje (např. autentizace obličejem – tzv. face ID nebo autentizace hlasem);
- zavedení nového prodejního kanálu banky (např. nová online platforma);
- zavedení nového automatizovaného procesu pro scoring klientů;
- zavedení zcela nového produktu.

Ve vhodných případech přitom banka do výše popsaného procesu DPIA zapojí relevantní třetí osoby, případně včetně subjektů údajů, resp. jejich zástupců, formou konzultací.

Výsledné posouzení vlivu, vč. akceptace zbytkového rizika, schvaluje odpovědná osoba určená správcem, odlišná od DPO.

Banky nejsou povinny výsledky DPIA zveřejňovat. DPIA není jednorázový proces, a banka proto periodicky nebo v případě mimořádné události kontroluje dodržování závěrů DPIA v rámci nastavených procesů a ověřuje, zda nedošlo ke změně vstupních parametrů nebo rizik, které by odůvodňovaly přehodnocení dosavadního procesu a případně spuštění nového procesu DPIA, včetně přehodnocení požadavků na vypracování DPIA (uplatnitelnost výjimky apod.).

Za případ dobré praxe lze označit zpracování interní metodiky popisující vztah DPIA k projektovému (change) managementu, odpovědnost jednotlivých pracovníků banky včetně jejich zapojení do procesu DPIA a kritérií pro vypracování posouzení (dle seznamu vydaného ÚOOÚ), zda je či není DPIA třeba, vypracování samotné DPIA a jejího životního cyklu.

## 4. Doba uchování (archivace) údajů

*(Pro účely tohoto dokumentu je počátkem běhu doby uchování údajů po fázi jejich aktivního zpracovávání v rámci poskytované služby zpravidla okamžik ukončení smlouvy, tj. jednotlivého bankovního obchodu, mezi bankou a klientem. S ohledem na rozsah zpracovávaných údajů a*

[6] viz například povinnost dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, pokud se předmětné povinnosti na banku vztahují.

*komplexitu informačních systémů bank může však v některých případech být stanoven počátek lhůty uchování údajů ukončení vztahu s klientem, tj. všech jeho smluv.)*

Banky jako správci osobních údajů mají celou řadu povinností, které musí při zpracování osobních údajů plnit, a to včetně povinnosti uchovávat osobní údaje o klientech a bankovních operacích pro účely plnění povinností stanovených sektorovou regulací i po ukončení samotného bankovního obchodu. V souladu se zásadou „omezení uložení" mají být tyto údaje uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Z pohledu GDPR lze při výkonu bankovní činnosti nalézt oporu pro zákonné zpracování v případě uchovávání osobních údajů zejména v rámci právních titulů:

I. zpracování nezbytné pro splnění právní povinnosti (uložené sektorovou regulací, včetně specifických lhůt pro takové uchovávání), která se na banky vztahuje, a to zejména

   a) ZoB, který stanoví zejména povinnost zpracování osobních údajů nezbytných pro uskutečnění obchodu a posouzení rizik;
   b) AML zákonem, který bankám stanoví povinnost zpracovávat osobní údaje zejména pro účely identifikace a následné kontroly klienta;
   c) zákonem č. 256/2004 Sb., o podnikání na kapitálovém trhu, ve znění pozdějších předpisů (dále jen „ZPKT"), vztahujícím se zejména na záznamy komunikace a dokumenty týkající se poskytnuté investiční služby;
   d) zákonem č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů, týkajícím se uchovávání osobních údajů pro účely archivnictví.

   Zákon o bankách stanoví povinnost uchovávat údaje o uskutečněných obchodech po dobu 10 let od jejich ukončení. Tuto lhůtu tak lze považovat s ohledem na realizované obchody za základní pro všechny interakce banky se svými klienty.

II. zpracování nezbytné pro účely oprávněných zájmů banky, a to zejména ve vztahu k

   a) uplatňování práv v občanském soudním řízení

   Zákon č. 89/2012 Sb., občanský zákoník (dále jen „OZ"), který stanoví promlčecí lhůtu 15 let pro úmyslně způsobené škody nebo újmy a úmyslně nabyté bezdůvodné obohacení. Z tohoto důvodu by banka měla mít oprávněný zájem archivovat data o klientech po dobu 15 let (dokud nebudou potenciální nároky klienta promlčeny). Přiměřenost této lhůty vyhodnotí banka v rámci balančních testů, ideálně na úrovni jednotlivých kategorií bankovních obchodů, a to i s ohledem na pravděpodobnost a důsledky takového úmyslného jednání a reálně pozorovaný časový horizont jejich odhalení.

   b) uplatňování práv v trestním řízení a
   c) uplatňování práv ve správním řízení

   Na dobu, po kterou musí banka údaje držet pro ochranu svých práv, mají vliv také promlčecí doby přestupků a trestných činů, kterých by se banka, resp. jednající osoby mohly potenciálně dopustit. Pro účely prokázání, že nedošlo ke spáchání přestupku ani trestného činu by banka měla uchovávat údaje o provedených obchodech, v odůvodněných případech až po dobu 15 let od skončení obchodu, pokud další uchování není v konkrétním případě nezbytné. Promlčecí doba přestupků vyplývajících ze ZoB, AML a ZPKT je 3letá (zákon č. 250/2016 Sb., o odpovědnosti za

přestupky a řízení o nich), promlčecí doby trestných činů vychází ze zákona č. 40/2009 Sb., trestní zákoník (dále jen „TZ“). Na trestné činy, kterých by se banka mohla dopustit, se vztahuje 15letá promlčecí doba (např. zpronevěra, podvod, zneužití informace v obchodním styku atd.). Uplatnění konkrétní přiměřené lhůty musí reflektovat pravděpodobnost a skutečně pozorované události rozhodné pro posouzení účelu této lhůty pro daný typ činnosti banky.

S ohledem na skutečnost, že řízení lhůt uchování a následné mazání/anonymizace údajů jsou zpravidla zajištěny systémovými dávkovými procesy, je přiměřené, že základní lhůta odvozená z výše uvedených předpokladů se prodlouží až o 1 rok. Rovněž tak v případech, kdy může dojít ke stavení promlčecí doby, může být v zájmu banky v některých případech uchovávat osobní údaje po dobu dalších 2 let po uplynutí 15leté lhůty po skončení obchodu za účelem prevence důkazní nouze v případě soudního sporu. Ze zkušeností ze soudní praxe se banka nemusí dozvědět o tom, že již nějaké řízení proti ní bylo zahájeno – jde o obvyklou soudní praxi, kdy předtím, než se žalovaný dozví o podání žaloby (tj. je mu zaslána od soudu k vyjádření), může soud od podání žaloby (což je okamžik stavějící promlčecí dobu) provést celou řadu procesních úkonů (např. rozhodnutí o příslušnosti soudu k rozhodnutí, rozhodnutí o osvobození od soudního poplatku, rozhodnutí o podjatosti soudce, výzva soudu žalobci k doplnění žaloby v případě chybějících základních náležitostí apod.). O těchto soudních úkonech nemá žalovaný obvykle žádné informace a opakovaná praxe ukazuje, že se žaloba k bance dostane až s velkým zpožděním. Z tohoto důvodu banky mohou využít přiměřenou časovou rezervu dvou let.

## 5. Podmínky uchovávání osobních údajů

Banky mají povinnost zajistit, aby informace, týkající se zejména účelu zpracování, kategorií osobních údajů, kategorií subjektů údajů, kategorií příjemců a doby uchování byly subjektům údajů (klientům) sděleny před začátkem zpracování v rámci plnění informační povinnosti.

V rámci zachování principu proporcionality je nezbytné posoudit zpracování (uchovávání) osobních údajů individuálně a neaplikovat lhůty plošně tak, aby osobní údaje nebyly uchovávány po dobu delší než nezbytnou k účelu zpracování. Aby bylo zajištěno, že osobní údaje nebudou uchovávány déle, než je nezbytné, měly by banky lhůty pro uchovávání osobních údajů rovněž pravidelně přezkoumávat včetně průkazné dokumentace.

Dále musí být přijata vhodná opatření, aby byla zajištěna oprava nebo výmaz osobních údajů, které jsou předmětem zpracování, tedy, aby byla respektována práva subjektu údajů, zejména právo na to, aby jeho osobní údaje byly vymazány a nebyly dále zpracovávány, pokud již neexistuje právní titul pro jejich zpracování.

Dále musí být stanovena taková technická a organizační opatření, aby bylo zamezeno jejich neoprávněnému zpracování, zejména přijetí takových opatření, která vedou k zajištění jejich bezpečnosti, důvěrnosti a integrity. Pokud banky využívají pro některé činnosti zpracovatele, jsou rovněž povinny zajistit po ukončení zpracování, aby zpracovatel osobní údaje vrátil nebo vymazal, jestliže není podle práva Unie nebo členského státu, které se na zpracovatele vztahuje, požadováno uložení těchto osobních údajů.

Co do formy uchovávání osobních údajů, osobní údaje by měly být dále zpracovány pouze tehdy, nemůže-li být účelu zpracování přiměřeně dosaženo jinými prostředky. V takovém případě je nezbytné vést v patrnosti práva klientů na ochranu před neoprávněným zasahováním do soukromého a osobního

života, a jakmile je to možné, osobní údaje smazat, případně anonymizovat, tedy nezpracovávat ve formě, která umožňuje identifikaci subjektu údajů.

## VZTAH KE KLIENTŮM

### 1. Zajištění práv klientů bank

#### 1.1 Právo na omezení zpracování

Správce je na základě čl. 18 GDPR v několika taxativně vymezených případech povinen omezit zpracování osobních údajů subjektů údajů. Jedná se o situaci, kdy:

- subjekt údajů popírá přesnost osobních údajů[7],
- zpracování je protiprávní nebo již není nezbytné pro dosažení účelu, ale subjekt údajů místo jejich výmazu požaduje jejich uchování[8],
- subjekt údajů vznesl námitku proti zpracování osobních údajů založeném na oprávněném zájmu správce či další osoby[9].

Omezením zpracování se dle definičního ustanovení v čl. 4 bodu 3 GDPR rozumí označení předmětných údajů tak, aby bylo omezeno jejich další zpracování v budoucnu. Podle příslušného recitálu způsoby omezení zpracování zahrnují např. dočasný přesun dotčených údajů do jiného systému zpracování, znepřístupnění údajů uživatelům či jejich dočasné stažení z veřejně dostupných internetových stránek.[10]

Technické řešení omezení zpracování bude obecně vždy záviset na systému a prostředcích, ve kterém, resp. jejichž prostřednictvím, jsou data zpracovávána, ať už automatizovaně, nebo manuálně. Omezení může být s ohledem na rozsah zpracování, komplexitu technických prostředků i povinnost banky zajišťovat pro klienta, který tento podnět učinil, další služby, realizováno i přidáním specifického příznaku k daným údajům. Nemusí se tedy nezbytně jednat jen o blokování či skrytí údajů.

Banka může po klientovi, který uplatní podnět týkající se omezení zpracování osobních údajů, požadovat alespoň základní odůvodnění tohoto podnětu. Banky mohou vyžadovat, aby byl podnět určitý a srozumitelný, a aby dotčený subjekt údajů byl dostatečně identifikovaný.

Podnět směřující proti přesnosti údajů musí obsahovat specifikaci údaje či kategorie bankou zpracovávaných údajů, které mají být dle názoru klienta nepřesné, a klient by měl alespoň označit (či přímo přiložit) podklady na podporu svého tvrzení. Pouze v takovém případě pak banka přistoupí k omezení zpracování (a sdělí tuto skutečnost i příjemcům údajů) a zahájí přezkum daného podnětu.

[7] Čl. 18 odst. 1 písm. a) GDPR.
[8] Čl. 18 odst. 1 písm. b) a c) GDPR.
[9] Čl. 18 odst. 1 písm. d) GDPR.
[10] Recitál čl. 67 GDPR.

V případě, že se klient domáhá omezení zpracování z důvodu nepřesnosti osobních údajů, banka omezí jen zpracování těch osobních údajů, u kterých je namítána nepřesnost (klient např. namítá, že jeho kontaktní adresa je nepřesná a banka po dobu omezeného zpracování na takovou adresu nezasílá žádnou komunikaci); ostatní osobní údaje však může nadále zpracovávat bez omezení. V případech uvedených v čl. 18 odst. 1 písm. b) a c) GDPR je banka povinna vyhovět žádosti subjektu údajů a omezit zpracování jen za podmínky, že taková žádost jí je doručena před vymazáním osobních údajů.

Omezení zpracování také může mít přímý dopad na služby poskytované bankou. Toho si sice klient nemusí být vědom, avšak omezení zpracování může mít za následek rozpor s povinností poskytovat službu (službu jako takovou nebo službu s určitými parametry) podle zvláštního právního předpisu. Za příklad nejlepší praxe lze označit postup, kdy banka žádost o omezení zpracování nejprve na základní úrovni posoudí i z hlediska dopadu na poskytované služby a pokud takto závažný dopad pro klienta identifikuje, klienta na tento důsledek a na možnost vyjádřit souhlas se zpracováním nezbytným pro tuto službu[11] upozorní.

### 1.2 Právo na výmaz

Podmínky, při jejichž splnění je správce povinen osobní údaje dotčené osoby vymazat[12], jsou taxativně vypočteny v čl. 17 odst. 1 GDPR. Výjimky z nich, resp. situace, kdy správce není povinen údaje vymazat, jsou pak uvedeny v čl. 17 odst. 3 GDPR.

Situace, kdy dotčená osoba může uplatnit právo na výmaz, lze rozdělit do několika skupin případů:

- uchování či jiné zpracování osobních údajů dotčené osoby je protiprávní[13],
- správci je uložena právní povinnost osobní údaje vymazat[14],
- dotčená osoba odvolá souhlas se zpracováním osobních údajů a správce nemá jiný právní titul pro jejich zpracování [15],
- uplatnění principu opt-out ze zpracování údajů pro přímý marketing[16].

U prvních dvou případů není v činnosti bank spatřováno žádné specifikum. Pokud je zpracování osobních údajů protiprávní nebo je bance uložena povinnost dané údaje vymazat, je banka povinna postupovat v souladu s právem.

V bankovním prostředí na základě souhlasu dotčených osob probíhá jen velmi malá část zpracování osobních údajů. V případě klientů je bance sektorovými předpisy, především ZoB, AML, zákonem č. 257/2016 Sb., o spotřebitelském úvěru (dále jen „ZSÚ“) či ZPKT, uložena povinnost klienta identifikovat a uchovávat údaje o něm a obchodech s ním i řadu let po skončení obchodního vztahu.

[11] Čl. 18 odst. 2 GDPR.
[12] Účelu souvisejících ustanovení GDPR lze dosáhnout jak úplným vymazáním osobních údajů, tak i jejich nevratnou anonymizací.
[13] Čl. 17 odst. 1 písm. a), c) a d) GDPR.
[14] Čl. 17 odst. 1 písm. e) GDPR.
[15] Čl. 17 odst. 1 písm. b) a písm. f) ve spojení s čl. 8 odst. 1 GDPR.
[16] Čl. 17 odst. 1 písm. c) ve spojení s čl. 21 odst. 2 GDPR.

V případě zaměstnanců je pak banka povinna řídit personální bezpečnost jako součást svého obezřetného podnikání, ale i povinnost, která jí je ve vztahu k některým skupinám zaměstnanců uložena zvláštním zákonem (ZSÚ, zákon o distribuci pojištění a zajištění, u některých bank zákon o kybernetické bezpečnosti). I na banku jako na zaměstnavatele pak dopadá povinnost zpracovávat a uchovávat řadu údajů o zaměstnancích na základě zvláštních zákonů nebo pro ochranu jejich či svých oprávněných zájmů.

K otázce přímého marketingu lze uvést, že předmětná norma bezprostředně nedopadá na elektronicky zasílaná marketingová sdělení, tzn. komunikaci zaslanou na elektronické kontakty (e-mail, telefonní číslo), protože ta mají samostatný právní režim (srov. čl. 95 GDPR, který odkazuje na ePrivacy směrnici, která je v této části transponována zákonem č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů). Dopadá tedy na přímý marketing ve formě fyzického zasílání nabídek a telefonických hovorů a na zpracování osobních údajů a související profilování při přípravě nabídek zasílaných elektronicky. Pokud se jedná o klienty či jiné osoby, o kterých je banka povinna údaje uchovávat na základě výše zmíněných právních předpisů a jejich údaje jsou nezbytné pro realizaci bankovních obchodů a plnění právních povinností banky, ani po vyjádření nesouhlasu s přímým marketingem je banka nemůže vymazat. Na tuto situaci se totiž uplatní výjimka čl. 17 odst. 3 písm. b) GDPR. Fakticky se tak v tomto případě bude jednat zejména o vyjádření odmítnutí zpracování za účelem přímého marketingu a o případné smazání odvozených údajů využitých pouze k marketingu, typicky spotřebitelského profilu, nikoliv o vymazání dat jako takových.[17]

V praxi tak k úplnému výmazu osobních údajů zpracovávaných bankou bude docházet obvykle jen u osob, které nejsou klienty či žadateli o produkt banky nebo jejími zaměstnanci, ale jejichž údaje banka shromáždila a zpracovává zejména pro marketingové účely.

V souvislosti s výmazem osobních údajů, ať už na základě žádosti dotčené osoby, nebo při pravidelném procesu nastaveném bankou, je nutné s ohledem na specifika v bankovním prostředí upřesnit ještě několik procesních či technických aspektů:

- ✓ Pokud banka hodlá osobní údaje vymazat, má smazat i záznamy o tom, že je v minulosti zpracovávala a kdy je vymazala?

Při řešení této otázky je nutno vycházet především ze smyslu práva na výmaz, jímž je obvykle nevratná likvidace jiných než identifikačních údajů (přímých identifikátorů), zejména údajů o ryze osobní, ekonomické, společenské či kulturní identitě. Naproti tomu pouhé uchování po přiměřenou dobu, nikoliv aktivní využívání, identifikačních údajů subjektu údajů spolu s informací o tom, jaké kategorie osobních údajů, příp. v jakém období a z jakého důvodu správce zpracovával a informací o realizaci výmazu, zejména ve formě logu, a související komunikace se subjektem údajů, lze označit za zpracování údajů nezbytné pro ochranu oprávněného zájmu správce[18]. Tímto zájmem je schopnost doložit splnění požadavku subjektu údajů a tím i splnění čl. 17 GDPR a vyhnutí se riziku sankce[19] či jiného postihu. Za

[17] Zpracování osobních údajů za marketingovými účely je komplexně pojednáno v kapitole 2.
[18] Nejméně po dobu běhu promlčecí, resp. prekluzivní lhůty.
[19] Za porušení povinností upravených v čl. 17 GDPR lze v souladu s čl. 83 odst. 5 písm. b) téhož předpisu uložit pokutu až do výše 20 000 000 euro nebo 4 % celkového světového ročního obratu skupiny za předchozí finanční rok.

tímto účelem by zpracovávané údaje měly být uchovávány samostatně a správce je povinen zajistit, že nebudou využity za jiným účelem. Údaje v uvedeném rozsahu uchovávané za tímto účelem, např. jako součást logu, samy o sobě nemohou být předmětem úspěšné žádosti o výmaz, v případě, že trvá oprávněný zájem správce na jejich uchování, neboť se na ně nevztahuje žádná z možností upravených v čl. 17 odst. 1 GDPR.

Na základě právní úpravy lze považovat za přijatelné řešení také postup, kdy dojde k nevratnému výmazu všech osobních údajů nebo k nevratnému výmazu identifikačních údajů subjektu údajů a zbývající osobní údaje se v důsledku toho stanou anonymizovanými údaji. Předpokladem pro tento postup je skutečnost, že správce má jasně stanovená interní pravidla o vymazávání identifikačních údajů po uplynutí předem definovaných dob. Ze žádného ustanovení GDPR neplyne pro správce povinnost prokazovat datum výmazu konkrétního osobního údaje (správce si ale samozřejmě může nastavit takové řešení, které toto bude umožňovat). Proto by v tomto případě mělo postačovat, aby správce byl schopen prokázat, že má nastavena pravidla pro likvidaci všech osobních údajů nebo identifikačních údajů podle předem vydefinovaných dob a že nadále neeviduje (veškeré osobní údaje byly nevratně vymazány), ani jinak nezpracovává žádné zbývající osobní údaje, u kterých již uplynula stanovená doba pro jejich zpracovávání nebo u kterých nedisponuje titulem k takovému zpracování.

Možné jsou obě varianty. Záleží vždy na konkrétní bance, správci údajů, kterou z nich zvolí s ohledem na své vnitřní procesy a technické prostředí. Celý proces však musí být popsán ve vnitřních předpisech a dokumentován.

✓ Ve kterých úložištích je nutné data bezprostředně mazat?

Výmaz údajů musí být realizován především v aktivně využívaných databázích a systémech. Povinnost bezodkladně realizovat výmaz údajů není nutné ve stejném rozsahu aplikovat i na systémy určené pouze k uchování údajů, u kterých obvykle postačí plošné mazání údajů v předem stanovených lhůtách. V případě obnovení dat ze záloh je následně nutné, aby osobní údaje, u kterých pominul účel zpracování, byly smazány.

✓ Jak realizovat právo na výmaz v případě fyzicky vedené dokumentace?

V případě fyzicky vedené dokumentace obsahující osobní údaje je dostatečným postupem, když banka vede, resp. archivuje smluvní dokumentaci konkrétního klienta a ke skartaci přistoupí až po vypršení zákonné lhůty po skončení posledního z obdobných produktů poskytnutých danému klientovi.

### 1.3 Právo na přenositelnost

Přenositelností se rozumí předání některých údajů subjektu údajů od jednoho poskytovatele služeb ke druhému nebo k samotnému subjektu údajů. Dalo by se říct, že právo na přenositelnost doplňuje již zavedené právo na přístup k osobním údajům.

Z nařízení GDPR vyplývá, že aby mohlo dojít k přenosu dat subjektu údajů, musí být kumulativně splněny následující podmínky:

a) zpracování je založeno na souhlasu nebo smlouvě[20], a
b) zpracování se provádí automatizovaně[21].

Forma předávaných údajů

Předávávané osobní údaje se mají dle nařízení GDPR poskytnout ve strukturovaném, běžně používaném a strojově čitelném formátu (např. XML, CSV). To ovšem neznamená, že nový správce musí údaje od původního správce bezvýhradně přijmout, neboť GDPR nestanovuje povinnost správce taková data dále zpracovat. I když správce použije jeden z běžně používaných a strojově čitelných formátů, automaticky to nemusí implikovat „čitelnost dat" u příjemce dat/u nového správce, ke kterému subjekt údajů data přenáší. Subjekt by neměl mít právo vybrat si, jakým způsobem se údaje budou novému správci posílat. Je na bance, aby zohlednila a rozhodla o způsobu předání dat a posoudila, zda je přenos technicky proveditelný a bezpečný. To, že banka zvolí bezpečný a zároveň přiměřený způsob komunikace, byť třeba odlišný od toho, který zvolil klient (např. prostřednictvím k tomu účelu vytvořené aplikace třetí strany) neznamená, že banka nesplnila svoji povinnost podle čl. 20 GDPR. O tomto je subjekt údajů informován.

Rozsah předávaných údajů bankami

S ohledem na rozsah a citlivost informací zpracovávaných v bankovním sektoru, mj. i s přihlédnutím k bankovnímu tajemství, by mělo toto právo být vykládáno v širším slova smyslu. Proto je rovněž možné v některých případech požadovat po subjektu údajů zdůvodnění konkrétní žádosti. Rozsah dat by měl být limitován pouze na data subjektu údajů s ohledem na skutečnost, že subjekt údajů má právo volně nakládat právě s vlastními osobními údaji. Osobní údaje, u kterých dochází k přesunu, by měly být ty, které byly aktivně poskytnuty subjektem údajů, buď skrze písemný nebo webový formulář, za účelem uzavření smlouvy o poskytnutí produktu nebo služby, případně aktivně poskytnuty na základě souhlasu. Toto právo by nemělo být uplatňováno na data, která banka odvodí z chování subjektu údajů. Takovými daty mohou být například platební transakce, které klient provedl nebo informace poskytnuté v rámci telefonického hovoru s klientem. Předání takových informací v rámci práva na přenositelnost by zasahovalo do práv třetích osob. Banky považují za velmi problematické přenášet data v neomezeném rozsahu na základě žádosti klienta, a to zejména s ohledem na rozsah dat zpracovávaných bankami. Příliš extenzivní výklad práva na přenositelnost by byl ostatně v rozporu s účely zpracování, neboť každý správce může zpracovávat pouze nezbytně nutný rozsah údajů, proto i z tohoto důvodu není na místě, aby banky předávaly například telefonním operátorům údaje o platebních transakcích. Navíc při přenosu dat je třeba vždy myslet na to, aby nebyla nepříznivě dotčena práva třetích stran, povinnost dbát na bezpečnost předávaných dat a tím zároveň chránit subjekt údajů.

S ohledem na rozsah zpracovávaných dat musí být bankovní sektor referencí pro bezpečnost dat, zejména pro velmi silné technické a organizační zabezpečení dat. V zájmu subjektu údajů je, aby banky vykládaly právo na přenositelnost údajů tak, aby důvěrná data podléhající bankovnímu tajemství nemohla být zneužita třetí stranou. V rámci finančního sektoru budou banky poskytovat pouze takové informace, které pro subjekt údajů nejsou jednoduše dostupné a směřují primárně k tomu, aby byl schopen si obdobný / srovnatelný produkt sjednat u jiné finanční instituce. GDPR tento výklad posouvá

[20] Čl. 20 odst. 1 písm. a) GDPR.
[21] Čl. 20 odst. 1 písm. b) GDPR.

i na nefinanční data, proto mají banky za to, že by mělo jít jen o identifikační, kontaktní, případně sociodemografická data, která by mohla subjektu údajů pomoci při žádosti o jiný než bankovní produkt nebo službu. O širší rozsah osobních údajů může subjekt údajů požádat v rámci práva na přístup k osobním údajům a s kopií zpracovaných osobních údajů, kterou obdrží od správce, dále volně disponovat.

Oprávnění, nikoliv povinnost banky přijmout data

GDPR nestanovuje správci údajů přímou povinnost přijímat data subjektu údajů, které si přenese od třetí strany. Jelikož v bankovním prostředí je kladen velký důkaz na bezpečnost interních systémů pracujících s daty, tak jakýkoliv přenos přes medium od třetí strany může znamenat riziko ohrožení bankovního prostředí virem, případně jiným malwarem. Právo na přenositelnost by proto mělo být zejména naplňováno při využití prostředků zákona o platebním styku. V jiných případech může být obtížné právo na přenositelnost realizovat z bezpečnostních důvodů.

Právo na přenositelnost údajů vs. mobilita v bankovním prostředí

V bankovním prostředí existuje speciální úprava přenositelnosti v oblasti platebních účtů na základě směrnice o platebních službách, která je v České republice transponována zákonem č. 370/2017 Sb., o platebním styku (dále „ZPS“)[22]. ZPS představuje v tomto duchu speciální (zvláštní) úpravu, která má při žádosti o přenesení dat k jinému poskytovateli téže služby vůči GDPR aplikační přednost.

V případě, že by byla odlišně nastavená pravidla pro přenos platebního účtu (pravidla dle GDPR vs. ZPS), dostala by se do rozporu s pravidly pro změnu banky a s pravidly služby informování o účtu (*account information service*) obsaženými v zákoně o platebním styku, které zcela dostatečně pokrývají účel institutu, tedy usnadnění sektorové mobility.

### 1.4 Právo na přístup

Subjekt údajů dle čl. 15 GDPR má právo na přístup ke svým osobním údajům. Smyslem tohoto práva je možnost zjistit, co o subjektu údajů konkrétní správce zpracovává. Subjekt údajů se dozví, jak se s údaji pracuje, které údaje banka jako správce nebo zpracovatel zpracovává, komu mohou být údaje předány a odkud jsou získávány. Toto právo je aktivováno až po podání žádosti subjektem údajů.

Forma předaných informací subjektu údajů

Dle čl. 12 GDPR je nezbytné, aby byly předávané informace podány stručně, transparentním a srozumitelným způsobem za použití jasných a jednoduchých jazykových prostředků. Z výše uvedeného vyplývá, že správce by měl informace ze systémů utřídit a poskytnout je tak, aby jim subjekt údajů rozuměl. Informace mohou být předány subjektu údajů jak ústně (pokud si to subjekt údajů vyžádá), tak písemně (fyzicky na papíře/elektronicky). Informace předávané elektronickou formou lze

[22] Srov. § 203 – 209 ZPS.

poskytnout v běžně užívaném elektronickém formátu (např. pdf, xls, csv atd.), je na uvážení banky, zda si takový formát zvolí či nikoli.

Způsoby předání informací

Každá banka si stanoví, jaký je pro ni nejbezpečnější způsob komunikace. Za případ dobré praxe lze považovat poskytnutí údajů subjektu údajů do schránky v internetovém bankovnictví.

Obsah předávaných informací

Správce má povinnost poskytnout subjektu údajů konkrétní informace o zpracování osobních údajů, tj. jaké osobní údaje správce zpracovává, z jakého zdroje pocházejí, za jakým účelem jsou zpracovány, na jak dlouho, zda byly, nebo by mohly být zpřístupněny dalším subjektům – příjemcům a další informace uvedené v čl. 15 odst. 1 GDPR. Rozsah předávaných údajů se bude v bankovním sektoru lišit v závislosti na sjednaných produktech. Cílem tohoto práva je poskytnout subjektu údajů ucelenou informaci o tom, jaké údaje banka zpracovává. Znamená to, že subjekt, který využije své právo na přístup, by měl získat představu o tom, co všechno banka o něm zpracovává s tím, že není vyloučeno vrstvení informací. Banky nejsou povinny předávat subjektu údajů informace, které mu již byly poskytnuty nebo které má k dispozici, jako například transakční údaje dostupné v internetovém bankovnictví nebo poskytované formou výpisu z účtu. Správce vždy informuje subjekt údajů o účelech zpracování a o zpracovávaných kategoriích údajů a dalších náležitostech zpracování, může to být však v obecné rovině k jednotlivým kategoriím údajů.

Jednotlivé fáze vyřízení žádosti:

a) Identifikace klienta

Po podání žádosti GDPR stanoví správci povinnost subjekt údajů identifikovat. Recitál 64 GDPR uvádí, že má správce využít všech vhodných opatření k ověření identity subjektu údajů. Správce je povinen tuto skutečnost subjektu údajů sdělit a umožnit mu, aby svoji identitu doložil určitým způsobem (např. návštěvou pobočky nebo na základě ověření elektronické identity). Pokud subjekt údajů odmítne a při komunikaci na dálku opakovaně identitu nedoloží, správce žádosti nevyhoví. Je na správci, aby posoudil, jaká míra ověření je pro něj dostatečná, není tedy vyloučeno požadovat po subjektu údajů například ověřený podpis, a to s ohledem na formu komunikace a charakter dat, která správce o subjektu údajů zpracovává, ale současně by měl žadatel mít možnost výběru z více možností identifikace tu, které pro něj představuje nejmenší překážku.

b) Potvrzení o zpracování osobních údajů

Banka má povinnost sdělit subjektu údajů, zda osobní údaje o něm zpracovává či nikoli. Po provedení potvrzení má banka povinnost bez zbytečného odkladu, nejpozději do jednoho měsíce od podání žádosti a v odůvodněných případech nejpozději do 3 měsíců, poskytnout konkrétní informace o zpracování. O odůvodněný případ se může jednat například v případě, kdy správce bude potřebovat součinnost třetí strany (karetní asociace apod.). Není vyloučeno poskytnout potvrzení o zpracování osobních údajů subjektu údajů zároveň s poskytnutím konkrétních informací o subjektu údajů, ovšem za předpokladu, že k oběma úkonům dojde bez zbytečného odkladu.

Možný postup bank při poskytování informací subjektu údajů v případě využití práva na přístup k osobním údajům (příklad dobré praxe):

- Nejprve banka poskytne obecný rámec zahrnující konkrétní informace, jako jsou identifikační a kontaktní údaje, souhrn poskytnutých produktů a další informace, které přiblíží subjektu údajů, jakými údaji správce disponuje. Cílem je poskytnout ucelenou informaci subjektu údajů o aktuálních osobních údajích, a to s ohledem na transparentnost, srozumitelnost a efektivnost poskytovaných informací.
- Správce v této fázi není povinen předávat subjektu údajů konkrétní historické údaje, pokud správce splní informační povinnost vůči subjektu údajů a subjekt ví, že jimi správce disponuje. Správce si sám určí, zda a jak osobní údaje subjektu údajů předá s ohledem na rozsah poskytnutých služeb.
- V případě, že subjekt údajů nebude spokojen s předanými daty a bude požadovat konkrétní informace vztahující se ke konkrétní službě, konkrétnímu účelu, nebo konkrétní kategorii dat, správce je povinen mu takovou informaci poskytnout. V této fázi se může jednat o historická data (klient může například žádat informace o vydaných platebních kartách za celou dobu smluvního vztahu).

Limity práva na přístup k osobním údajům

Tak jako každé právo má své limity, i právo na přístup k osobním údajům může být limitováno. Může se stát, že nebude možné subjektu údajů poskytnout veškeré informace. V tomto případě bude mít správce možnost poskytnout subjektu údajů informaci s odůvodněním, že poskytnutí osobních údajů není možné, protože by vyžadovalo neúměrně vynaložené úsilí správce[23]. Tímto nepřiměřeným úsilím by tak například mohlo být poskytování technických údajů na zálohovacích páskách, se kterými již nejsou prováděny aktivní operace, nebo by se mohlo jednat o informace, kde by zájem jiné osoby převážil nad zájmem subjektu údajů. Dále není vyloučeno odepření informace, pokud to vyžadují zvláštní právní předpisy, které mají aplikační přednost a bance ukládají určitou povinnost (typicky se může jednat o obezřetnostní požadavky vyplývající ze ZoB, AML, trestní řád, občanský soudní řád atd.).

Vzhledem k tomu, že GDPR považuje za zpracování nejen aktivní činnost s daty, ale i uchování, kterým se rozumí neaktivní zpracování, kdy správce osobní údaje ke své činnosti (plnění smlouvy) již aktivně nepoužívá, ale zákon přikazuje správci osobní údaje uchovávat ve smyslu dočasné archivace (typicky se může jednat o osobní údaje uložené u správce na různých uložištích, jako jsou zálohy, archiv, pásky, se kterými správce aktivně nenakládá), je nutné si stanovit, jaká míra detailu bude subjektu údajů předána. Pokud by totiž v praxi znamenalo poskytnout subjektu údajů veškeré informace, které správce aktivně nevyužívá jinak než k plnění zákonných povinností pro uchování údajů, musel by správce použít neúměrné úsilí k tomu, aby „oživil“ tyto historické údaje. Dokud tedy subjekt údajů důvodně nevyžaduje konkrétní historické údaje, považuje se za dostatečný rozsah poskytnutí aktivně využívaných osobních údajů.

## 2. Marketing

[23] Srov. recitál čl. 62 GDPR.

## 2.1 Přímý marketing

Banky při své činnosti využívají různé způsoby oslovení klientů. Jedním z hlavních způsobů je využití přímého marketingu, který však není v GDPR konkrétně definován, přestože GDPR s tímto pojmem pracuje a chápe takové zpracování jako zpracování prováděné z důvodu oprávněného zájmu dle čl. 6 odst. 1 písm. f) GDPR. GDPR nicméně umožňuje subjektům údajů, aby proti takovému zpracování osobních údajů vznesly námitku. V takovém případě nebudou již osobní údaje subjektu údajů pro účely tohoto marketingu zpracovávány.

### a) Oprávněný zájem v přímém marketingu

Mezi oprávněné zájmy banky lze zařadit např. situaci, kdy existuje konkrétní vztah mezi správcem osobních údajů a subjektem osobních údajů (typicky se bude jednat o vztah klienta s bankou).

Pro účely komunikace v souvislosti s přímým marketingem využívají jednotlivé banky různé komunikační kanály. Typicky se jedná o e-mail, krátké textové zprávy (SMS), internetové bankovnictví, personalizované reklamní bannery, telefon, *push* notifikaci nebo poštu. Aby byla zajištěna práva adresátů, lze u jednotlivých bank využít možnosti vznést námitku proti oprávněnému zájmu v přímém marketingu. Banky pro účely přímého marketingu mohou využívat osobní údaje, pokud existuje souvislost mezi účelem zpracování a nabídkou banky.

U reklamních bannerů, které se nachází v bankovním prostředí (internetové a mobilní bankovnictví) a které jsou neindividualizované (není prováděna segmentace ani profilování) není možné použít námitku proti zpracování, neboť při jejich přípravě nedochází ke zpracování osobních údajů subjektu údajů. Jedná se o reklamní prostor s nepersonalizovanou nabídkou, kterou lze analogicky přirovnat k plakátu v prostorách kamenné pobočky banky.

### b) Očekávatelnost marketingových nabídek ze strany klientů

Všechny banky jsou podnikatelskými subjekty, které se v rámci své podnikatelské činnosti snaží vytvářet finanční zisk. Za tímto účelem může být klient osloven bankou nabídkami produktů a služeb dané banky. Banka může nabízet i produkty dalších společností, které jsou členy dané skupiny, jako jsou spoření, pojištění, investování apod., nebo dalších služeb souvisejících s placením, přičemž musí splnit požadavky transparentnosti dle čl. 5 GDPR, tj. zejména uvést seznam členů skupiny. Banky mohou využít k oslovení klientů oprávněný zájem ve smyslu GDPR, rovněž však mohou oslovit klienty dle § 7, odst. 3 z. č. 480/2004 Sb. Banky musí dodržet odpovídající způsob informování o důvodu zaslání a způsobu odhlášení zasílání takových nabídek. Podrobněji uvádí bod 2.5.

## 2.2 Kategorizace a profilování v přímém marketingu

### a) Jednoduchá kategorizace – oprávněný zájem

V zájmu objektivity pracují banky s několika druhy kategorizace v přímém marketingu. V jednoduché kategorizaci pracují banky pouze se základními identifikačními a kontaktními údaji a tímto způsobem může být oslovena široká skupina klientů. Při zpracování dochází k třídění subjektu údajů – klientů do

určitých cílových skupin (zvolená např. dle konkrétního bydliště, věku, konkrétního produktu apod.). V rámci takové nabídky může klient od banky obdržet rovněž nabídku produktu, který je nabízen v rámci konkrétní finanční skupiny.

b) Pokročilá kategorizace neboli hrubá segmentace – oprávněný zájem

Banky pro svoji marketingovou činnost využívají pokročilou kategorizaci subjektu údajů, která umožňuje lépe zacílit na konkrétní cílovou skupinu. Typicky se může jednat o zpracování základních osobních údajů subjektu údajů odvozených z transakční historie (např. souhrn příjmů a výdajů subjektu údajů). Konkrétní nabídka může například spočívat v nabídnutí určité slevy nebo odměny konkrétnímu segmentu klientů. Banky předpokládají, že ze strany klientů je očekáván přiměřený servis, a to např. tím, že dle vybraných údajů klienta mu bude poskytnuta odpovídající marketingová nabídka. V rámci této kategorizace může být klientovi zaslána rovněž nabídka jiné entity, pokud je předmětem nabídky očekávatelná služba, tj. služba doplňující nebo rozšiřující produkty, které má klient již sjednané s bankou

c) Profilování v marketingu – souhlas

Banky při své činnosti získávají velké množství osobních údajů jednotlivých klientů. Typicky se může jednat o různé kombinace údajů a ukazatelů o klientovi, jejichž zpracování má za cíl vytvoření profilu s jeho preferencemi a očekávanými potřebami. Takový způsob zpracování slouží pro lepší pochopení chování klienta a následné trvalé držení této informace nad konkrétním klientem, nikoli konkrétní jednotlivé zacílení. Při zpracování jsou používány pokročilé statistické a analytické metody, vč. např. technologií umělé inteligence. Zpracování osobních údajů klienta tímto způsobem již vyžaduje souhlas ze strany klienta, a to jak pro samotné vytvoření profilu, tak pro jeho následné marketingové využití.

## 2.3 Předschválené úvěrové limity

Jednou z hlavních činností bank je poskytování úvěrových produktů. Nabídka předschváleného úvěrového limitu pro klienta je nezávazná a pouze ukazuje, jaké jsou klientovy případné úvěrové možnosti. Taková nabídka nemá pro klienta právní dopad. Tzv. předschválené úvěrové limity slouží rovněž ke zlepšení a zrychlení obsluhy klienta. V tomto případě, do okamžiku cíleného sdělení předschváleného limitu či z něj odvozených informací klientovi, se nejedná o marketingovou činnost v pravém slova smyslu.

## 2.4 Průzkumy spokojenosti stávajících klientů

Banky se v rámci své obchodní činnosti snaží zajistit kvalitní servis klientům a dále zlepšovat své služby. Za tímto účelem mohou oslovovat své klienty s různými průzkumy, typicky s průzkumy spokojenosti, průzkumy týkajícími se relevantnosti nabízených produktů a průzkumy souvisejícími s vývojem a přípravou nových služeb. S takovýmto průzkumem mohou banky oslovit klienty prostřednictvím e-mailu, call centra či dalším běžným komunikačním nástrojem. Z tohoto pohledu se však nejedná o marketingovou činnost v pravém smyslu slova, ale o oprávněný zájem banky na tom, aby nejen zlepšovala své služby, produkty, ale i zjišťovala zájem o konkrétní produkty apod. Pokud má komunikace formu obchodního sdělení, je nutné splnit podmínky stanovené z.č. 480/2004 Sb.

## 2.5 Obchodní sdělení vs. servisní a technické zprávy

Kromě výše uvedené legislativy musí banka při některých formách marketingového oslovení (např. e-mail, SMS) aplikovat i další legislativu, kterou je zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů. Dle této legislativy může správce šířit obchodní sdělení elektronickými prostředky, pokud v rámci takové nabídky může klient jednoduchým způsobem šíření takových obchodních sdělení odmítnout. Takové obchodní sdělení je navíc řádně označeno spojením „obchodní sdělení“ nebo „OS“, přičemž nesmí být utajován odesílatel. V takovém obchodním sdělení musí být k dispozici rovněž platná adresa, na kterou lze zaslat informaci o tom, že si adresát nepřeje další zasílání obchodních sdělení anebo uvedený jiný způsob pro odhlášení odběru dalších obchodních sdělení. Takovým obchodním sdělením v případě bank může být např. informace o novém produktu, která je zaslána na portfolio klientů, jejichž kontaktní údaje banka zpracovává v souvislosti s již vedenými produkty. Obchodním sdělením je rovněž informování klientů o úspěších banky nebo jejích produktů v soutěžích s cílem podpory značky banky nebo prodeje produktů.

Banky nicméně mohou se svými klienty komunikovat nejen marketingovým oslovením či zasláním obchodního sdělení, ale ve vybraných případech musí klienty informovat např. o právních dokumentech (změna produktových podmínek, bankovní výpis, výpis ročních poplatků atd.). Rovněž mohou informovat klienty o tom, že bude odstaveno internetové bankovnictví, které klient využívá, či že došlo k jeho odstávce v důsledku technické chyby. Stejně tak může být klient informován o tom, že některá pobočka banky je uzavřena z důvodu poruchy nebo rekonstrukce, o změně otevírací doby pobočky apod.

V takových případech se nejedná o obchodní sdělení ve smyslu zákona č. 480/2004 Sb. Jedná se o technické a servisní zprávy, které jsou banky povinny zasílat svým klientům z titulu plnění zákonné povinnosti nebo z titulu plnění smlouvy.

Pokud je však servisní zpráva spojena se zprávou, která má charakter obchodního sdělení, uplatní se na ní pravidla pro obchodní sdělení.

## 2.6 Cookies

Finanční instituce při provozování webů používají tzv. soubory cookies. Banky, které používají cookies, poskytují uživatelům webu vysvětlující informace a možnost nastavení cookies, přičemž při zpracování cookies vycházejí z principu opt-in. Tyto informace musí být dostupné na každé webové stránce či podstránce banky, včetně internetového bankovnictví, mobilních a desktopových aplikací.

Minimální informace, které banky zveřejňují na svých webových stránkách, jsou:

- Základní vysvětlení, co jsou cookies,
- Vysvětlení účelu použití cookies a jejich přínosu pro uživatele,
- Typy cookies v základních kategoriích (např. Nezbytné/Technické, Funkční/Preferenční, Statistické a marketingové) a jejich vysvětlení,
- Seznam cookies používaných na webové stránce ( alespoň v rozlišení 1st a 3rd party cookies), lhůta uchování, specifikace informací, které se do nich ukládají, popis jejich funkcionality a právní titul aplikovaný při jejich zpracování (zejm. oprávněný zájem nebo souhlas),

- Návody na změnu nastavení cookies, případně jejich odstranění.

## 3. Informační povinnost

Subjekt údajů má právo na poskytnutí informací v souladu s čl. 12-14 GDPR.

Při poskytování těchto informací je třeba zejména dbát zásad transparentní komunikace, srozumitelné formy jazyka a čitelnosti. Proto je vhodné objem poskytovaných informací vrstvit, při zachování maximální transparentnosti. Alespoň základní údaje dle čl. 13 odst. 1 GDPR, resp. čl. 14 odst. 1 GDPR, poskytne banka v první úrovni informace, podrobnější a doplňující informace (zejm. dle čl. 13 odst. 2 GDPR, resp. čl. 14 odst. 2 GDPR) lze poskytnout odkazem nebo na jiné stránce. V online prostředí je také možné použít postupné poučení o zpracování osobních údajů tam, kde jsou subjekty údajů informovány o zpracovávání jejich údajů ve více krocích (tento přístup spočívá v poskytnutí klíčových informací v krátkém oznámení s odkazem, který dále rozšíří každou část poučení na úplnou verzi).

Banky obecně plní svou informační povinnost zveřejněním Informace o zpracování osobních údajů (tzv. Informační memorandum) na svých webových stránkách. Informační memorandum musí být přehledné a srozumitelné (zejména vyhýbající se používání vysoce odborných výrazů, právních formulací), úplné v rozsahu požadavků čl. 13 a 14 GDPR a snadno dostupné. Vhodnou praxí je vytvořit na webových stránkách sekci ochrany osobních údajů přístupnou přímo z hlavní stránky. Informační memorandum obsahující všechna běžná zpracování prováděná bankou může být doplněno dílčími Informacemi o specifických nebo dočasných zpracováních (např. v souvislosti s prováděním mimořádných vládních opatření apod.).

Banky poskytují informace dle čl. 13 GDPR v okamžiku získání osobních údajů od subjektu údajů. Vhodnou praxí je poskytnutí těchto informací s pomocí Informačního memoranda, které je subjektu údajů během jednání k dispozici (v tištěné nebo elektronické formě) a má možnost si jej fyzicky odnést, nebo jej získat elektronicky (např. na svou e-mailovou adresu). Odkaz na zveřejněné informační memorandum je součástí dokumentů předávaných klientovi. Zejména v online prostředí je vhodné klientům vedle odkazu na obecné Informační memorandum poskytnout i vybrané konkrétní informace o daném zpracování.

Je dostačující provést seznámení na začátku jednání. Pokud správce získává další údaje, anebo k jiným účelům, o kterých dosud neinformoval, informuje o nich aktuálním Informačním memorandem na webových stránkách. Na podstatné změny informačního memoranda jsou klienti upozorněni. Informace není třeba subjektu údajů poskytovat v případě, že subjekt údajů tyto informace má.

Jestliže osobní údaje nebyly získány přímo od subjektu údajů, tedy je správce přebírá od jiné osoby nebo správce, může být v odůvodněných případech informační povinnost přenesena na tuto jinou osobu, zejména pokud by bylo třeba vyvinout nepřiměřené úsilí k předání těchto informací (například povinnost klienta informovat pojištěného odlišného od osoby pojistníka).

Informační povinnost se neuplatní v případě zpracování na základě zákonné povinnosti, ve veřejném zájmu (například bezpečnost), anebo na základě zvláštních zákonů – FATCA, AML, předcházení podvodům, nebo pokud by tím byl narušen účel daného zpracování osobních údajů, a zároveň jsou stanovena další pravidla na ochranu oprávněných zájmů subjektů údajů (např. mlčenlivost).

## 4. Klient právnická osoba ve vztahu k GDPR

Jak uvádí recitál č. 14 GDPR, na data klientů – právnických osob se GDPR nevztahuje. Aplikace GDPR tak měla na zpracování údajů týkajících se přímo právnických osob pouze minimální dopad. Mezi takovéto údaje patří typicky název (obchodní firma) dané korporace, právní forma, adresa sídla či jednotlivých provozoven, kontaktní údaje, pokud neobsahují osobní údaje fyzických osob (např. telefonní ústředna, e-mailová adresa ve tvaru „info@firma.cz“ atp.).

Avšak jakmile jsou v souvislosti s obsluhou klientů – právnických osob nebo v rámci plnění smluv uzavřených s dodavateli banky zpracovávány osobní údaje týkající se přímo konkrétních fyzických osob, je již třeba ustanovení GDPR na toto zpracování odpovídajícím způsobem aplikovat. Příkladem tohoto postupu může být zpracování adresy trvalého bydliště, soukromého telefonního čísla, čísla či kopie identifikačního dokladu, data narození či rodného čísla dané osoby. V těchto případech je tedy třeba nalézt odpovídající právní titul pro dané zpracování, a uplatňovat všechna další relevantní pravidla pro zpracování těchto údajů zejména s ohledem na právní titul a účel daného zpracování.

Nejčastějším případem v této situaci jsou údaje o konkrétních fyzických osobách oprávněných klienta zastupovat, ať již údaje o členech statutárních orgánů daných korporací, osob oprávněných disponovat s účty či jinak komunikovat s ohledem na plnění sjednaného produktu či služby, případně disponovat s platebními kartami. V těchto případech je nezbytné zpracovávat osobní údaje těchto osob zejména za účelem jejich řádné identifikace.

Banka tedy musí v tomto ohledu odpovídajícím způsobem plnit požadavky GDPR, zejména minimalizovat množství zpracovávaných údajů, určit doby jejich zpracování, případně odpovídajícím způsobem zajistit aktualizaci daných údajů.

Co se týče plnění informační povinnosti, to může být v těchto případech značně nepraktické, případně i nemožné. Banka by tedy měla dané subjekty údajů o jejich zpracování informovat napřímo pouze tehdy, je-li to prakticky a efektivně realizovatelné. Naopak není-li to efektivně realizovatelné (například v případech, kdy dané údaje fyzických osob shromažďuje a předává bance přímo daná právnická osoba jako data svých zaměstnanců), měla by o předání údajů danou fyzickou osobu přiměřeným způsobem informovat sama právnická osoba, která údaje bance předává (jde například o předání údajů pro účely vystavení, předání a používání služební platební karty). Zároveň je možné zvážit zahrnutí tohoto postupu do smlouvy mezi bankou a danou právnickou osobou. Stejným způsobem může být upravena i povinnost údaje o fyzických osobách přiměřeným způsobem aktualizovat.

O podrobnostech zpracování dat fyzických osob v souvislosti s obsluhou klientů – právnických osob by měla banka transparentně informovat širokou veřejnost prostřednictvím volně dostupného a veřejně deklarovaného informačního memoranda.

Specifické případy zpracování, například údaje o konečných vlastnících právnických osob zpracovávané pro účely plnění AML zákona či uschování údajů o uskutečněných obchodech pro účely plnění ZoB, je možné vykonávat na základě právního titulu plnění právní povinnosti. Toto zpracování tedy není nutné podrobněji specifikovat a subjekty údajů o tomto zpracování informovat.

Ve vztahu ke klientům právnickým osobám se v praxi objevuje řada případů, kdy tito klienti požadují předávání osobních údajů svých zaměstnanců realizované běžným platebním stykem (například výplatou mezd, proplácení nákladů v rámci služebních cest atp.) ukotvit uzavřením zpracovatelské smlouvy s bankou, ve které by právě banka figurovala v roli zpracovatele. V tomto ohledu ale platí, že banky sice při poskytování svého produktu plní pokyny zadané klientem, tedy realizují dané transakce,

nicméně nejsou v postavení zpracovatele, který by prováděl zpracování osobních údajů za správce (klienta), a to s ohledem na zvláštní právní úpravu pro poskytování daného produktu (ZPS, ZoB), V těchto případech tedy není třeba nad rámec stávajících smluvních vztahů uzavírat specifickou smlouvu či dodatek týkající se zpracování osobních údajů.

## 5. Automatizované individuální rozhodování vč. profilování

V souvislosti s nezbytností zpracování velkých objemů osobních údajů, ke kterému dochází při poskytování bankovních služeb, jsou vyvíjeny a nasazovány i nové plně automatizované postupy pro efektivnější poskytování finančních služeb a řádné plnění regulatorních povinností. S ohledem na rozsah zpracovaných osobních údajů a výpočetní náročnost takového zpracování jsou mnohdy procesy založené na automatizovaném rozhodování (včetně profilování) zaváděny primárně s cílem zajistit konzistentnost a korektnost výstupů, například v oblasti řízení rizik s cílem snížit pravděpodobnost lidské chyby nebo jako prevence podvodného jednání.

V oblasti samotné obsluhy klienta a s ní spojeným poskytováním produktů a služeb umožňuje automatizované rozhodování bankám zrychlení a celkové zefektivnění procesu obsluhy klienta, z kterého těží zejména klient. V rámci plně automatizovaného procesu může například systém bez lidského zásahu rozhodnout o žádosti o úvěr (zejména spotřebitelský), včetně stanovení rizikového profilu žadatele, dále například o stanovení investičního profilu při uzavírání investičních produktů nebo bez lidského zásahu detekovat podvodné jednání v prostředí elektronických kanálů atd.

Vstupem pro automatizované rozhodnutí mohou být jak osobní údaje poskytnuté přímo subjektem údajů (např. identifikační a kontaktní údaje), tak osobní údaje získané od třetí strany (např. z úvěrového registru), dále i odvozené nebo dovozené údaje týkající se subjektu údajů (např. rizikový profil klienta). Automatizovaná rozhodnutí mohou být činěna s využitím profilování anebo bez něho; tedy profilování lze provádět bez automatizovaného rozhodování a nejedná se nutně o propojené činnosti.

Automatizované individuální rozhodování musí být založené výhradně na automatizovaném zpracování, tedy příslušná ustanovení GDPR[24] se nevztahují na rozhodování, které je založené pouze na částečně automatizovaném zpracování. To neplatí v případě, že v některé části rozhodovacího procesu je zapojení lidského faktoru pouze formální, bez logického vlivu na výsledek rozhodování. Například tedy pokud je žádost o úvěr zpracována a vyhodnocena automatizovaně, ale rozhodnutí o poskytnutí úvěru je v odpovědnosti osoby určené vnitřními předpisy a postupy banky, která má možnost a povinnost při zohlednění všech faktorů žádosti rozhodnout odlišně od automatického vyhodnocení (doporučení), nejedná se o automatizované rozhodování.

Odpovídajícím právním titulem pro automatizované rozhodování (včetně profilování) je:

- souhlas klienta,
- uzavření nebo plnění smlouvy, jejíž smluvní stranou je subjekt údajů (klient banky),
- požadavky práva Unie nebo členského státu.

[24] Především čl. 22 GDPR.

S ohledem na možnou budoucí potřebu prokázaní zákonnosti automatizovaného rozhodování (včetně profilování), například před orgánem dozoru, nelze než doporučit správci postupovat tak, aby existenci řádného právního titulu pro zpracování byl schopen po celou dobu zpracování doložit.

Automatizované rozhodování (včetně profilování) lze provádět za kumulativního splnění následujících podmínek:

**a)** Seznámit subjekt údajů prostřednictvím dokumentu popisujícího podmínky ochrany soukromí s informací, že k automatizovanému rozhodování (včetně profilování) dochází, včetně použitého postupu a případnými důsledky takového zpracování pro subjekt údajů.

Splněním této podmínky by neměla být nepříznivě dotčena práva banky, například kdy zveřejnění detailních informací o postupu použitém při automatizovaném rozhodování může pro banku představovat jednání, které by mohlo ohrozit nebo porušit obchodní tajemství nebo ohrozit její opatření v oblasti prevence podvodů.

Je doporučeno zhodnotit, zda by informování subjektu údajů nemělo proběhnout již při zadávání osobních údajů v samotném procesu (např. informace tom, že se jedná o proces automatizovaného rozhodování, je zřetelně uvedena ve formuláři žádosti o poskytnutí úvěru, který klient vyplňuje v prostředí elektronických kanálů), než budou osobní údaje v procesu automatizovaného rozhodování zpracovány.

**b)** Správce má povinnost subjektu údajů umožnit výkon jeho práv, a to

- práva na lidský zásah ze strany správce,
- práva vyjádřit svůj názor,
- práva napadnout rozhodnutí, ke kterému došlo v důsledku automatizovaného rozhodování (včetně profilování).

Klient banky (fyzická osoba, subjekt údajů) má podle čl. 22 GDPR právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká. Typickým právním účinkem je vznik, změna nebo zánik smluvního vztahu.

Není ale povinností banky jako správce umožnit subjektu údajů nebýt předmětem automatizovaného rozhodování (včetně profilování) tím způsobem, že subjekt údajů požádá o manuální zpracování již na počátku procesu (např. žadatel o úvěr požádá výhradně o manuální posouzení žádosti). Důvodem je zachování jednotného a transparentního přístupu ke všem subjektům údajů a zajištění rychlosti a efektivity příslušného procesu. Tím nijak není dotčeno právo subjektu údajů vznést námitku proti rozhodnutí, ke kterému došlo v důsledku automatizovaného rozhodování (včetně profilování) a žádat o dodatečné manuální posouzení.

S ohledem na skutečnost, že automatizované rozhodování spočívá v systematickém a rozsáhlém vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad, má správce při přípravě takovéhoto zpracování či nového procesu povinnost

**c)** řádně posoudit vliv daného automatizovaného rozhodování na ochranu osobních údajů (tzv. DPIA)

Je plně v gesci každého správce, jaké nástroje a postupy pro zpracování osobních údajů zvolí.Při zavádění procesu automatizovaného rozhodování (a dále po celou dobu jeho existence) však musí být správce schopen prokázat, že daný způsob zpracování je s ohledem na účel zpracovaní a povahu osobních údajů přiměřený, a že stejného výsledku by nebylo možné dosáhnout pro zajištění soukromí subjektu údajů méně invazivními postupy/metodami, tedy že automatizované rozhodování je přiměřeným postupem.

S ohledem na dopad automatizovaného rozhodování na subjekt údajů je nezbytné, aby procesy, které jsou na tomto způsobu zpracování osobních údajů založeny, podléhaly pravidelné revizi a testování s cílem zajištění jejich správnosti a účinnosti. Banky mají povinnost přijmout taková technická a organizační opatření, která minimalizují rizika chyb zpracování osobních údajů v rámci automatizovaného rozhodování a zabezpečit tyto osobní údaje takovým způsobem, který zohledňuje potenciální rizika pro zájmy a práva subjektu údajů.

## SPECIFICKÁ PRAVIDLA PRO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZAMĚSTNANCŮ BANK

Pro zajištění stability banky a s ohledem na provázanost bankovního sektoru, tedy i stability tohoto segmentu národního hospodářství jako takového, je nezbytné, aby banka při své činnosti postupovala obezřetně, identifikovala a řídila rizika, kterým při své činnosti může čelit, a zavedla dostatečný vnitřní kontrolní systém.

Detailní požadavky pro práci s riziky a pro řídící a kontrolní systém banky obsahuje především ZoB a vyhláška České národní banky č. 163/2014 Sb., o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry, ve znění pozdějších předpisů, dále jen „obezřetnostní vyhláška“. Otázka personální bezpečnosti jako nedílné součásti celkového systému je upravena především v § 17 odst. 3 a 4 obezřetnostní vyhlášky. Banka je podle těchto ustanovení především povinna stanovit zásady řízení lidských zdrojů, a to i zásady pro výběr zaměstnanců, včetně nastavení a uplatňování konkrétních pravidel pro ověřování důvěryhodnosti zaměstnanců a členů orgánů.

Požadavek na důvěryhodnost zaměstnanců je formulován rovněž dalšími předpisy, které upravují některé bankou poskytované produkty. Jedná se například o § 72 ZSÚ či § 14a ZPKT, které oba shodně požadují, aby banka zajistila, že její zaměstnanci, kteří se budou podílet na poskytování daného produktu, jsou důvěryhodní.

Banka je tedy na základě sektorové regulace a předmětu své činnosti povinna stanovit pravidla pro ověřování důvěryhodnosti svých zaměstnanců, a to nejen pro doložení splnění svých právních povinností, ale i pro ochranu svých oprávněných zájmů, jako je především ochrana majetku banky i jejích klientů.

Pro ochranu výše uvedených zájmů je nezbytné ověřovat důvěryhodnost jak při výběrovém řízení na obsazení pracovní pozice, tak v průběhu trvání pracovněprávního vztahu. U některých pracovních pozic je důkladné posouzení bezúhonnosti uchazeče přímo uloženo zvláštním právním předpisem[25], u jiných to pak lze s ohledem na konkrétní okolnosti provést pro zajištění oprávněných zájmů banky a dalších osob. Ve druhém případě záleží na konkrétní bance, jak vyhodnotí riziko spojené s danou pracovní pozicí a jaké osobní údaje bude považovat za nezbytné pro ověření důvěryhodnosti daného zaměstnance či uchazeče o zaměstnání. Takovéto posouzení bude zároveň tzv. balančním testem ve smyslu čl. 6 GDPR, při kterém banka zváží zájmy své a svých klientů a na druhé straně práva dotčených osob na ochranu soukromí.

Mezi skutečnosti, které je obvykle nutno při hodnocení míry rizika pracovní pozice, resp. při provádění balančního testu, zhodnotit, patří zejména tyto:

- předmět pracovní činnosti zaměstnance a jeho souvislost s dalšími interními procesy banky,
- rozsah přístupu k důvěrným informacím,
- možnost přímo či nepřímo přispět k neoprávněné manipulaci s majetkem banky a jejích klientů,
- kvalita a funkčnost automaticky prováděných kontrol činnosti zaměstnance,
- síla a parametry dalších vnitřních kontrol banky.

[25] Např. u fyzických osob podílejících se na poskytování spotřebitelského úvěru, u kterých je povinnost ověřit jejich důvěryhodnost upravena v § 72 ZSÚ.

Na základě zhodnocení rizika a provedení balančního testu nastavených procesů lze v přiměřeném rozsahu zpracovávat osobní údaje za účelem ověření důvěryhodnosti zaměstnance či uchazeče o zaměstnání. Právním titulem k takovému zpracování je oprávněný zájem dle čl. 6 odst. 1 písm. f) GDPR.

Osobní údaje lze získat v zásadě ze tří zdrojů: od zaměstnance či uchazeče o zaměstnání, z veřejných zdrojů (živnostenský rejstřík, insolvenční rejstřík, centrální evidence exekucí, další veřejně přístupné údaje) a od dalších správců údajů, kteří mohou potvrdit správnost informací uvedených zaměstnancem či uchazečem o zaměstnání a mají k tomu dostatečný právní titul, jako je předchozí zaměstnavatel, škola či certifikační autorita, jejímž certifikátem má daný zaměstnanec nebo uchazeč o zaměstnání disponovat. Právní titul oprávněného zájmu lze obecně využít pro shromáždění a další zpracování osobních údajů ze všech typů zdrojů. Souhlasu zaměstnance bude pro poskytnutí informací potřeba jen tehdy, pokud tak výslovně stanoví zvláštní právní úprava, jako např. § 314 odst. 2 zákona č. 262/2006 Sb., zákoník práce.

## VZTAH K DOZOROVÉMU ÚŘADU

### Porušení zabezpečení dat (*data breaches*)

Banky mají v oblasti informační bezpečnosti nastavenu řadu procesů a zavedeny nástroje pro předcházení, identifikaci a řešení bezpečnostních incidentů. GDPR, stejně jako některé další předpisy[26], bankám ukládá, aby určitý druh bezpečnostních incidentů oznamovaly ÚOOÚ (při zohlednění výjimky dle § 12 zákona č. 110/2019 Sb.), a v některých případech i přímo dotčeným osobám.

- ✓ Pro posouzení, zda konkrétní bezpečnostní incident odpovídá definici porušení zabezpečení osobních údajů dle GDPR[27], je nutné zohlednit, zda se týkal osobních údajů zpracovávaných bankou, ať už se jedná o údaje klientů, zaměstnanců či dalších osob, a zda skutečně došlo k porušení zabezpečení údajů.

Porušením ve smyslu výše uvedené definice není bezpečnostní událost, která může způsobit narušení bezpečnosti zpracovávaných osobních údajů, ale pouze skutečný incident, v jehož důsledku došlo k uvedeným následkům, tzn. k zásahu do důvěrnosti, integrity či dostupnosti osobních údajů. Porušením zabezpečení by tak nebyla situace, kdy by byla identifikována chyba v zabezpečení, která by pouze potenciálně mohla vést k protiprávnímu zpřístupnění dat. O porušení by se jednalo, pokud by např. došlo ke skutečnému zneužití slabě chráněného mobilního telefonu zaměstnance, které by mělo výše uvedené následky.

V případech, kdy došlo k předání osobních údajů jiné osobě, než oprávněnému adresátovi (např. zaslání výpisu z účtu), je rozhodující, zda je doložitelné, že chybnou adresu bance sdělil sám oprávněný adresát (např. neaktualizoval korespondenční adresu, tel. číslo). V takovém případě se o případ porušení zabezpečení nejedná.

[26] ZPS, zákon o kybernetické bezpečnosti.
[27] Čl. 4 odst. 12 GDPR.

- ✓ Čl. 33 odst. 1 GDPR spojuje počátek běhu lhůty pro ohlášení případu porušení zabezpečení osobních údajů s okamžikem, kdy se o porušení dozví správce, tedy banka.

Porušení zabezpečení dat, resp. podezření na bezpečnostní incident, může v praxi zjistit velký okruh zaměstnanců – pracovník na pobočce (bankéř), zaměstnanec v marketingovém útvaru v centrále, ostraha, pracovník IT security, Compliance, Anti-fraud, archiv, atd. Typově se bude jednat o značně odlišné případy (ztracená či odcizená dokumentace, násilný vstup do archivu, omylem zaslané informace neoprávněnému příjemci, externí zásah do systému, technická chyba aplikace atd.), stejně jako bude odlišná kvalifikace zaměstnance k posouzení toho, zda se jedná či nejedná o incident, který má eskalovat dále.

Za klíčové pro splnění povinností uložených bankám v této oblasti GDPR je tudíž možné označit určení osoby či osob odpovědných za posuzování bezpečnostních incidentů a nastavení celkového procesu tak, aby každý zaměstnanec, který může zjistit indicie či událost nasvědčující porušení zabezpečení údajů, věděl, na koho se s touto informací obrátit.

Začátek lhůty by tak měl být dle dikce i účelu daného ustanovení GDPR spojen s okamžikem, kdy určený zaměstnanec má či by měl mít dostatek informací ke konstatování toho, že k porušení zabezpečení osobních údajů s velkou mírou pravděpodobnosti došlo. Neznamená to ale, že začátek lhůty běží až od chvíle, kdy správce či zpracovatel, resp. pověřený zaměstnanec, má k dispozici veškeré informace o incidentu. Zjišťování všech informací má být předmětem šetření. Klíčové pro počátek běhu lhůty tedy je prvotní posouzení, zda k bezpečnostnímu incidentu s velkou mírou pravděpodobnosti došlo. Pokud správce dospěje k závěru, že tomu tak skutečně být mohlo, v tomto okamžiku začíná běžet lhůta 72 hodin pro ohlášení případu porušení zabezpečení osobních údajů. Složitost konkrétního případu pak může mít vliv na to, zdali ohlášení bude podáno v dané lhůtě, nebo později. Analogicky lze počátek běhu lhůty pro ohlášení ÚOOÚ dovodit i pro případy porušení identifikované zpracovatelem pověřeným ke zpracování bankou, tj. od okamžiku, kdy zpracovatel měl nebo měl mít dostatek informací ke konstatování toho, že k porušení zabezpečení osobních údajů s velkou mírou pravděpodobnosti došlo.

Obdobně banka postupuje v případě povinnosti oznámení incidentu dotčeným subjektům údajů, které musí učinit bez zbytečného odkladu.

- ✓ Posuzování bezpečnostního incidentu

Z dikce čl. 33 a 34 GDPR vyplývá, že v případě zjištění incidentu jsou podle jeho závažnosti, resp. míry rizika pro práva a svobody fyzických osob, možné tři postupy:

a) Incident pravděpodobně nepředstavuje riziko pro práva a svobody dotčených osob. Proto nemusí být ani ohlášen dozorovému úřadu, ani oznámen dotčeným osobám. I tyto incidenty je však nutné interně evidovat.
b) Incident pravděpodobně představuje riziko pro práva a svobody dotčených osob, nicméně nejedná se o vysoké riziko. Předpokladem ohlášení je to, že reálně hrozí nebo vznikne újma. Takovýto incident musí být ohlášen dozorovému úřadu. Samotné selhání bezpečnostního prvku bez výše uvedeného důsledku, stejně jako neúspěšný útok, nejsou předmětem ohlašovací povinnosti dle GDPR.

c) Incident pravděpodobně představuje vysoké riziko pro práva a svobody dotčených osob. O incidentu tohoto druhu je nutno vyrozumět jak dozorový úřad, tak dotčené osoby, pokud se neuplatní některá z výjimek dle čl. 34 odst. 3 GDPR.

Jako rozhodující pro posouzení rizikovosti je nutno zohlednit zejména druh a závažnost rizika pro dotčenou osobu, typ porušení zabezpečení osobních údajů, povahu, citlivost a rozsah údajů, kategorie dotčených osob, snadnost identifikace osob, jejichž data byla porušením dotčena, neoprávněného příjemce, a počet dotčených osob. Za případ dobré praxe lze označit zpracování interní metodiky popisující, jakým způsobem a podle jakých kritérií jsou jednotlivé případy porušení zabezpečení osobních údajů posuzovány[28]. Posouzení však vždy musí být individuální, nikoliv mechanické, zohledňující kontext a pravděpodobné dopady daného případu.

[28] Vhodným standardem jsou doporučení ENISA dostupná na https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches

## SDÍLENÍ OSOBNÍCH ÚDAJŮ

### 1. Klientské registry

Za účelem ověření bonity a úvěruschopnosti žadatele o úvěr mezi sebou banky sdílejí potřebné osobní údaje o fyzických osobách, žadatelích o úvěr. Sdílení může probíhat i s dalšími nebankovními subjekty, které sledují stejný účel (ověření důvěryhodnosti a platební morálky žadatelů o službu). Ke sdílení osobních údajů za výše popsaným účelem dochází prostřednictvím tzv. klientských registrů, které mohou banky využívat.

Legislativní rámec pro fungování klientských registrů je v ČR vymezen souběžnou existencí několika právních předpisů (ZoB, ZSÚ, zákon o ochraně spotřebitele), které upravují základní pravidla odlišným způsobem a jejichž vzájemný vztah není jednoznačně určitelný.

V důsledku tohoto roztříštěného a nejednotného právního rámce je fungování jednotlivých klientských registrů, které banky využívají za účelem ověření bonity a úvěruschopnosti žadatele (fyzické osoby) o úvěr, rozdílné a je založeno na rozdílných zákonných titulech.

#### a) Bankovní a Nebankovní registry klientských informací

BRKI – Bankovní registr klientských informací

Zákonným titulem pro zpracování osobních údajů a informací o všech relevantních bankovních produktech získaných bankou z registru BRKI je plnění právní povinnosti banky - správce - založené především na požadavcích ZoB a ZSÚ.

NRKI – Nebankovní registr klientských informací

Zákonným titulem pro zpracování osobních údajů získaných bankou z registru NRKI je plnění právní povinnosti uživatele registru – banky – správce - vyplývající zejména ze zákona o spotřebitelském úvěru, ale i dalších předpisů upravujících povinnost ověřit úvěruschopnost žadatele o finanční produkt a bránit jeho předlužení.

Pro zpracování osobních údajů, které souvisejí s poskytnutím jiných než spotřebitelských úvěrů fyzickým osobám, je zákonným titulem oprávněný zájem uživatelů registru.

Sdílení údajů mezi registry BRKI a NRKI

Z pohledu bank je zákonným titulem plnění právní povinnosti správce, vyplývající především ze ZoB a ZSÚ.

#### b) Registry Solus

Negativní registry Solus (Registr FO a Registr IČ)

Zákonným titulem pro zpracování osobních údajů získaných bankou z negativních registrů Solus je v souladu se zákonem o ochraně spotřebitele oprávněný zájem banky - správce.[29]

[29] § 20za odst. 1 zákona o ochraně spotřebitele.

Pozitivní registr Solus

Zákonným titulem pro zpracování osobních údajů získaných bankou z pozitivního registru Solus je v souladu se zákonem o ochraně spotřebitele souhlas subjektu údajů.[30]

Detailní pravidla jsou upravena v dokumentech, jejichž prostřednictvím jednotlivé klientské registry plní svou informační povinnost. Za dobrou praxi lze označit postup, kdy banky informují své klienty a žadatele o úvěrový produkt alespoň rámcovým způsobem o zpracování jejich údajů v klientských registrech (např. formou informačního memoranda), a ohledně detailů odkazují na informační dokumenty příslušných registrů.

## 2. Spolupráce v oblasti obchodního zastoupení (zprostředkování)

Finanční instituce napříč finančním trhem spolupracují jednak proto, aby mohly oslovit co nejširší skupinu potenciálních klientů, a jednak proto, aby svým klientům nabídly co nejkompletnější produktovou nabídku.

V souvislosti se spoluprací v oblasti obchodního zastoupení mohou nastat následující dva základní scénáře:

a) Obchodní zástupci bank

Jedná se o situace, kdy produkty bank distribuují jejich obchodní zástupci. Těmi mohou být jak fyzické, tak právnické osoby (typicky makléřské společnosti).

b) Banka v postavení obchodního zástupce

Jedná se o situace, kdy banka distribuuje produkty partnerské společnosti (typicky např. produkty pojistné, doplňkového penzijního spoření, stavebního spoření, investiční atd.).

### Distribuční vztahy v kontextu zásad zpracování osobních údajů

V obou výše uvedených případech je správcem osobních údajů primárně subjekt, který poskytuje daný produkt (v případě podle písm. a) tedy banka, podle písm. b) pojišťovna, penzijní společnost, stavební spořitelna, investiční společnost atd.) a obchodní zástupce, jedná-li jménem správce, je v postavení zpracovatele osobních údajů.

Paralelně však obchodní zástupce může být vůči stejným osobním údajům v postavení správce osobních údajů, a to zejména v případě, že zpracování mají odlišný účel a předmětné osobní údaje:

a) je povinen zpracovávat, aby splnil svou zákonnou povinnost vyplývající zejména z regulace distribuce finančních produktů,

b) je oprávněn zpracovávat pro vlastní účely, pokud mu k tomu klient udělil souhlas (např. pro marketingové účely),

c) je povinen zpracovávat pro účely plnění smlouvy s klientem,

[30] § 20za odst. 6 zákona o ochraně spotřebitele.

d) zpracovává na základě svého oprávněného zájmu (např. pro účely přímého marketingu na základě oprávněného zájmu).

Jinými slovy, obchodní zástupce je v pozici zpracovatele osobních údajů vždy, pokud činí úkony jménem finanční instituce (typicky úkony jako jednání o smlouvě, uzavření smlouvy, klientský servis v souvislosti se smlouvou) a v ostatních případech (např. v souvislosti s plněním povinností, které mu jako zprostředkovateli spotřebitelského úvěru vyplývají ze ZSÚ), je v pozici správce osobních údajů.

V některých případech mohou být dokonce oba subjekty v rámci obchodního zastoupení správci osobních údajů. Takovou situací je např. činnost tzv. „tipařů“, což jsou osoby, které samy nejsou oprávněny zprostředkovávat finanční produkty, nýbrž pouze mohou zjistit zájem konkrétního člověka o finanční produkt a předat tuto informaci a jeho kontaktní údaje jím vybrané bance. K předání údajů je v tomto případě nezbytný explicitní a jmenovitý (tj. označující konkrétní banku nebo banky či jiné správce, kterým mohou být údaje předány) souhlas zájemce, za jehož získání a doložitelnost odpovídá zprostředkovatel.

V případě tzv. doplňkových služeb k produktům banky, jako jsou například asistenční služby k platebním kartám, může být banka a poskytovatel služby ve vztahu společných správců v rozsahu zpracování údajů klienta prokazujících nárok na čerpání služby. Pokud poskytovatel samotnou službu poskytuje pod vlastním jménem a na vlastní odpovědnost, je v této části samostatným správcem údajů uživatele služby.

Konkrétnímu typu vzájemné spolupráce by pak mělo odpovídat i smluvní ošetření zpracování osobních údajů. Kromě obvyklé smlouvy o zpracování osobních údajů mezi správcem a zpracovatelem dle GDPR, může v některých případech přicházet v úvahu i smlouva o zpracování osobních údajů mezi dvěma správci, popř. společnými správci, nebo kombinace obou typů smluv.

3. Sdílení dat v rámci finanční skupiny (konsolidovaného celku)

   Banky mohou sdílet osobní údaje s třetími osobami v rámci své finanční skupiny (tedy s mateřskými, sesterskými nebo dceřinými společnostmi, a to i v jiných zemích), pouze pokud k tomu mají některý z právních titulů dle Nařízení GDPR, čl. 6. Obecné zásady pro předávání osobních údajů v rámci skupiny podniků do podniku nacházejícího se ve třetí zemi zůstávají nedotčeny.

   Recitál 48 GDPR uvádí, že správci mohou mít oprávněný zájem na předání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely, včetně zpracování osobních údajů zákazníků či zaměstnanců.

   Současně banky musí respektovat požadavek na ochranu bankovního tajemství. Podmínky, za nichž mohou banky data sdílet, stanovuje zákon o bankách (ZoB). Zejména dle §38b mohou banky předávat data pro účely plnění pravidel obezřetného podnikání. Takovým účelem je například řízení kreditních či jiných rizik, prevence podvodů, apod. Sdílení dat v nezbytném rozsahu pro tyto účely tak lze považovat za oprávněný zájem podle GDPR.

   Sdílení dat pro marketingové účely je zpravidla založeno na souhlasu klientů.

## 4. Bankovní identita

Banky a pobočky zahraničních bank jsou od 1. 1. 2021 oprávněny poskytovat identifikační služby ve smyslu § 1 odst. 4 písm. c) ZoB a vystupují tak v roli tzv. poskytovatelů identity (identity provider, dále jen „IdP“). Od 1. 1. 2021 je tak umožněno poskytování služeb tzv. elektronické bankovní identity (dále jen „EBI“) a souvisejících služeb různým poskytovatelům online služeb (service providerům, dále jen „SeP“).

Pokud banky poskytují služby EBI, jsou v postavení samostatných správců osobních údajů zapojeny:

a) banky v roli IdP, potvrzující totožnost klientů bank a zákazníků SeP (dále jen „klienti“ nebo jednotlivě „klient“) na základě identifikace klienta v rozhraní IdP prostřednictvím EBI;
b) poskytovatelé online služeb v roli SeP, vůči kterým klient s využitím EBI prokazuje svou totožnost; a
c) poskytovatel identifikačních služeb podle § 38aa ZoB, který na základě pokynu Subjektu údajů přenáší osobní údaje nezbytné k identifikaci klienta od IdP ke zvolenému SeP; poskytovatelem identifikačních služeb podle § 38aa ZoB je v systému EBI v tuto chvíli společnost Bankovní identita, a.s., IČO: 095 13 817, se sídlem: Smrčkova 2485/4, Libeň, 180 00 Praha 8 (dále jen „BankID“).

EBI a související služby mohou být ze strany bank v pozici IdP poskytovány ve dvojím režimu, a sice:

a) prostřednictvím kvalifikovaného systému pro elektronickou identifikaci podle § 2 zákona č. 250/2017 Sb., o elektronické identifikaci (dále jen „ZoEI“);
b) mimo rámec kvalifikovaného systému pro elektronickou identifikaci podle § 38ab odst. 1 ZoB.

V rámci kvalifikovaného systému pro elektronickou identifikaci poskytují banky EBI prostřednictvím Národního bodu pro identifikaci a autentizaci ve smyslu § 20 ZoEI (dále jen „NIA“). V rámci NIA je EBI dostupná pro veřejnoprávní SeP, tedy státní orgány a územní samosprávné celky. Tento režim využití EBI tak umožňuje ji využít např. pro přístup klientů k Portálu občana (portal.gov.cz), portálu České správy sociálního zabezpečení a dalším portálům eGovernmentu. Některé banky umožňují svým klientům používat EBI v tomto režimu již od 1. 1. 2021. Na poskytování EBI a souvisejících služeb v tomto režimu se BankID žádným způsobem nepodílí a služby EBI jsou ze strany bank poskytovány napřímo prostřednictvím NIA.

Mimo rámec kvalifikovaného systému pak mohou banky poskytovat na smluvní bázi identifikační služby soukromoprávním SeP, jako jsou telefonní operátoři, poskytovatelé energií, pojišťovny a další komerční subjekty. Za tímto účelem mohou banky poskytovat SeP své služby buď přímo nebo prostřednictvím poskytovatele identifikačních služeb ve smyslu § 38aa ZoB.

Služby EBI spočívají v potvrzování totožnosti fyzických osob a poskytování vybraných údajů o fyzických osobách ze strany IdP (bank) vůči SeP. Služby EBI jsou přitom ve vztahu ke konkrétnímu klientovi banky poskytovány vždy na jeho pokyn a s jeho souhlasem ve vztahu k bankovnímu tajemství dle zákona o bankách. Souhlas je v tomto případě udělován k předání osobních údajů klienta od IdP k SeP.

Poskytnutí služby EBI tak iniciuje vždy klient tím, že v prostředí konkrétního SeP zvolí, že pro své ztotožnění chce využít služby BankID. Následně zvolí v prostředí BankID, pomocí kterého konkrétního IdP (konkrétní banky) chce ztotožnění provést. V prostředí banky potvrdí rozsah údajů předávaných SeP a tyto údaje jsou od IdP (banky) přeneseny ze strany BankID směrem k SeP.

Právním základem zpracování v rámci poskytování služeb EBI na straně bank je plnění smlouvy s klientem ve smyslu čl. 6 odst. 1 písm. b) GDPR, konkrétně smlouvy, na základě které jsou klientovi

poskytovány služby a produkty banky a jejichž součástí je rovněž vydávání prostředků pro elektronickou identifikaci a poskytování identifikačních služeb. Osobní údaje zpracovávané na základě plnění smlouvy budou ze strany bank zpravidla uchovávány po dobu trvání příslušné smlouvy, nebude-li další zpracování založené na jiném právním titulu vyžadovat další uchování (např. z důvodu plnění právních povinností).

Právním základem zpracování na straně BankID je oprávněný zájem správce ve smyslu čl. 6 odst. 1 písm. f) GDPR, spočívající v:

a) poskytování identifikačních služeb tak, aby BankID mohla plnit svou integrační úlohu v systému EBI a zajišťovat poskytování služeb EBI a předávání údajů klienta od IdP k SeP;
b) ochraně právních nároků tak, aby byla BankID schopna vést možnou budoucí obhajobu právních nároků vznesených vůči BankID ze strany SeP nebo třetích osob.

Zpracování lze založit na oprávněném zájmu BankID, neboť BankID uchovává osobní údaje po velmi krátkou dobu a následně tyto pseudonymizuje, zpracování tak nemá významný negativní dopad na zájem klientů jako subjektů údajů. Naopak, zpracování v souvislosti s poskytnutím služby EBI dává klientovi přiměřené záruky, že nedojde k neoprávněnému přístupu k uživatelskému účtu ve službě SeP (včetně neoprávněného přístupu k osobním údajům uloženým ve službě SeP) ze strany jiné osoby vydávající se vůči SeP za klienta. Rovněž je zpracování osobních údajů v zájmu všech zúčastněných subjektů, tedy BankID, IdP, SeP i klientů, jakož i v zájmu celého tržního ekosystému, neboť zapojení BankID umožnuje propojení všech zúčastněných IdP a SeP, a tedy efektivní poskytování služeb EBI napříč trhem v měřítku zamýšleném zákonodárcem.

V rámci předání údajů poskytování IdP konkrétnímu SeP zpracovává BankID údaje v rozsahu dle požadované služby EBI pouze dobu technicky nezbytnou k realizaci daného přenosu. Následně jsou za účelem prokazatelnosti poskytnutí služby uchovány pouze pseudonymizované údaje o konkrétní identifikační transakci. Ve vztahu k účelu ochrany právních nároků BankID bude doba zpracování dána délkou trvání promlčecí lhůty (tedy 15 let).

Právní základ zpracování na straně SeP bude vždy záležet na konkrétním vztahu SeP s klientem a na tom, pro jaký účel klient vůči SeP službu EBI iniciuje. V praxi se může jednat o plnění smlouvy (např. ověření totožnosti klienta před uzavřením smlouvy se SeP), plnění právní povinnosti (např. identifikace klienta ve smyslu § 7 AML zákona) či oprávněný zájem správce.