Kódex správania pre spracúvanie osobných údajov v bankovom sektore

OBSAH

Preambula

(1) Spracúvanie osobných údajov bankami je nevyhnutnou súčasťou poskytovania bankových služieb, plnenia zmluvných a zákonných povinností alebo ochrany oprávnených záujmov bánk. Vzťah dôvery a transparentnosti medzi klientom a bankou je základom kontrahovania v bankovom sektore.

(2) Bankový sektor patrí medzi najregulovanejšie sektory a predpisy na ochranu osobných údajov môžu v tomto špecificky regulovanom prostredí spôsobovať praktické a teoretické interpretačné právne problémy. Zároveň, nie všetky právne predpisy vzťahujúce sa na bankový sektor sú vzájomne prepojené a prispôsobené. Je prínosom pre banky, ich klientov a Úrad na ochranu osobných údajov, ak budú tieto interpretačné problémy vysvetlené, pričom článok 40 ods. 1 GDPR predpokladá, že Kódex má prispieť k správnemu uplatňovaniu GDPR berúc do úvahy osobitné črty bankového sektora.

(3) Tento Kódex bol vypracovaný už s prihliadnutím na nový režim ochrany osobných údajov v EÚ a reflektuje povinnosti bánk podľa GDPR a zároveň podľa kľúčových národných predpisov vzťahujúcich sa na oblasť bankovníctva. Pri skúmaní obsahu Kódexu je nevyhnutné vychádzať zo zámeru umožniť jednotlivým bankám, na ktoré sa tento Kódex vzťahuje, určitú voľnosť pri zabezpečovaní výkladu a súladu s GDPR zohľadňujúc osobitné okolnosti spracúvania osobných údajov. Kódex nepredstavuje dodatočnú reguláciu bánk nad rámec existujúcich právnych predpisov ani technologický štandard bankového sektora.

(4) Tento Kódex neslúži ako technologický štandard bánk v oblasti bezpečnosti osobných údajov. Zmyslom Kódexu v oblasti bezpečnosti osobných údajov je vysvetlenie prístupu bánk k bezpečnosti osobných údajov z pohľadu iných technologickejšie zameraných predpisov a noriem. Konkrétny prístup k zabezpečeniu celkovej ochrany osobných údajov je podľa GDPR individuálnou záležitosťou banky za podmienky, že táto ochrana je primeraná.

(5) Týmto Kódexom je pre dotknuté osoby zaručená doplnková možnosť obrátiť sa na kontaktné miesto Slovenskej bankovej asociácie nad rámec predpokladaný GDPR. Slovenská banková asociácia môže poskytovať dotknutým osobám všeobecný výklad tohto Kódexu, ktorý však nenahrádza žiadnym spôsobom povinnosti bánk podľa GDPR ale poskytuje len doplnkovú právne nezáväzné konzultáciu alebo názor Slovenskej bankovej asociácie.

(6) Tento Kódex predstavuje národný kódex správania vzťahujúci sa na slovenský bankový sektor.

(7) V súlade s článkom 24 ods. 3 GDPR sa môže dodržiavanie Kódexu použiť ako prvok na preukázanie splnenia povinností bánk vyplývajúcich z GDPR. Zároveň, pri rozhodovaní o uložení pokuty Úradom na ochranu osobných údajov a jej výške sa majú podľa č. 83 ods. 2 GDPR v každom jednotlivom prípade náležite zohľadniť viaceré skutočnosti, medzi ktoré patrí aj dodržiavanie Kódexu.

VZHĽADOM NA VYŠŠIE UVEDENÉ SA SLOVENSKÁ BANKOVÁ ASOCIÁCIA ROZHODLA PRIJAŤ TENTO KÓDEX V NASLEDOVNOM ZNENÍ:

1 Pôsobnosť a aplikácia Kódexu

1.1 Pôsobnosť Kódexu

1.1.1 Tento Kódex sa vzťahuje na všetky banky a pobočky zahraničných bánk, ktoré pristúpili k dodržiavaniu Kódexu v súlade s bodom 1.2 nižšie. Tento Kódex sa nevzťahuje na také spracúvanie osobných údajov bankami, na ktoré sa nevzťahuje slovenské právo ani na spracovateľské činnosti bánk vykonávané v iných členských štátoch ako je Slovenská republika s poukazom na to, že tento Kódex predstavuje národný kódex správania podľa článku 40 ods. 7 GDPR.

1.1.2 Tento Kódex sa vzťahuje na spracúvanie osobných údajov vykonávané bankami len vo vzťahu k/ku:

a. klientom bánk, ktorí sú fyzickými osobami;
b. fyzickým osobám, ktoré sú oprávnené zastupovať klientov bánk, ktorými sú právnické a fyzické osoby;
c. niektorým ďalším fyzickým osobám, ktorých osobné údaje sú spracúvané v priamej súvislosti s vykonávaním bankových činností podľa § 2 ods. 2 Zákona o bankách, pričom ide najmä o osoby, ktoré vstupujú do záväzkových vzťahov s bankou alebo záväzkových vzťahov súvisiacich s bankovými obchodmi (napríklad predávajúci nehnuteľnosti nadobúdanej z hypotekárneho úveru, konečný užívateľ výhod a pod.)

Pojem klient v rámci Kódexu zahŕňa všetky osoby alebo skupiny osôb uvedené v písm. a, b, c vyššie.

1.1.3 Tento Kódex sa nevzťahuje na spracúvanie osobných údajov vykonávané bankami vo vzťahu k iným osobám ako sú uvedené vyššie. Pre odstránenie pochybností, tento Kódex sa nevzťahuje na spracúvanie osobných údajov vykonávané bankami najmä, avšak nie len, vo vzťahu k dotknutým osobám, ktorými sú zamestnanci bánk, členovia orgánov bánk, profesionálni poradcovia bánk, finanční agenti bánk, dodávatelia tovarov / služieb pre banky a zamestnanci týchto osôb.

1.1.4 Tento Kódex sa takisto nevzťahuje na také spracúvanie osobných údajov vykonávané bankami, na ktoré sa nevzťahuje GDPR ani Zákon o ochrane osobných údajov.

1.2 Pristúpenie ku Kódexu

1.2.1 Pristúpenie ku Kódexu je dobrovoľné a nie je ním podmienené členstvo banky v Slovenskej bankovej asociácii. Členstvo banky v Slovenskej bankovej asociácii nie je podmienkou pristúpenia ku Kódexu. Pristúpenie ku Kódexu prebieha prostredníctvom písomného vyhlásenia banky prostredníctvom jednotného formulára o pristúpení ku Kódexu (ďalej len „**Vyhlásenie o pristúpení ku Kódexu**“) doručeného na adresu Slovenskej bankovej asociácie uvedenú v jednotnom formulári. Vo Vyhlásení o pristúpení ku Kódexu banka čestne a verejne vyhlási, že sa dobrovoľne zaväzuje dodržiavať Kódex pri spracúvaní osobných údajov na ktoré sa vzťahuje tento Kódex.

1.2.2 Slovenská banková asociácia pripraví jednotný formulár pre banky, ktorý bude slúžiť ako vzor pre Vyhlásenie o pristúpení ku Kódexu a zverejní tento jednotný formulár na svojom webom sídle. Banka, ktorá má záujem pristúpiť ku Kódexu je povinná použiť jednotný formulár pripravený zo strany Slovenskej bankovej asociácie a nesmie vo Vyhlásení o pristúpení ku Kódexu uvádzať akékoľvek výhrady, výluky, obmedzenia alebo podmienky pristúpenia ku Kódexu, právnej záväznosti Kódexu alebo aplikácie jednotlivých častí Kódexu na konkrétnu banku. Pristupujúca banka nesmie vo Vyhlásení o pristúpení ku Kódexu uvádzať žiadne doplňujúce informácie, ktoré by mohli

spôsobovať pochybnosti o úmysle banky riadiť sa Kódexom. V prípade, ak Vyhlásenie o pristúpení ku Kódexu a/alebo banka pristupujúca ku Kódexu nespĺňajú akékoľvek požiadavky podľa tohto Kódexu, je Slovenská banková asociácia oprávnená zamietnuť pristúpenie konkrétnej banky ku Kódexu, pričom v takom prípade nie je pristúpenie banky ku Kódexu platné ani účinné. Banka je vo Vyhlásení o pristúpení ku Kódexu povinná stanoviť dátum účinnosti pristúpenia ku Kódexu, ktorý nesmie byť skorší ako dátum doručenia Vyhlásenia o pristúpení ku Kódexu Slovenskej bankovej asociácii.

1.2.3 Slovenská banková asociácia na svojom webovom sídle vedie a aktualizuje zoznam bánk, ktoré dodržiavajú Kódex na základe mechanizmu pristúpenia ku Kódexu, pričom zmeny v tomto zozname nie sú považované za zmeny Kódexu a nepodliehajú schvaľovaniu zmeny Kódexu zo strany Úradu na ochranu osobných údajov.

1.3 Právna záväznosť Kódexu

1.3.1 Rozhodnutie Úradu na ochranu osobných údajov o schválení tohto Kódexu znamená, že tento Kódex je v súlade s požiadavkami GDPR. Vyhlásenie o pristúpení ku Kódexu v súlade s týmto Kódexom znamená, že banka je povinná ku dňu účinnosti pristúpenia dodržiavať Kódex. Kódex má podľa článku 40 ods. 1 GDPR prispieť k správnemu aplikovaniu GDPR berúc do úvahy osobitné črty podnikania v bankovom sektore.

1.3.2 Ak by sa ukázalo, že existuje rozpor medzi usmerneniami a rozhodnutiami dozorných orgánov a súdov na jednej strane a ustanoveniami tohto Kódexu na druhej strane, banky sú oprávnené riadiť sa ustanoveniami tohto Kódexu až do momentu, kým Úrad na ochranu osobných údajov nerozhodne voči konkrétnej banke inak podľa § 102 ods. 1 písm. a) alebo b) Zákona o ochrane osobných údajov alebo až do zmeny Kódexu. To nemá vplyv na tie ustanovenia, z ktorých podstaty vyplýva, že banky sa od nich môžu odchýliť, majú odporúčací charakter alebo majú príkladný (demonštratívny) charakter.

1.4 Vzťah Kódexu k právomoci Úradu na ochranu osobných údajov

Týmto Kódexom nie sú dotknuté žiadne právomoci Úradu na ochranu osobných údajov podľa GDPR alebo Zákona o ochrane osobných údajov vo vzťahu k bankám ako kontrolovaným subjektom alebo účastníkom konania. Napriek tomu, že dodržiavanie Kódexu banky môžu použiť ako prvok na preukázanie súladu s GDPR, samotné pristúpenie ku Kódexu neznamená automaticky zabezpečenie súladu banky s GDPR alebo inými predpismi na ochranu osobných údajov. Každá banka je povinná zabezpečovať súlad s GDPR a inými predpismi na ochranu osobných údajov, pričom Kódex slúži ako záväzný výklad GDPR v tejto súvislosti. Pristúpením ku Kódexu nie je dotknutá možnosť dotknutých osôb obrátiť sa akýmkoľvek podaním na Úrad na ochranu osobných údajov alebo na príslušný súd.

1.5 Zmeny Kódexu

Akékoľvek zmeny alebo rozšírenia Kódexu podliehajú predchádzajúcemu schváleniu zo strany Úradu na ochranu osobných údajov, pričom tieto je oprávnená navrhovať výlučne Slovenská banková asociácia a to spôsobom, akým rozhoduje prostredníctvom svojich orgánov podľa platných stanov Slovenskej bankovej asociácie. Aktualizácia zoznamu bánk, ktoré pristúpili ku Kódexu, vykonávaná zo strany Slovenskej bankovej asociácie, nie je zmenou ani rozšírením Kódexu a nepodlieha schváleniu zo strany Úradu na ochranu osobných údajov. Slovenská banková asociácia je kedykoľvek oprávnená rozhodnúť o zrušení tohto Kódexu, pričom zrušenie Kódexu musí Slovenská banková asociácia oznámiť Úradu na ochranu osobných údajov do 60 dní.

1.6 Vzťah k iným právnym predpisom

1.6.1 GDPR predstavuje všeobecný právny predpis Európskej únie pre oblasť ochrany osobných údajov. Podľa zásady *lex specialis derogat legi generali* vo všeobecnosti platí, že ak iné právne predpisy precizujú podmienky spracúvania osobných údajov, takéto právne predpisy predstavujú tzv. špeciálne predpisy vo vzťahu k GDPR.

1.6.2 Na bankový sektor sa vzťahuje množstvo ďalších predpisov, ktoré upravujú spracúvanie osobných údajov. Okrem iného ide o Zákon o bankách, Zákon o elektronických komunikáciách (a pripravované e-Privacy nariadenie), Zákon o kybernetickej bezpečnosti (implementujúci Smernicu NIS) alebo Zákon o platobných službách (implementujúci Smernicu PSD2).

1.6.3 Bankový sektor patrí medzi najregulovanejšie sektory vôbec, pričom regulácia bankového sektora a povinností bánk okrem iného aj vo vzťahu k spracúvaniu osobných údajov vychádza primárne z práva Európskej únie. Z toho dôvodu je pre bankový všeobecným predpisom na ochranu osobných údajov GDPR. Ustanovenia §2, §5, druhej a tretej časti Zákona o ochrane osobných údajov sa na bankový sektor nevzťahujú.

1.7 Vysvetlenie niektorých súvisiacich pojmov

1.7.1 Osobné údaje

Osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby, pričom táto fyzická osoba sa v rámci oblasti ochrany osobných údajov označuje ako dotknutá osoba. Zásady ochrany údajov by sa preto nemali uplatňovať na anonymné informácie, konkrétne na informácie, ktoré sa nevzťahujú na identifikovanú alebo identifikovateľnú fyzickú osobu, ani na osobné údaje, ktoré sa stali anonymnými takým spôsobom, že dotknutá osoba nie je alebo už nie je identifikovateľná. GDPR sa preto netýka spracúvania takýchto anonymných informácií vrátane spracúvania na štatistické účely alebo účely výskumu. GDPR sa nevzťahuje ani na spracúvanie osobných údajov, ktoré sa týkajú právnických osôb, a najmä podnikov založených ako právnické osoby vrátane názvu, formy, identifikačných (napr. IČO) a kontaktných údajov právnickej osoby.

1.7.2 Identifikovaná fyzická osoba

Fyzická osoba sa vo všeobecnosti môže považovať za identifikovanú vtedy, keď je v rámci skupiny osôb odlíšiteľná od všetkých ostatných príslušníkov skupiny, čiže dôjde k jednoznačnému určeniu jej identity.

1.7.3 Identifikovateľná fyzická osoba

Identifikovateľná fyzická osoba je osoba, ktorú je možné identifikovať prostriedkami, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby. Každá fyzická osoba je v teoretickej rovine identifikovateľná. Pre účely posudzovania či je fyzická osoba identifikovateľná z pohľadu definície osobných údajov (t.j. či ide o osobné údaje) je rozhodujúci test primeranej pravdepodobnosti upravený v recitáli č. 26 GDPR.

1.7.4 Test primeranej pravdepodobnosti

Na zistenie toho, či je primerane pravdepodobné, že sa prostriedky použijú na identifikáciu fyzickej osoby, by sa mali zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj. Test primeranej pravdepodobnosti nie je splnený, keď je identifikácia dotknutej osoby je zakázaná právnymi predpismi alebo

prakticky neuskutočniteľná, napríklad preto, lebo by si vyžadovala neprimerane veľa času, financií alebo ľudských zdrojov, takže pravdepodobnosť identifikácie sa v skutočnosti javí ako zanedbateľná.[1] Výsledkom aplikácie testu primeranej pravdepodobnosti môže byť v konkrétnom prípade aj záver, že spracúvané informácie nepredstavujú osobné údaje, nakoľko neexistuje primeraná pravdepodobnosť použitia prostriedkov na identifikáciu fyzickej osoby, ktorej sa tieto informácie týkajú.

1.7.5 Informačný systém

Pojem informačný systém je podľa GDPR testom na určenie toho, či osobné údaje spracúvané manuálne (t.j. v papierovej alebo fyzickej podobe) majú spadať pod pôsobnosť GDPR alebo nie. Daný test je upravený v článku 4 (6) GDPR: „*akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe*."[2] Vizitky, tabuľky na dverách alebo menovky na uniformách síce môžu predstavovať alebo obsahovať osobné údaje, avšak typicky nepredstavujú informačný systém v zmysle článku 4 (6) GDPR. Na spracúvanie osobných údajov v manuálnej podobe, ktoré navyše nepredstavujú súčasť informačného systému a ani nie sú určené na to, aby tvorili súčasť informačného systému sa GDPR v zmysle článku 2 ods. 1 GDPR nevzťahuje.

1.7.6 Dotknutá osoba

Dotknutá osoba je fyzická osoba, o ktorej osobné údaje sa v danom prípade jedná. V bankovom sektore ide najčastejšie o fyzickú osobu, ktorou je klient banky, alebo fyzickú osobu, ktorá rokuje s bankou o uzatvorení zmluvy (potenciálny klient banky). Pre účely tohto Kódexu je potrebné pojem dotknutá osoba vykladať v súlade s vymedzením pôsobnosti tohto Kódexu v bode 1.1.2 vyššie. Tento Kódex sa nevzťahuje na spracúvanie osobných údajoch o všetkých dotknutých osobách vykonávaných bankami. Okruh dotknutých osôb pre účely tohto Kódexu je užší ako skutočný okruh všetkých dotknutých osôb, o ktorých banky spracúvajú osobné údaje, ktorý by inak zahŕňal aj ďalšie osoby ako napr. zamestnancov bánk.

1.7.7 Pseudonymizované a anonymizované osobné údaje

Podľa GDPR sa za osobné údaje považujú aj tzv. pseudonimizované osobné údaje.[3] O pseudonymizované osobné údaje môže ísť napríklad v prípade, ak banka používa vo svojich systémoch namiesto mena a priezviska dotknutej osoby identifikátor (napr. „ID12345"), ktorý neumožňuje osobe bez prístupu k zoznamu identifikátorov a ostatných osobných údajov (napr. mien a priezvisk) identifikovať danú osobu. Pseudonymizácia spolu so šifrovaním osobných údajov je odporúčaným bezpečnostným opatrením, ktoré znižuje riziko identifikácie dotknutých osôb ako aj riziko pre práva a slobody fyzických osôb v rámci bežnej prevádzky banky alebo pri porušení ochrany osobných údajov. GDPR sa naopak nevzťahuje na anonymizované údaje,[4] pričom anonymizovanými údajmi sa môžu vykonaním určitých opatrení stať aj osobné údaje. Anonymizácia alebo pseudonymizácia osobných údajov nepredstavuje spracúvanie

[1] Rozsudok Súdneho dvora EÚ vo veci C-582/14 (Breyer vs Nemecko) zo dňa 19. októbra 2016, ods. 46.
[2] Tento pojem je v GDPR použitý výlučne v súvislosti s vecnou pôsobnosťou GDPR uvedenou v článku 2 ods. 1.
[3] Článok 4 ods. 5 GDPR: „*Pseudonymizácia je spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe* ***bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene*** *a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe.*"
[4] Recitál 26 GDPR: „*Zásady ochrany údajov by sa preto nemali uplatňovať na* ***anonymné informácie****, konkrétne na informácie, ktoré sa nevzťahujú na identifikovanú alebo identifikovateľnú fyzickú osobu,* ***ani na osobné údaje, ktoré sa stali anonymnými takým spôsobom, že dotknutá osoba nie je alebo už nie je identifikovateľná. Toto nariadenie sa preto netýka spracúvania takýchto anonymných informácií vrátane spracúvania na štatistické účely alebo účely výskumu****.*"

osobných údajov na nový účel, ktoré by bolo podmienené použitím osobitného právneho základu spracúvania osobných údajov.

1.7.8 Špecificky a štandardne navrhnutá ochrana osobných údajov

Článok 25 GDPR vyžaduje prístup, ktorý je založený na predpokladaní, zohľadňovaní, zmierňovaní a riadení rizík pre práva a slobody fyzických osôb v inom rozsahu ako typicky zabezpečujú technické normy v oblasti informačnej bezpečnosti. Tento prístup môže zahŕňať viaceré prvky ako napr. zohľadňovanie súkromia na začiatku projektov, interných procesov, vývoja nových produktov a služieb (*by design*) alebo zvolenie ako východzích také nastavenia, ktoré menej zasahujú do súkromia (*by default*). Špecificky a štandardne navrhnutú ochranu osobných údajov môže banka preukázať najmä internými politikami, nadväzujúcimi procesmi alebo bezpečnostnými opatreniami, ktoré obsahujú tieto prvky prípadne internou komunikáciou, analýzami, výstupmi, zápismi zo stretnutí alebo obdobnými informáciami ktoré potvrdzujú, že zohľadňovanie aspektov ochrany osobných údajov je súčasťou prijímania takých kľúčových rozhodnutí banky, ktoré môžu mať dopad na práva a slobody fyzických osôb. Spôsob, akým je špecificky a štandardne navrhnutá ochrana osobných údajov implementovaná jednotlivými bankami sa môže líšiť.

2 Postavenie bánk pri spracúvaní osobných údajov

2.1 Banka ako prevádzkovateľ

Prevádzkovateľ je osoba, ktorá rozhoduje o účeloch („prečo“) a prostriedkoch („ako“) spracúvania osobných údajov, čím je oprávnená formálne prijímať rozhodnutia týkajúce sa spracúvania osobných údajov. Vo všeobecnosti banky vystupujú vo vzťahu k svojim klientom ako prevádzkovatelia. Banka nie je považovaná za prevádzkovateľa, ak získa osobné údaje náhodným spôsobom bez predchádzajúceho určenia účelov a prostriedkov spracúvania, pričom v takom prípade sa ňu GDPR nevzťahuje. Môže ísť o situácie, kedy sú banke poskytnuté osobné údaje omylom, nedopatrením, špekulatívnym spôsobom alebo sú jej poskytnuté také osobné údaje, o ktoré nežiadala a nemá záujem tieto osobné údaje ďalej spracúvať na žiadne účely. Banka je oprávnená vrátiť alebo vymazať náhodne získané údaje. Vrátanie alebo vymazanie náhodne získaných osobných údajov bez predchádzajúceho určenia účelov podľa predchádzajúcej vety nepredstavuje spracúvanie osobných údajov banky ako prevádzkovateľa.

2.2 Banka ako sprostredkovateľ

Sprostredkovateľ je osoba, ktorá spracúva osobné údaje v mene prevádzkovateľa. Sprostredkovateľ na rozdiel od prevádzkovateľa nemá oprávnenie rozhodovať o účeloch a prostriedkoch spracúvania a preto nie je oprávnený formálne prijímať rozhodnutia týkajúce sa spracúvania osobných údajov. To však neznamená, že by sprostredkovateľ nebol oprávnený spracúvať tie isté osobné údaje aj ako prevádzkovateľ, v takom prípade musia byť splnené všetky podmienky spracúvania osobných údajov vyžadovaných od prevádzkovateľov. Banka môže takisto vystupovať ako sprostredkovateľ pre iných prevádzkovateľov. Najčastejšie ide o situácie, kedy klient rokuje s bankou o uzatvorení zmluvy alebo plnení zmluvy s inou spoločnosťou, vo vzťahu ku ktorej banka vystupuje ako jej sprostredkovateľ. Môže ísť napr. o sprostredkovanie poistenia u poisťovne, avšak prostredníctvom banky. Banka môže takisto vystupovať ako sprostredkovateľ inej spoločnosti patriacej do jej skupiny. V takýchto prípadoch zodpovedá banka ako sprostredkovateľ len za tieto povinnosti týkajúce sa spracúvania osobných údajov, ktoré jej vyplývajú so zmluvy medzi bankou ako sprostredkovateľom a inou spoločnosťou ako prevádzkovateľom a zároveň za tie,

ktoré vyplývajú sprostredkovateľom priamo z GDPR. Banka bude k daným dotknutým osobám spravidla naďalej vystupovať aj ako prevádzkovateľ vo vzťahu k svojim vlastným účelom spracúvania. GDPR predpokladá, že ten istý subjekt môže vystupovať súčasne aj ako prevádzkovateľ a sprostredkovateľ vo vzťahu tej istej osobe a tým istým osobným údajom.

2.3 Skupina finančných inštitúcií

2.3.1 GDPR dovoľuje bankám viacero legitímnych modelov nastavenia skupinových vzťahov vo vzťahu k zdieľaniu alebo spoločnému spracúvaniu osobných údajov, pričom tento Kódex nepreferuje ani nezakazuje žiadnu z nich a rovnako nezakazuje ani kombinácie týchto modelov medzi vybranými bankami v rámci skupiny. Ak vzniknú nejasnosti ohľadne postavenia jednotlivých bánk patriacich do tej istej skupiny, nemusí tým automaticky dôjsť k zásahu do práv a oprávnených záujmov dotknutých osôb, ak je v rámci skupiny bánk materiálne zabezpečené plnenie povinností podľa GDPR jednotlivými subjektami. Materiálne plnenie povinností podľa GDPR voči dotknutým osobám je vždy dôležitejším faktorom ako formálne určenie postavenia jednotlivých subjektov patriacich do skupiny bánk.

2.3.2 Skupina finančných inštitúcií môže predstavovať spoločných prevádzkovateľov. Z definície pojmu prevádzkovateľ vyplýva, že banka môže určiť účely a prostriedky spracúvania osobných údajov aj spoločne s inými prevádzkovateľmi. V takom prípade ide o tzv. spoločných prevádzkovateľov podľa článku 26 GDPR. Banky, ktoré sú spoločnými prevádzkovateľmi by mali transparentne určiť svoje príslušné zodpovednosti za plnenie povinností podľa GDPR, najmä pokiaľ ide o vykonávanie práv dotknutej osoby, a svoje povinnosti poskytovať informácie uvedené v článkoch 13 a 14 GDPR, a to formou vzájomnej dohody. Podľa článku 26 ods. 2 GDPR by sa základné časti dohody spoločných prevádzkovateľov mali poskytovať dotknutým osobám. Táto povinnosť je splnená, ak banka zmysluplným spôsobom poskytne dotknutým osobám základné informácie o spoločnom spracúvaní osobných údajov v rámci skupiny, pričom banka nie je povinná poskytovať alebo zverejňovať túto dohodu alebo jej znenie, najmä nie časti týkajúce sa prijatých bezpečnostných opatrení. Princíp bánk ako spoločných prevádzkovateľov môže mať význam aj v iných situáciách, napríklad pri spoločných marketingových aktivitách viacerých, ale nie všetkých bánk patriacich do jednej skupiny.

2.3.3 Banky patriace do tej istej skupiny môžu byť navzájom vo vzťahu prevádzkovateľov a sprostredkovateľov, a to najmä, ak jeden subjekt v rámci skupiny bánk vykonáva určité spracovateľské činnosti v mene a podľa pokynov iných subjektov. Povinnosť prevádzkovateľa preveriť dostatočné záruky sprostredkovateľa pred jeho poverením na spracúvanie osobných údajov podľa článku 28 ods. 1 GDPR je v kontexte zdieľania údajov v rámci tej istej skupiny bánk splnená, ak tieto záruky vyplývajú pre sprostredkovateľa z interných politík, zmlúv alebo štandardov celej skupiny. Tým však nie je dotknutá povinnosť uzatvoriť zmluvu so sprostredkovateľom podľa článku 28 ods. 3 GDPR.

2.3.4 Ustanovenia vyššie podporujú existujúcu prax prijímania mnohostranných skupinových zmlúv o spracúvaní / zdieľaní osobných údajov alebo interných skupinových politík zameraných na skupinové spracúvanie / zdieľanie osobných údajov, ktoré môžu slúžiť na transparentné vymedzenie povinností bánk podľa GDPR. Tieto skupinové zmluvy alebo politiky môžu zároveň plnohodnotne nahrádzať zmluvy medzi spoločnými prevádzkovateľmi a/alebo zmluvy medzi prevádzkovateľmi a sprostredkovateľmi a zároveň môžu obsahovať záruky týkajúce sa cezhraničných prenosov do tretích krajín, ako napr. zmluvné doložky, vnútropodnikové záväzné pravidlá a pod. za

predpokladu, že spĺňajú náležitosti podľa článkov 26 resp. 28 GDPR.Z dôvodu ochrany svojho know-how alebo obchodného tajomstva nie sú banky povinné zverejňovať alebo poskytovať tieto zmluvy alebo politiky dotknutým osobám. Tým nie sú dotknuté povinnosti poskytovať dotknutým osobám základné informácie podľa článkov 13 a 14 GDPR a povinnosti týkajúce sa cezhraničných prenosov do tretích krajín podľa článku 44 a nasledujúcich GDPR.

3 Účely spracúvania osobných údajov v bankovom sektore

3.1 Hlavné účely spracúvania osobných údajov

3.1.1 Účel spracúvania osobných údajov odpovedá dotknutým osobám na otázku *prečo sú ich osobné údaje spracúvané*. V bankovom sektore typicky dochádza k spracúvaniu osobných údajov, ktoré sú uvedené v nižšie uvedenom príkladnom výpočte hlavných účelov. Nič v tomto Kódexe nebráni bankám spracúvať osobné údaje aj na inak definované účely za podmienok stanovených v GDPR. Banky sú oprávnené pristupovať osobitne k pomenovaniu týchto účelov a k ich presnému či detailnému vymedzeniu a kategorizovaniu. Napr. zabezpečovanie súladu s právnymi predpismi môže tvoriť súčasť účelu poskytovanie bankových produktov a služieb. Zároveň, nie všetky banky musia spracúvať osobné údaje na všetky účely uvedené nižšie. Zmyslom Kódexu v tomto smere nie je obmedzovať banky v ich prístupe k určovaniu účelov, miere detailu pri ich určovaní a prostriedkov spracúvania osobných údajov, nakoľko tento prístup sa môže medzi bankami líšiť z viacerých objektívnych dôvodov ako napríklad rôzne bankové produkty poskytované bankami alebo príslušnosť bánk do skupín s hlavnými prevádzkarňami v rôznych členských štátoch. V bankovom sektore typicky dochádza k spracúvaniu osobných údajov na nasledovné hlavné účely spracúvania:

Hlavný účel spracúvania osobných údajov	**Právny základ podľa GDPR**	**Súvisiace právne predpisy**
Poskytovanie bankových produktov a služieb	Plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba podľa článku 6 ods. 1 písm. b) GDPR a/alebo splnenie zákonnej povinnosti prevádzkovateľa podľa článku 6 ods. 1 psím. c) GDPR	Zákon o bankách, Zákon o spotrebiteľských úveroch, Zákon o úveroch na bývanie, Zákon o cenných papieroch, Zákon zmenkový a šekový, Zákon o platobných službách, Obchodný a Občiansky zákonník a ďalšie právne predpisy
Marketingové účely	Súhlas dotknutej osoby podľa článku 6 ods. 1 písm. a) GDPR a/alebo oprávnený záujem bánk alebo tretích strán podľa článku 6 ods. 1 psím. f) GDPR	Zákon o elektronických komunikáciách a ďalšie právne predpisy, recitál 47 GDPR, Občiansky alebo Obchodný zákonník
Zabezpečovanie súladu s právnymi predpismi	Splnenie zákonnej povinnosti prevádzkovateľa podľa článku 6 ods. 1 psím. c) GDPR a/alebo oprávnený záujem bánk alebo tretích strán podľa článku 6 ods. 1 psím. f) GDPR	GDPR, Zákon o dohľade nad finančným trhom, SSM Nariadenie, Zákon o NBS, Zákon o bankách, usmernenia a odporúčania NBS alebo ESFD, Zákon o ochrane pred legalizáciou príjmov z trestnej činnosti (AML), Zákon o cenných papieroch a investičných službách (MiFID), Zákon o platobných službách (PSD 2 a e-Money), Zákon

		o automatickej výmene informácií o finančných účtoch, FATCA a ďalšie právne predpisy, osobitné právne predpisy v oblasti účtovníctva a správy daní
Preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov	Oprávnený záujem bánk alebo tretích strán podľa článku 6 ods. 1 písm. f) GDPR (aj v kontexte článku 9 ods. 2 písm. f) GDPR) a/alebo splnenie zákonnej povinnosti prevádzkovateľa podľa článku 6 ods. 1 písm. c) GDPR	Civilný sporový poriadok, Civilný mimosporový poriadok, Súdny správny poriadok, Občiansky súdny poriadok, Správny poriadok, osobitné právne predpisy týkajúce sa konaní pred orgánmi verejnej moci, Zákon o bankách, Občiansky zákonník, Obchodný zákonník, Exekučný poriadok, Zákon o konkurze a reštrukturalizácii
Štatistické účely, archívne účely vo verejnom záujme, účely historického a vedeckého výskumu	Pôvodný právny základ v zmysle režimu článku 89 GDPR (zlučiteľné účely)	Zákon o archívoch v súvislosti s archívnymi účelmi vo verejnom záujme

3.1.2 Vyššie uvedené hlavné účely spracúvania sú bližšie vysvetlené v nasledovných bodoch. Banky sú oprávnené pristupovať k účelom spracúvania tak ako sú vymedzené vyššie alebo aj podrobnejšie, tak ako sú vysvetlené nižšie, vždy podľa okolností konkrétneho prípadu. Pri niektorých hlavných účeloch spracúvania môže byť potrebné, aby banky bližšie vysvetlili, aké spracovateľské operácie alebo aj samostatné účely sú zahrnuté do daných hlavných účelov. Tieto bližšie informácie môžu byť poskytované dotknutým osobám vrstveným spôsobom, tak aby dotknutá osoba nebola zahltená príliš detailnými informáciami o účeloch spracúvania pri prvom oboznámení sa s informačnou povinnosťou.

3.2 Bližšie vysvetlenie vybraných hlavných účelov spracúvania osobných údajov

3.2.1 Každý hlavný účel spracúvania môže mať v praxi viacero rovín, podôb, právnych základov a môže zahŕňať rozličné spracovateľské operácie alebo činnosti banky.

3.2.2 Poskytovanie bankových produktov a služieb môže zahŕňať napr. nasledovné činnosti banky:

- Identifikácia a overenie identifikácie klientov a ich zástupcov, vrátane spracúvania biometrických údajov týchto osôb;
- Príprava zmluvného vzťahu na žiadosť klienta;
- Uzatváranie a vykonávanie obchodov medzi bankou a jej klientami;
- Poskytovanie bankových, finančných a platobných služieb;
- Realizácia tuzemských a zahraničných platobných príkazov;
- Výroba, správa a personalizácia platobných kariet;
- Kontrola správnosti zúčtovania platobných transakcií;
- Zasielanie servisných správ;
- Správa a kontrola záväzkového vzťahu medzi klientom a bankou;
- Poštová, emailová, telefonická a osobná komunikácia s klientom banky týkajúca sa konkrétneho zmluvného vzťahu;

- Poskytovanie doplnkových služieb s pridanou hodnotou pre klienta (napr. internet banking alebo mobilné bankové aplikácie);
- Vybavovanie reklamácií a sťažností;
- Poskytovanie zákazníckej alebo technickej podpory.

3.2.3 Marketingové účely môžu zahŕňať spracúvanie osobných údajov, ktoré je nevyhnutné napr. pre nasledovné činnosti banky:

- Marketing na základe oprávnených záujmov banky alebo tretej strany;
- Zasielanie marketingových ponúk;
- Marketing vlastných a podobných tovarov;
- Marketingové prieskumy a prieskumy spokojnosti klientov;
- Reklamné kampane;
- Zobrazovanie cielenej reklamy;
- Marketingové informácie a ponuky zverejnené na pobočke banky alebo v elektronickom prostredí banky (aplikácie) na základe oprávneného záujmu;
- Profilovanie za účelom personalizácie ponúk produktov a služieb;
- Vytváranie analytických modelov pre prispôsobovanie marketingovej stratégie banky do budúcnosti;
- Používanie analytických riešení na vyhodnocovanie úspešnosti marketingových kampaní a stratégií banky;
- Používanie analytických riešení na personalizáciu marketingových oslovení alebo ponúk;
- Používanie prediktívnych analytických riešení na personalizáciu produktov, služieb a marketingových aktivít banky;
- Informovanie o prvkoch alebo funkciách produktu alebo služby, ktoré by mohli byť pre dotknutú osobu vhodné, účelné alebo odporúčané (*you may like*);
- Uchovávanie námietok dotknutých osôb proti spracúvaniu ich osobných údajov na účely priameho marketingu;
- Organizovanie a vyhodnocovanie spotrebiteľských súťaží.

3.2.4 Zabezpečovanie súladu s právnymi predpismi môže zahŕňať napr. nasledovné činnosti banky:

- Ochrana integrity finančného sektora pred podvodnými konaniami;
- Poskytovanie základných informácií o platobných operáciách osobám, ktoré boli vykonané chybným spôsobom, oprávneným osobám najmä v súvislosti s § 92 ods. 1 Zákona o bankách;
- Plnenie povinností v rámci ESFS;
- Zabezpečenie súladu s rozhodnutiami, opatreniami alebo odporúčaniami ECB, NBS, ESMA alebo EBA;
- Uplatňovanie medzinárodných sankcií a plnenie úloh podľa medzinárodných zmlúv;
- Vnútro-skupinové zdieľanie a prenosy osobných údajov na vyššie uvedené účely (§ 92 ods. 11 Zákona o bankách);
- Plnenie povinností na úseku účtovníctva a správy daní;
- Oznamovanie protispoločenskej činnosti (*whistleblowing*) v súlade so Zákonom o oznamovaní protispoločenskej činnosti;
- Príprava výročných správ alebo obdobných dokumentov.

3.2.5 Preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov ako samostatný účel môže zahŕňať ochranu práv banky najmä prostredníctvom súdnej ochrany alebo ochrany prostredníctvom správnych a iných konaní v súvislosti s činnosťami, ktoré nespadajú pod účel poskytovania bankových produktov a služieb. Ide napríklad

o ochranu majetku banky, ochranu práv a právom chránených záujmov pred protiprávnym konaním osôb, ktoré nie sú klientmi banky alebo zamestnancami a pod.

3.2.6 Banky získavajú osobné údaje spracúvané na vyššie uvedené účely najmä komunikáciou s klientami bánk na pobočkách, písomnou korešpondenciou, telefonicky alebo elektronicky. V praxi môže dôjsť k situácií, kedy klient banky poskytne banke aj osobné údaje o iných fyzických osobách, ktoré je banka povinná alebo oprávnená na spracúvať na vlastné účely. Predchádzajúci písomný súhlas týchto iných osôb nie je podľa § 78 ods. 6 Zákona o ochrane osobných údajov potrebný, ak klient banky poskytovaním údajov banke chráni svoje práva alebo právom chránené záujmy; oznamuje skutočnosti, ktoré odôvodňujú uplatnenie právnej zodpovednosti tejto inej osoby; alebo banka je povinná alebo oprávnená osobné údaje o tejto inej osobe spracúvať na základe osobitných zákonov. Takáto situácia nastáva napríklad v prípade spracúvania osobných údajov na účely stanovené zákonom o bankách, pričom v zmysle § 93a ods. 1 a nasl. Banky sú oprávnené požadovať od klientov, potenciálnych klientov alebo osôb, ktoré sa vydávajú za klientov poskytnutie dokladov ich totožnosti na účely overenia totožnosti alebo splnenia zákonných alebo zmluvných povinností bánk a sú oprávnené tieto doklady skenovať, kopírovať alebo inak zaznamenávať bez súhlasu dotknutej osoby.

3.3 Spracúvanie osobných údajov v rámci ochrany oprávnených záujmov

Právny základ ochrany oprávnených záujmov bánk alebo tretej strany podľa článku 6 ods. 1 písm. f) GDPR typicky súvisí so spracúvaním osobných údajov na účely, ktoré nie sú upravené ako výslovná, explicitná zákonná povinnosť bánk resp. nevyplývajú z iných právnych základov. Oprávnený záujem môže slúžiť aj ako doplňujúci právny základ pre spracúvanie osobných údajov na účely, ktoré síce predpokladá právny predpis, ktorý však nedostatočne špecifikuje podmienky spracúvania osobných údajov. Typickým príkladom kedy spracúvanie osobných údajov môže byť založené na právnom základe ochrany oprávnených záujmov ale súčasne aj na iných právnych základoch je napr. oblasť informačnej bezpečnosti v súvislosti s povinnosťou bánk prijať primerané bezpečnostné opatrenia na ochranu osobných údajov podľa GDPR, pričom prijatie bezpečnostných opatrení môže predstavovať nie len ochranu oprávnených záujmov ale aj povinnosť vyplývajúcu zo všeobecne záväzného právneho predpisu. Zvolenie právneho základu spracúvania údajov v obdobných prípadoch by malo byť ponechané na banke ako prevádzkovateľovi, ktorý rozhoduje o účeloch a prostriedkoch spracúvania.

3.4 Osobitné prípady spracúvania osobných údajov

3.4.1 Prechod osobných údajov pri predaji podniku alebo časti podniku (tzv. *asset deal*)

i. V prípade predaja podniku alebo časti podniku dochádza podľa § 477 ods. 1 Obchodného zákonníka k prechodu všetkých práv a záväzkov, na ktoré sa predaj vzťahuje, z predávajúcej banky na kupujúcu banku. Z obchodno-právneho pohľadu na kupujúcu banku môžu prechádzať (a spravidla aj prechádzajú) niektoré alebo všetky zmluvy s klientami predávajúcej banky. Prechod všetkých práv a záväzkov vo vzťahu k prechádzajúcim zmluvám predpokladá aj prechod práva predávajúcej banky ďalej spracúvať osobné údaje v súvislosti s týmito zmluvami na kupujúcu banku, a to bez súhlasu dotknutých osôb. Prechod práva ďalej spracúvať dané osobné údaje znamená aj prechod samotných osobných údajov, a to bez súhlasu dotknutej osoby.

ii. Osobné údaje, ktoré sú spracúvané predávajúcou bankou v súvislosti s prechádzajúcimi zmluvami sa nemusia týkať len klienta banky ako zmluvnej strany

danej zmluvy. Tieto osobné údaje sa môžu týkať aj iných fyzických osôb napr. v prípade, ak sú spracúvané v súvislosti s danou zmluvou, avšak na právnom základe osobitných predpisov vzťahujúcich sa na predávajúcu banku alebo na inom právnom základe. Zmluvné strany sa môžu dohodnúť, či sa prechod vzťahuje aj na tieto ďalšie údaje alebo nie.

iii. Ak sa predaj vzťahuje aj na právo predávajúcej banky spracúvať osobné údaje získané na základe súhlasu dotknutej osoby, tieto súhlasy predstavujú práva, ktoré prechádzajú na kupujúcu banku. Spolu so súhlasmi dotknutých osôb prechádzajú na kupujúcu banku aj samotné osobné údaje, na ktoré sa súhlasy vzťahujú, a to bez súhlasu dotknutých osôb.

iv. Ak prechod osobných údajov a súhlasov dotknutých osôb so spracúvaním osobných údajov predpokladá zmluva o predaji podniku alebo časti podniku, nejde o poskytnutie alebo sprístupnenie osobných údajov tretej strane ani o ďalší prenos osobných údajov (tzv. *onward transfer*), ale o prechod na základe Obchodného zákonníka, pričom na tento prechod sa nevzťahuje podmienka získania súhlasu dotknutej osoby.

v. Pri predaji podniku alebo časti podniku však dochádza k zmene identity banky, ktorá vystupuje vo vzťahu k dotknutým osobám spravidla ako prevádzkovateľ, ako aj k zmene niektorých ďalších informácií, ktoré sa majú poskytovať podľa článkov 13 a 14 GDPR ako napr. kontaktné informácie zodpovednej osoby banky. Oznámenie zmeny týchto informácií môže realizovať predávajúca alebo kupujúca banka, pričom medzi predávajúcou a kupujúcou bankou by mala existovať výslovná dohoda o splnení obdobných povinností.

vi. Pri predaji podniku alebo časti podniku je odporúčaným postupom bánk podľa tohto Kódexu zohľadniť najmä otázku cezhraničných prenosov osobných údajov do tretích krajín a medzinárodných organizácií. Dotknuté osoby musia byť informované o zamýšľaných prenosoch osobných údajov do tretej krajiny alebo medzinárodnej organizácie a o existencii alebo neexistencii rozhodnutia Komisie o primeranosti alebo v prípade prenosov uvedených v článku 46 alebo 47 GDPR či v článku 49 ods. 1 druhom pododseku GDPR aj o odkaze na primerané alebo vhodné záruky a prostriedky na získanie ich kópie, alebo kde boli poskytnuté, pokiaľ z GDPR alebo iných právnych predpisov nevyplýva inak.

vii. Vyššie uvedené pravidlá sa nevzťahujú na prípady zmeny akcionára alebo akcionárskej štruktúry banky (tzv. *share deal*). Odporúčaným postupom bánk podľa tohto Kódexu je aj v takom prípade zohľadniť, či nedochádza k zmene informácií, ktoré sa majú dotknutým osobám poskytovať podľa článkov 13 a 14 GDPR.

viii. Vyššie uvedené pravidlá nemajú vplyv na povinnosť bánk získať predchádzajúci súhlas Národnej banky Slovenska podľa Zákona o bankách.

ix. V rámci vyššie uvedených transakcií môže dôjsť k poskytnutiu osobných údajov osobe, s ktorou banka jedná o predaji a zároveň jej profesionálnym poradcom. Takéto poskytnutie prebieha na základe § 92 ods. 9 Zákona o bankách, pričom je odporúčaným postupom podľa tohto Kódexu uzatvárať s danými osobami zmluvy o zachovaní mlčanlivosti aj v prípade, ak sa na predaj nevzťahuje predchádzajúci súhlas Národnej banky Slovenska. Bez toho aby boli dotknuté všeobecné

informačné povinnosti a zákonnosť spracúvania, banky ani poradcovia nie sú v týchto prípadoch povinní osobitne poskytovať informácie týkajúce sa transakcií a na dané spracúvanie a poskytnutie osobných údajov nie je potrebný súhlas dotknutých osôb.

3.4.2 Zaznamenávanie telefonickej a elektronickej komunikácie s klientami

i. K zaznamenávaniu telefonickej a elektronickej komunikácie s klientmi zo strany bánk môže dochádzať z viacerých dôvodov, pričom tieto môžu predstavovať odlišné účely spracúvania osobných údajov, na ktoré sa vzťahujú odlišné právne režimy.

ii. Banka je povinná zaznamenávať určitú telefonickú a elektronickú komunikáciu s klientom podľa § 75 Zákona o cenných papieroch (režim Smernice MiFID II). Daná povinnosť sa vzťahuje len na takú komunikáciu, v ktorej banka vystupuje ako obchodník s cenným papiermi, ktorý poskytuje investičné služby, investičné činnosti a vedľajšie služby podľa Zákona o cenných papieroch. Takéto zaznamenávanie a súvisiace spracúvanie osobných údajov je zákonnou povinnosťou banky a nie je podmienené súhlasom dotknutej osoby so spracúvaním osobných údajov podľa GDPR. Takéto záznamy slúžia aj na ochranu klientov banky, nakoľko môžu byť poskytnuté Národnej banke Slovenska pri vykonávaní dohľadu nad bankami. Banka je podľa Zákona o cenných papieroch povinná informovať nových i existujúcich klientov o tom, že takýto telefonický rozhovor sa bude nahrávať. Takéto oznámenie sa môže uskutočniť raz pred poskytnutím investičných služieb novým klientom alebo existujúcim klientom. Ak si banka už splnila povinnosť informovania o nahrávaní vo vzťahu ku konkrétnemu klientovi, nie je povinná uvedenú informáciu poskytovať pri ďalšej telefonickej alebo elektronickej komunikácii. Zaznamenané záznamy sa na požiadanie poskytnú dotknutým klientom a uchovávajú sa počas piatich rokov a na žiadosť Národnej banky Slovenska počas siedmich rokov. Banky sú oprávnené uchovávať dané záznamy spolu s akoukoľvek inou dokumentáciou klienta.

iii. Banka je oprávnená zaznamenávať telefonickú a elektronickú komunikáciu s klientom aj na účely skvalitňovania svojich služieb a produktov, pričom tieto môžu predstavovať oprávnené záujmy banky alebo skupiny, do ktorej banka patrí za podmienky, že banka vie prevahu týchto oprávnených záujmov preukázať s poukazom na článok 6 ods. 1 písm. f) GDPR. V tomto prípade banka nie je povinná získavať súhlas dotknutej osoby so spracúvaním osobných údajov podľa GDPR. Stačí, ak je na začiatku komunikácie klient oboznámený so zaznamenávaním telefonickej alebo elektronickej komunikácie na účely skvalitňovania služieb a produktov banky a po tomto oznámení klient v telefonickom hovore pokračuje.

iv. Banky sú podľa Zákona o bankách povinné uchovávať údaje a kópie dokladov o preukázaní totožnosti klienta a doklady o zisťovaní vlastníctva prostriedkov použitých klientom na vykonanie obchodu a zmluvy a iné doklady o uskutočnených obchodoch najmenej päť rokov od ukončenia obchodu. Tieto doklady môžu byť v relevantných prípadoch zaznamenané aj prostredníctvom telefonickej alebo elektronickej komunikácie s klientom.

v. Banky sú podľa Zákona o bankách oprávnené monitorovať svoje priestory a bankomaty pomocou videozáznamu alebo audiozáznamu aj súhlasu

dotknutých osôb na účely odhaľovania trestných činov, na zisťovanie ich páchateľov a pátranie po nich, a to najmä na účely ochrany pred legalizáciou príjmov z trestnej činnosti a pred financovaním terorizmu, odhaľovania nezákonných finančných operácií, súdneho konania, trestného konania, konania o priestupkoch a dohľadu nad plnením zákonom ustanovených povinností bánk a pobočiek zahraničných bánk.

3.4.3 Vnútorná kontrola a audity

i. Vyššie uvedenými ustanoveniami o zaznamenávaní komunikácie nie sú dotknuté povinnosti bánk týkajúce sa vytvorenia systému vnútornej kontroly a vnútorného auditu podľa Zákona o bankách alebo povinnosť vykonať audit alebo štatutárny audit podľa osobitných predpisov. Spracúvanie osobných údajov týkajúce sa týchto činností bánk by malo byť považované za spracúvanie osobných údajov, ktoré je nevyhnutné na splnenie zákonných povinností v bankovom sektore.

3.4.4 Testovanie IT systémov s použitím osobných údajov

i. Samotné testovanie IT systémov nepredstavuje samostatný účel spracúvania osobných údajov, nakoľko testovanie IT systémov spravidla smeruje k dosiahnutiu iného zámeru banky, pričom tento zámer môže predstavovať účel spracúvania osobných údajov. Testovaním IT systémov môže banka sledovať napr. zaistenie bezpečnosti siete alebo informačnej bezpečnosti, plnenie zmluvného vzťahu, vývoj a zlepšovanie svojich produktov a služieb, testovanie nových funkcionalít IT systémov, produktov alebo služieb, prechod alebo upgrade na novšie IT systémy, splnenie zákonných povinností týkajúcich sa napr. reportovania regulátorom alebo bezpečnostných a iných auditov alebo iné oprávnené záujmy, ktoré nie sú podmienené súhlasom dotknutých osôb so spracúvaním ich osobných údajov.

ii. Rozhodnutie banky testovať IT systémy s použitím skutočných osobných údajov by malo byť vždy založené na dôkladnom posúdení toho, do akej miery je možné splniť sledovaný účel testovania IT systémov s použitím anonymizovaných alebo fiktívnych údajov. Štandardne (*by default*), by testovanie IT systémov bánk malo prebiehať na anonymizovaných alebo fiktívnych údajoch a len v prípade, že použitie takýchto údajov by znemožňovalo alebo neprimerane komplikovalo dosiahnutie sledovaného účelu, by banky mali byť oprávnené testovať IT systémy s použitím skutočných osobných údajov. Použitie psedunymizovaných osobných údajov zmierňuje riziká pre práva a slobody fyzických osôb pri testovaní IT systémov a môže byť použité ako prvok na preukázanie súladu s GDPR v tejto súvislosti. Dosiahnutie sledovaného účelu môže byť neprimerane komplikované napr. nepresnosťou dát alebo výsledkov testovania, skreslením výsledku testovania, nezobrazením alebo zahmlením vád alebo chýb, nízkou pridanou hodnotou testovania, neprimeranými finančnými nákladmi testovania, neprimerane dlhou dobou testovania alebo podobnými faktormi, ktoré môžu byť zohľadnené v prospech použitia skutočných osobných údajov na testovanie IT systémov bánk. Vo všeobecnosti možno povedať, že čím vyššie (neskoršie) je štádium vývoja aplikácie alebo systému, tým vyššia môže byť opodstatnenosť použitia osobných údajov ako testovacích dát.

iii. Recitál č. 49 GDPR poskytuje demonštratívny výpočet spracovateľských operácií s osobnými údajmi na zaistenie bezpečnosti siete a informačnej bezpečnosti.

Uvedený recitál výslovne spomína, že dané spracúvanie osobných údajov v nevyhnutne potrebnom a primeranom rozsahu predstavuje oprávnený záujem prevádzkovateľa. Testovanie IT systémov bánk na uvedené účely takisto predstavuje oprávnený záujem bánk.

iv. V niektorých osobitných prípadoch môže banka oprávnene testovať IT systémy len vo vzťahu k nízkemu počtu dotknutých osôb, u ktorých sa zistila určitá chyba. Na zistenie príčiny a odstránenie chyby IT systémov konkrétne vo vzťahu k daným osobám je potrebné vykonať testovanie na skutočných osobných údajoch. Takéto testovanie IT systémov môže predstavovať oprávnený záujem banky.

v. Existujú prípady testovania IT systémov, kedy objektívne nie je možné dosiahnuť sledovaný zámer banky s použitím fiktívnych údajov. Táto nemožnosť môže spočívať napr. v existencii systému na detekciu (ne)konzistentnosti dát, ktorý zabráni vykonaniu alebo dokončeniu testu v testovanom prostredí alebo v nepresnosti fiktívnych údajov, ktoré nie sú naviazané na konkrétne fyzické osoby. Takýmto prípadom môže byť napr. testovanie IT systémov súvisiace s validáciou jedinečného ľudského hlasu dotknutej osoby, testovanie vzťahov medzi skutočnými osobami alebo validácia pravidiel produktov, ktoré sú naviazané na konkrétnu charakteristiku dotknutej osoby (napr. vek). V takýchto prípadoch je možné testovanie vykonať len s použitím skutočných osobných údajov.

3.4.5 Špecifické pravidlá vo vzťahu k neplnoletým osobám

i. Podľa článku 8 GDPR môže dieťa, ktoré má aspoň 16 rokov, udeliť platný súhlas so spracúvaním jeho osobných údajov v súvislosti s ponukou služieb informačnej spoločnosti, ktorá je adresovaná priamo tomuto dieťaťu, pričom ak by dieťa nemalo 16 rokov, tento súhlas musí udeliť jeho zákonný zástupca. Uvedené obmedzenie sa však nevzťahuje na spracúvanie osobných údajov dieťaťa v inej súvislosti ako je ponuka služby informačnej spoločnosti. Článok 8 ods. 3 GDPR pokračuje v tomto smere keď spresňuje, že uvedeným obmedzením nie je dotknuté všeobecné zmluvné právo členských štátov, napríklad pravidlá platnosti, uzatvárania alebo účinkov zmluvy vo vzťahu k dieťaťu.

ii. Banky môžu spracúvať osobné údaje týkajúce sa neplnoletých osôb, avšak typicky k danému spracúvania dochádza k kontexte plnení zmluvných a zákonných povinností bánk, pričom na tieto situácie sa článok 8 GDPR nevzťahuje.

iii. Ak banky postupujú podľa článku 8 GDPR, sú oprávnené spoliehať sa na pravdivosť poskytnutých informácií o veku napr. prostredníctvom čestného vyhlásenia dotknutej osoby.

3.4.6 Ďalšia analytika dát

i. Vďaka ďalšej analytike dát môžu klienti bánk využívať inovatívnejšie a personalizovanejšie produkty a služby bánk a banky môžu lepšie prispôsobiť svoj obchodný model potrebám svojich klientov. Ďalšia analytika dát môže predstavovať spracovateľskú operáciu s osobnými údajmi, pričom by sa vždy mala posudzovať ako súčasť spracúvania za vymedzeným účelom. Banky sú oprávnené využívať riešenia na ďalšiu analytiku dát v súlade so všeobecnými podmienkami spracúvania osobných údajov vyžadovaných GDPR. Banky sú oprávnené založiť

spracúvanie osobných údajov vrátane ďalšej analytiky dát vo všeobecnosti na akomkoľvek právnom základe.

ii. Na ďalšiu analytiku dát sa môžu podľa okolností konkrétneho prípadu vzťahovať osobitné podmienky podľa GDPR. Banky by pri používaní analytických modelov mali v prvom rade zohľadniť, či nedochádza k spracúvaniu osobných údajov na nové účely, o ktorých dotknuté osoby neboli informované. Pri niektorých plne automatizovaných rozhodnutiach je potrebné posúdiť aplikáciu pravidiel automatizovaného individuálneho rozhodovania podľa článku 22 GDPR. Zároveň, ak by ďalšia analytika mohla viesť k vysokým rizikám pre práva a slobody dotknutých osôb, banky by mali posúdiť aplikáciu pravidiel posúdenia vplyvu podľa článku 35 GDPR. Žiadne z týchto vyššie uvedených dodatočných podmienok sa však nevzťahuje na ďalšiu analytiku dát ako takú, len z dôvodu, že k je dochádza. Na aplikáciu týchto podmienok musia byť splnené predpoklady viažuce sa k týmto podmienkam.

iii. GDPR na viacerých miestach[5] potvrdzuje pravidlo, že právo na ochranu osobných údajov nie je absolútnym právom, ktoré musí proporcionálnym spôsobom existovať popri častokrát protichodných právach a oprávnených záujmoch prevádzkovateľov.

iv. V súlade s vyššie uvedeným prístupom GDPR k ochrane osobných údajov je aj skutočnosť, že ďalšou analytikou dát môže dochádzať k vytvoreniu k novej vrstvy dát, ktorá je kvalitnejšia a hodnotnejšia ako pôvodne vyzbierané dáta a ktorá patrí bankám ako osobám, ktoré investovali prostriedky do jej vytvorenia. Výbor (pôvodne Pracovná skupina čl. 29) nazýva tieto dáta odvodenými údajmi (tzv. *derived data*) a Európska bankova federácia ich nazýva spravovanými/odvodenými údajmi (tzv. *managed/derived data*). Oba prístupy predpokladajú, že ide stále o osobné údaje. Ak by nešlo o osobné údaje, ale o anonymné štatistické výsledky, informácie alebo údaje, na tieto sa vôbec nevzťahuje GDPR. Navyše, všetky typy dát uvedené v tomto bode môžu byť zároveň chránené ako vlastníctvo, duševné vlastníctvo alebo obchodné tajomstvo bánk.

4 Základné zásady spracúvania osobných údajov

4.1 Zásada zákonnosti, spravodlivosti a transparentnosti

4.1.1 Spracúvanie osobných údajov bankami musí byť vykonávané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe. Zákonný spôsob spracúvania znamená, že spracúvanie osobných údajov banky sa musí opierať o aspoň jeden z právnych základov. Súhlas so spracúvaním osobných údajov je len jedným z týchto právnych základov a neslúži ako univerzálny právny základ. Banky oveľa častejšie postupujú na základe právnych základov vyplývajúcich z osobitných predpisov, plnenia zmluvy a ochrany oprávnených záujmov, kedy súhlas so spracúvaním osobných údajov nie je potrebný. Banku sú oprávnené na dosiahnutie sledovaného účelu spracúvania osobných údajov postupovať na základe viacerých právnych základov súčasne.

[5] Najmä pri výnimkách z práv dotknutej osoby v článkoch 14 ods. 5, 15 ods. 4, 17 ods. 3, 20 ods. 5 a 22 ods. 2 GDPR ale výslovne aj v recitály (4): „*Právo na ochranu osobných údajov nie je absolútne právo; musí sa posudzovať vo vzťahu k jeho funkcii v spoločnosti a musí byť vyvážené s ostatnými základnými právami, a to v súlade so zásadou proporcionality.*“

4.1.2 V prípade, kedy sa banka spolieha na právny základ vyplývajúci z osobných predpisov, nie je nevyhnutné, aby daný osobitný predpis určoval presné podmienky spracúvania osobných údajov. Nie je nevyhnutné, aby osobitný predpis výslovne alebo opisným spôsobom definoval znenie účelu. Postačí, ak z daného predpisu jednoznačne vyplýva povinnosť, ktorú ma prevádzkovateľ splniť, pričom je zrejmé, že na splnenie tejto povinnosti je potrebné spracúvanie osobných údajov. Pod pojmom "právo členského štátu" v zmysle článku 6 ods. 3 je potrebné chápať nie len právne predpisy so silou zákona, ale akékoľvek všeobecne záväzné právne predpisy a teda aj medzinárodné zmluvy ratifikované Slovenskou republikou alebo Úniou ale aj niektoré podzákonné právne normy. Navyše, pre bankový sektor sú charakteristické aj niektoré právne nezáväzné normy správania vo forme odporúčaní, rozhodnutí, stanovísk alebo metodických usmernení regulátorov bankového trhu (ako napr. NBS, ECB, ESMA alebo EBA). Ak sa tieto právne nezáväzné normy správania opierajú o znenie alebo výklad povinností vyplývajúcich zo všeobecne záväzných právnych predpisov alebo by mohli napriek ich nezáväznému charakteru v prípade nedodržania znamenať pre banku akýkoľvek postih zo strany regulátora, banky sú oprávnené spracúvať osobné údaje v rozsahu nevyhnutnom na splnenie aj týchto nezáväzných noriem v režime právneho základu splnenia zákonných povinností. Právnym základom však v takom prípade nie sú dané nezáväzné normy, ale splnenie zákonnej povinnosti, ktorú dané nezáväzné normy bližšie vykladajú.

4.1.3 Ak sa banka spolieha na právny základ vyplývajúci z osobitného predpisu je možné, že účel spracúvania, ktorý tým banka sleduje, môže zároveň predstavovať aj oprávnený záujem banky alebo tretej strany podľa článku 6 ods. 1 písm. f) GDPR. Ak banka dokáže preukázať splnenie podmienok použitia právneho základu ochrany oprávnených záujmov, môže týmto spôsobom preukázať zákonnosť spracúvania osobných údajov vo väčšom rozsahu ako je nevyhnutné na splnenie zákonnej povinnosti podľa daného právneho predpisu.

4.1.4 Banky sa môžu spoliehať aj na právny základ „plnenia zmluvy", ktorý je upravený v článku 6 ods. 1 písm. b) GDPR. Pre použitie tohto právneho základu nie je rozhodujúce akú podobu, formu alebo charakter má zmluva s dotknutou osobou a zároveň tento právny základ dovoľuje spracúvať osobné údaje v rámci tzv. predzmluvných vzťahoch s dotknutou osobou (t.j. pred uzatvorením zmluvy). Pre použitie tohto právneho základu však je rozhodujúce, aký je rozsah zmluvných záväzkov banky a práv klienta ako druhej zmluvnej strany, nakoľko všetko spracúvanie osobných údajov. Od daného spracúvania je však potrebné striktne odlišovať povinnosti, ktoré bankám vyplávajú z osobitných predpisov. Pre bankový sektor je špecifické, že plnenie zmluvných vzťahov zároveň podlieha regulácií podľa osobitných predpisov. V situácii, kedy sa spracúvanie osobných údajov uskutočňuje v súvislosti s plnením zmluvy, ale je zároveň nevyhnutné na splnenie zákonnej povinnosti banky, sú banky oprávnené stanoviť, na základe ktorého z viacerých právnych základov toto spracúvanie uskutočňujú a na základe toho prispôsobiť plnenie ďalších povinností podľa GDPR. Banky sú rovnako oprávnené spracúvať osobné údaje za súčasnej existencie viacerých právnych základov.

4.1.5 Banky sa môžu pri spracúvaní osobných údajov na niektoré účely spoliehať na právny základ súhlasu dotknutej osoby so spracúvaním jej osobných údajov. Banky tak štandardne robia v prípadoch, kedy nie je možné spoľahnúť sa na iný právny základ alebo ak taký súhlas výslovne vyžadujú právne predpisy. Súhlas môže byť udelený akýmkoľvek spôsobom bez ohľadu na to, či ide o písomný, elektronický (napr. označenie políčka), zvukový alebo zvukovo-obrazový súhlas avšak vždy za dodržania podmienok uvedených v článku 7 GDPR. Súhlas musí predstavovať jasný prejav vôle, ktorý je slobodný, konkrétny, informovaný a jednoznačný. Za informovaný súhlas sa považuje aj taký súhlas, pri udeľovaní ktorého má dotknutá osoba možnosť oboznámiť

sa s ďalšími podmienkami spracúvania osobných údajov (napr. odkazom na ne), pričom v takom prípade nie je nevyhnutné, aby všetky informácie týkajúce sa daného súhlasu a zamýšľaného spracúvania boli obsiahnuté priamo v znení súhlasu. V súlade so zásadou transparentnosti by banky mali používať jednoduché, krátke a výstižné znenia súhlasov obsahujúce najmä zamýšľaný účel spracúvania a nezahlcovať znenia súhlasov informáciami, ktoré je možné poskytnúť prostredníctvom odkazu na podmienky spracúvania osobných údajov. Ak má banka povinnosť poskytnúť určité informácie pri prvej komunikácií s dotknutou osobou, môže tak urobiť odkazom na podmienky spracúvania osobných údajov. Samotné znenie súhlasu nemusí obsahovať identifikačné údaje dotknutej osoby ani prevádzkovateľa, avšak v danej situácii musí byť zjavné, kto je prevádzkovateľom získavajúcim súhlas. Táto informácia môže napríklad vyplývať zo základných informácií banky podľa článkov 13 a/alebo 14 GDPR, na ktoré odkazuje znenie súhlasu alebo súvisiaci text.

4.1.6 Zásada spravodlivého a transparentného spracúvania vyžaduje, aby dotknutá osoba bola informovaná o existencii spracovateľskej operácie a jej účeloch. Banky napĺňajú zásadu spravodlivého a transparentného spracúvania informáciami, ktoré poskytujú svojim klientom a verejnosti napr. zaslaním informácií o spracúvaní v elektronickej podobe priamo klientovi pri uzatváraní obchodného vzťahu alebo prostredníctvom podmienok spracúvania osobných údajov dostupnými na webovom sídle, na pobočkách, vo všeobecných obchodných podmienkach, v inej zmluvnej dokumentácií, v marketingových ponukách alebo v komunikácii s klientami. Napriek tomu, že niektoré z týchto informácií sú prístupne verejnosti, zásada spravodlivého a transparentného spracúvania neznamená, že banka je povinná informovať o spracúvaní osobných údajov všetky dotknuté osoby. Táto všeobecná zásada podlieha úprave informačných povinností bánk pri získavaní osobných údajov v článkoch 13 a 14 GDPR a pri žiadosti dotknutej osoby podľa článku 15 GDPR. Z týchto ustanovení vyplýva, že poskytovanie informácií dotknutým osobám nie je absolútna povinnosť bánk vo vzťahu ku všetkým dotknutým osobám vo všetkých prípadoch a situáciách a že z týchto povinností existuje viacero výnimiek odzrkadľujúcich reálne možnosti prevádzkovateľov systémov, charakter spracúvania a faktický prínos pre práva dotknutých osôb.

4.1.7 Spracúvanie osobných údajov na právnom základe ochrany oprávnených záujmov nepredstavuje nižší štandard ochrany osobných údajov ani otvorenú výnimku dovoľujúcu akékoľvek spracúvanie osobných údajov. Naopak, postup prevádzkovateľa pri posudzovaní oprávnenosti sledovaného záujmu spočívajúci z: (i) identifikácie konkrétneho sledovaného oprávneného záujmu; (ii) posúdenia proporcionality zásahu do súkromia dotknutej osoby porovnaním sledovaného oprávneného záujmu so záujmami dotknutej osoby v danom prípade (tzv. *balancing test*); a (iii) posúdenia nevyhnutnosti zamýšľaného spracúvania pre dosiahnutie sledovaného účelu predstavuje efektívny spôsob naplnenia zásady zákonnosti, spravodlivosti a transparentnosti spracúvania osobných údajov.

4.2 Zásada obmedzenia účelu

4.2.1 Zásada obmedzenia účelu vyžaduje, aby osobné údaje boli získavané na konkrétne určené, výslovne uvedené a legitímne účely a zakazuje osobné údaje ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi. V článku 6 ods. 4 GDPR upravuje tzv. test zlučiteľnosti nového účelu spracúvania s pôvodným účelom spracúvania, za ktorým boli osobné údaje získané. V aplikácií testu zlučiteľnosti však v bankovom sektore dochádza len zriedkavo, pretože banky získavajú osobné údaje súčasne na všetky účely, ktoré oznámia dotknutým osobám. Takéto spracúvanie osobných údajov –

dokonca aj tých istých osobných údajov – na viaceré účely, ktoré boli konkrétne určené, výslovne uvedené a legitímne pri ich získavaní nepodlieha testu zlučiteľnosti.

4.2.2 Niektoré účely sú automaticky považované za zlučiteľné s pôvodnými účelmi. Ide o účely archivácie vo verejnom záujme, účely vedeckého alebo historického výskumu a štatistické účely upravené v článku 89 GDPR.

4.2.3 Banka je povinná aplikovať test zlučiteľnosti iba v prípade, ak plánuje spracúvať osobné údaje na iný účel, než za akým boli osobné údaje pôvodne získané a zároveň len vtedy, ak spracúvanie nie je založené na súhlase dotknutej osoby alebo na práve Únie alebo práve členského štátu, ktoré predstavuje potrebné a primerané opatrenie v demokratickej spoločnosti na ochranu cieľov uvedených v článku 23 ods. 1 GDPR. Ak sa tento nový účel spracúvania týka existujúcich klientov banky, táto skutočnosť môže vo všeobecnosti patriť medzi okolnosti svedčiace v prospech zlučiteľnosti nového účelu v zmysle článku 6 ods. 4 písm. b) GDPR. Zlučiteľnosť nového účelu je však potrebné posudzovať s poukazom na všetky podmienky upravené v článku 6 ods. 4 GDPR a to aj s ohľadom na to, či môžu dotknuté osoby rozumne predpokladať ďalšie spracúvanie osobných údajov na nový účel.

4.3 Zásada minimalizácie údajov

4.3.1 Zásada minimalizácie údajov vyžaduje, aby banky spracúvali len také osobné údaje, ktoré sú primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. Za porušenie tejto zásady sa považuje spracúvanie osobných údajov v excesívnom rozsahu, ktoré znamená spracúvanie takých osobných údajov, ktoré nie sú potrebné na dosiahnutie účelov spracúvania. Banka by preto mala vedieť preukázať, že všetky spracúvané osobné údaje potrebuje na dosiahnutie sledovaných účelov spracúvania.

4.3.2 Zásada minimalizácie údajov však neznamená, že každá banka spracúva tie isté osobné údaje vo všeobecnosti ani tie isté údaje na dosiahnutie rovnakého účelu. Pre bankový sektor je špecifické, že regulátori bankového trhu (najmä ECB a NBS) vyžadujú od bánk využívať a zbierať čo najviac informácií pre účely splnenia zákonných povinností bánk a reportovania týchto informácií regulátorom s prihliadnutím na špecifické postavenie konkrétnej banky a činností, ktoré vykonáva. Tieto informácie nemusia ale môžu zahŕňať osobné údaje. Výsledkom regulácie bankového sektora preto môže byť odlišné nastavenie rizikového profilovania a rizikového modelu každej banky a nevyhnutne iný rozsah spracúvaných osobných údajov na dosiahnutie daných účelov. Špecifickú reguláciu bankového sektora je potrebné vnímať aj v kontexte reakcie regulátorov na finančnú krízu v roku 2008. Existuje množstvo medzinárodných, európskych a národných predpisov a štandardov, ktorých zmyslom je regulovať banky takým spôsobom, aby sa neopakovali príčiny vzniku finančnej krízy z roku 2008 a tým v konečnom dôsledku chrániť klientov bánk a verejnosť (ide napr. IFRS 9, regulácie Basel, MiFID, AnaCredit, Nariadenie o prudenciálnych požiadavkách, SSM Nariadenie, CRD, MCD a súvisiace národné predpisy ako Zákon o bankách, Zákon o burze cenných papierov a Zákon o cenných papieroch, Zákon o spotrebiteľských úveroch alebo Zákon o úveroch na bývanie). Spracúvanie osobných údajov v rozsahu, ktorý je potrebný na splnenie regulačných požiadaviek bankového sektora preto nie je porušením zásady minimalizácie údajov podľa GDPR.

4.3.3 Zásada minimalizácie údajov je okrem iného dotvorená aj povinnosťami týkajúcimi sa štandardne navrhnutej ochrany osobných údajov v článku 25 ods. 2 GDPR.

4.4 Zásada správnosti

4.4.1 Zásada správnosti vyžaduje, aby banky spracúvali správne a podľa potreby aktualizované osobné údaje, pričom musia byť prijaté potrebné opatrenia na to, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymazali alebo opravili. Zásada správnosti však nesmeruje k absolútnej objektívnej správnosti spracúvaných osobných údajov, ale k správnosti osobných údajov z hľadiska účelov, na ktoré sú dané osobné údaje spracúvané. Zásada správnosti preto predstavuje povinnosť, ktorá vyžaduje vynaloženie primeraného úsilia prevádzkovateľa na zabezpečenie správnosti spracúvaných osobných údajov a druhú stranu nezbavuje zo zodpovednosti poskytovať správne osobné údaje.

4.4.2 Žiadosť dotknutej osoby nebude úspešná ak osobné údaje napriek objektívnej nesprávnosti v čase žiadosti nebudú nesprávne z pohľadu účelov, na ktoré sa spracúvali predtým. Zásada správnosti sa preto neaplikuje smerom do minulosti a neaplikuje sa ani na prípady, kedy je aktualizácia uložených údajov právne zakázaná alebo neúčelná, keďže účel uchovávania údajov je v prvom rade zdokumentovať určité udalosti, bez ohľadu na ich objektívnu správnosť.

4.4.3 Banky sa v dobrej viere spoliehajú na to, že osobné údaje poskytnuté klientami sú pravdivé, aktuálne, úplné a správne, a to až do momentu oznámenia zmeny zo strany klienta. Medzi opatrenia, ktoré banky používajú na overenie správnosti osobných údajov patrí najmä zmluvná povinnosť klientov bánk poskytovať iba správne a aktuálne údaje a tiež napríklad povinnosť oznámiť banke ako druhej zmluvnej strane zmenu osobných údajov. Banky takisto môžu overovať správnosť osobných údajov na základe porovnania údajov napr. z bankových registrov, Sociálnej poisťovne či iných dostupných zdrojov ako aj v informácií uchovávaných, resp. inak spracúvaných bankou. Ak neexistujú iné primerané spôsoby overenia správnosti osobných údajov a klient neoznámi banke zmenu svojich údajov, banka neporuší zásadu správnosti údajov podľa GDPR tým, že pokračuje v spracúvaní. Jedným z opatrení prijatých bankou na zaistenie správnosti osobných údajov podľa článku 5 ods. 1 písm. d) GDPR môže byť aj zmluvná povinnosť klientov oznamovať banke zmenu svojich osobných údajov.

4.4.4 Za moment zistenia nesprávnosti osobných údajov sa považuje až moment úspešného overenia tejto informácie. V opačnom prípade by banky boli povinné bezodkladne vymazať aj správne osobné údaje pri podozrení o ich nesprávnosti. Banky sú preto oprávnené vykonať overenie správnosti osobných údajov napr. vyžiadaním aktualizovaných dokladov totožnosti.

4.5 Zásada minimalizácie uchovávania

4.5.1 Zásada minimalizácie uchovávania vyžaduje, aby banky uchovávali osobné údaje vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú. Vzhľadom na to, že osobné údaje sú bankami spracúvané súčasne na viacero účelov, nie je porušením tejto zásady, ak skončí jeden z účelov spracúvania, ale banka nepristúpi k vymazaniu osobných údajov z dôvodu, že tieto údaje potrebuje na iné prebiehajúce účely spracúvania. Tieto ďalšie účely môžu byť vymedzené od momentu získania osobných údajov spoločne alebo neskôr počas spracúvania v súlade so zásadou obmedzenia účelu, ktorá dovoľuje spracúvanie na ďalšie účely prostredníctvom testu zlučiteľnosti nového účelu s pôvodnými účelmi.

4.5.2 Banky by mali stanoviť interné pravidlá stanovujúce retenčné doby (doby uchovávania) osobných údajov na jednotlivé účely. Zásada minimalizácie uchovávania slúži ako pomôcka na stanovenie limitu, resp. hornej hranice retenčných dôb. Samotné retenčné doby však stanovuje prevádzkovateľ, nakoľko iba

prevádzkovateľ vie posúdiť dokedy je identifikácia dotknutých osôb potrebná na účely spracúvania osobných údajov. V niektorých prípadoch môžu retenčné doby vyplývať z osobitných predpisov alebo z oprávnených záujmov bánk alebo tretích osôb. Niektoré osobitné predpisy však stanovujú len minimálnu zákonnú dobu uchovávania (napr. uchováva najmenej 5 rokov), pričom retenčné doby môžu byť v daných prípadoch dlhšie, ak je to nevyhnutné na splnenie účelu spracúvania. Zásada minimalizácie uchovávania dovoľuje pokračovať v spracúvaní osobných údajov po uplynutí retenčných dôb na niektoré ďalšie vymedzené účely. Ide o účely archivácie vo verejnom záujme, účely vedeckého alebo historického výskumu a štatistické účely upravené v článku 89 GDPR.

4.5.3 Účely archivácie vo verejnom záujme podľa článku 89 GDPR sú bližšie upravené v Zákone o archívoch, pričom verejný záujem, ktorý sleduje tento predpis je uchovanie archívnych dokumentov, ktoré majú trvalú dokumentárnu hodnotu pre poznanie dejín Slovenska a Slovákov. Spracúvanie osobných údajov na účely archivácie vo verejnom záujme zahŕňa aj tzv. predarchivačnú činnosť. Zákon o archívoch dovoľuje bankám ako pôvodcom registratúry uchovávať došlé a vzniknuté registratúrne záznamy počas lehoty uloženia, ktorá predstavuje lehotu, počas ktorej banky potrebujú registratúrne záznamy pre svoju činnosť. Primerané lehoty uloženia môže banka stanoviť sama a je pritom oprávnená sa riadiť odporúčaniami a praxou Ministerstva vnútra SR, pričom tieto lehoty sú predmetom schválenia Slovenského národného archívu. Registratúrne záznamy môžu ale nemusia obsahovať osobné údaje dotknutých osôb vrátane kópií zmluvnej dokumentácie. Podľa GDPR sa na účely archivácie vo verejnom záujme vzťahujú primerané záruky pre práva a slobody dotknutej osoby. Uvedenými zárukami sa zaistí zavedenie technických a organizačných opatrení najmä s cieľom zabezpečiť dodržiavanie zásady minimalizácie údajov. Prijatý registratúrny poriadok a/alebo plán podľa Zákona o archívoch predstavuje také technické a organizačné opatrenia, ktoré sledujú dodržanie zásady minimalizácie. Banky by mali v podobných interných predpisoch obmedziť prístup k dokumentom uchovávaných na základe Zákona o archívoch. Ak banka postupuje podľa Zákona o archívoch, je povinná vymazať osobné údaje až vo vyraďovacom konaní podľa daného predpisu, pričom takýto postup je v súlade so zásadou minimalizácie uchovávania. Zásada minimalizácie uchovávania je okrem iného dotvorená aj povinnosťami týkajúcimi sa štandardne navrhnutej ochrany osobných údajov v článku 25 ods. 2 GDPR.

4.6 Zásada integrity a dôvernosti

Zásada integrity a dôvernosti vyžaduje, aby banky spracúvali osobné údaje spôsobom, ktorý zaručuje primeranú úroveň bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení (tzv. bezpečnostné opatrenia). Táto zásada je dotvorená ďalšími povinnosťami týkajúcich bezpečnosti osobných údajov, ktorým sa GDPR venuje v samostatnom oddiely 2 kapitoly IV, konkrétne v článkoch 32 až 34 GDPR. Zásada integrity a dôvernosti je bližšie vysvetlená v bode 8 nižšie.

4.7 Zásada zodpovednosti

4.7.1 Podľa zásady zodpovednosti sú banky zodpovedné za súlad so základnými zásadami spracúvania osobných údajov podľa článku 5 ods. 1 GDPR, pričom tento súlad musia banky vedieť preukázať. GDPR neupravuje spôsob preukazovania súladu so základnými zásadami spracúvania, ktorý je ponechaný na uvážení prevádzkovateľa. Táto zásada však smeruje výlučne voči úlohám a právomociam Úradu na ochranu

osobných údajov a neznamená, že banky by boli povinné preukazovať súlad so základnými zásadami komukoľvek inému.

4.7.2 V súlade so zásadou zodpovednosti môžu banky preukázať splnenie základných zásad spracúvania osobných údajov okrem iného napr.:

i. zavedením primeraných politík ochrany osobných údajov podľa článku 24 ods. 2 GDPR zohľadňujúc pritom prvky štandardnej a špecifickej ochrany osobných údajov podľa článku 25 GDPR;
ii. uzatvorením zmlúv so sprostredkovateľmi alebo spoločnými prevádzkovateľmi podľa článkov 26 alebo 28 GDPR;
iii. vedením záznamov o spracovateľských činnostiach podľa článku 30 GDPR;
iv. spolupracovaním s Úradom na ochranu osobných údajov pri výkone jeho úloh a právomocí podľa článku 31 GDPR;
v. prijatím primeraných bezpečnostných opatrení podľa článku 32 GDPR;
vi. vykonaním posúdenia vplyvu a prípadnej predchádzajúcej konzultácie podľa článku 35 a 36 GDPR;
vii. vzdelávaním zamestnancov v oblasti ochrany osobných údajov;
viii. vymenovania zodpovednej osoby podľa článkov 37 až 39 GDPR;
ix. dodržiavaním pravidiel a primeraných záruk pri cezhraničných prenosoch osobných údajov do tretích krajín alebo medzinárodných organizácií;
x. dodržovaním schválených certifikačných mechanizmov, pečatí alebo značiek podľa článku 42 a nasl. GDPR;
xi. dodržiavaním tohto Kódexu; alebo
xii. iným vhodným spôsobom.

5 Spracúvanie osobitných kategórií osobných údajov

5.1 Všeobecné podmienky

5.1.1 Osobitné kategórie osobných údajov (alebo tzv. citlivé osobné údaje) predstavujú podskupinu osobných údajov, na ktorú sa vzťahuje všeobecný zákaz uvedený v článku 9 ods. 1 GDPR.[6] Tento zákaz sa neuplatňuje, ak je splnená ktorákoľvek z podmienok uvedených v článku 9 ods. 2 GDPR. V praxi sú osobitné kategórie osobných údajov spracúvané na tie isté účely spoločne s bežnými osobnými údajmi. Ak sa banka spolieha na ktorúkoľvek z podmienok uvedených v článku 9 ods. 2 GDPR vo vzťahu k osobitným kategóriám osobných údajov, nevyhnutne súvisiace osobné údaje môžu byť spracúvané na ktoromkoľvek právnom základe vyplývajúcom z článku 6 GDPR alebo aj na základe článku 9 ods. 2 GDPR za podmienky, že článok 9 ods. 2 GDPR poskytuje striktnejšie a dostatočné požiadavky ako článok 6 GDPR. Napríklad, pri spoliehaní sa na výslovný súhlas podľa článku 9 ods. 2 písm. a) GDPR banka nie je povinná spoliehať sa komutatívne aj na článok 6 ods. 1 písm. a) GDPR, nakoľko daný súhlas je už súčasťou súhlasu podľa článku 9 ods. 2 písm. a) GDPR. Podľa Pracovnej skupiny čl. 29: „*Pracovná skupina čl. 29 považuje za potrebné vykonať analýzu na každom jednotlivom prípade, či samotný článok 9 GDPR vyžaduje striktnejšie a dostatočné požiadavky, alebo kumulatívna aplikácia článok 6 aj článok 9 GDPR je potrebná na zabezpečenie úplnej ochrany dotknutých osôb. V žiadnom prípade nesmie byť výsledkom posúdenia nižšia úroveň ochrany osobných údajov. To takisto znamená, že prevádzkovateľ spracúvajúci osobitnú kategóriu osobných údajov nikdy nemôže dané spracúvanie založiť výlučne na článok 6 GDPR. Tam kde je to relevantné,*

[6] Článok 9 ods. 1 GDPR: „*Zakazuje sa spracúvanie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, **biometrických údajov na individuálnu identifikáciu fyzickej osoby**, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.*“

článok 6 GDPR nebude rozhodujúci, ale bude sa aplikovať kumulatívnym spôsobom s článkom 9 GDPR pre zabezpečenie toho, že všetky relevantné záruky a opatrenia sú splnené."[7]

5.1.2 Na to, aby mohli byť akékoľvek informácie považované za osobitné kategórie osobných údajov, tieto informácie musia okrem podmienok uvedených v článku 9 ods. 1 GDPR spĺňať definíciu osobných údajov podľa článku 4 ods. 1 GDPR. Ak nejde o informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby, nemôže ísť ani o osobitné kategórie osobných údajov.

5.1.3 Rodné čísla a osobné údaje týkajúce sa uznania viny za trestné činy a priestupky sa nepovažujú za osobitné kategórie osobných údajov. Tieto osobné údaje je možné spracúvať na právnych základoch uvedených v článku 6 GDPR. Tým nie sú dotknuté dodatočné povinnosti vyplývajúce v súvislosti so spracúvaním daných osobných údajov uvedené napr. v článku 10 GDPR a § 78 ods. 4 Zákona o ochrane osobných údajov.

5.1.4 Spracúvanie fotografií by sa nemalo systematicky považovať za spracúvanie osobitných kategórií osobných údajov, pretože vymedzenie pojmu biometrické údaje sa na ne bude vzťahovať len v prípadoch, keď sa spracúvajú osobitnými technickými prostriedkami, ktoré *umožňujú alebo potvrdzujú jedinečnú identifikáciu fyzickej osoby* (napr. skenovanie tváre alebo rohovky pre overenie vstupu do chráneného priestoru). Za biometrické údaje v zmysle článku 9 ods. 1 GDPR by sa preto nemali považovať napr. záznamy z bezpečnostnej kamery, záznamy telefonickej komunikácie alebo hlasu (pokiaľ nejde o identifikáciu hlasom) alebo kópia dokladu totožnosti vrátane fotografie na danom doklade, nakoľko tieto metódy neumožňujú jedinečnú identifikáciu fyzickej osoby (t.j. nejde o spracúvanie biometrických údajov v zmysle GDPR). Banky sú navyše oprávnené spracúvať fotografie z dokladu totožnosti na základe Zákona o bankách.

5.2 Prípady spracúvania osobitných kategórií osobných údajov

5.2.1 Spracúvanie osobitných kategórií je možné vykonávať aj na základe súhlasu dotknutej osoby podľa článku 9 ods. 2 písm. a) GDPR. Rozdielom tohto súhlasu oproti „bežnému" súhlasu podľa článku 6 ods. 1 písm. a) GDPR je jeho výslovnosť. Podmienka výslovnosti smeruje k spôsobu vyjadrenia súhlasu dotknutou osobou.[8] Výslovný súhlas je opakom konkludentného súhlasu, a teda ide o súhlas, ktorý je vyjadrený výslovným právnym úkonom (napr. podpisom alebo označením políčka), pričom zároveň zo znenia alebo spôsobu vyjadrenia výslovného súhlasu je dostatočne zrejmé, že sa vzťahuje (okrem iného) aj na osobitné kategórie osobných údajov.

5.2.2 Spracúvanie osobitných kategórií osobných údajov je možné, ak je to nevyhnutné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov podľa článku 9 ods. 2 písm. f) GDPR. Banky sa môžu spoliehať na túto podmienku s cieľom preukázať, či je alebo nie je uzatvorená zmluva s klientom, či bol klient riadne identifikovaný alebo či klient dal alebo nedal banke pokyn na vykonanie určitej transakcie. Daná podmienka takisto umožňuje bankám zhromažďovať dôkazy pre účely trestného, správneho, civilného alebo iného konania. Napr. ak je pri niektorých špecifických produktoch podmienkou uzatvorenia zmluvy s bankou dobrý alebo určitý zdravotný stav klienta a neskôr sa ukáže, že klient túto podmienku už v čase uzatvorenia zmluvy nespĺňal, banka je oprávnená spracúvať údaje týkajúce sa zdravia klienta napr. prostredníctvom posudkového lekára, nakoľko také spracúvanie je vyhnuté na

[7] Pracovná skupina čl. 29 v usmernení č. 06/2014 k pojmu oprávneného záujmu prevádzkovateľa zo dňa 9. apríla 2014 používajúc analógiu medzi článkami 6 a 9 GDPR namiesto článkami 7 a 8 smernice 95/46/ES.
[8] Usmernenia Pracovnej skupiny čl. 29 k súhlasu, WP 259, str. 18.

preukázanie, uplatnenie alebo obhájenie právnych nárokov banky týkajúcich sa daného zmluvného vzťahu banky.

5.2.3 Spracúvanie osobitných kategórií osobných údajov je možné, ak je to nevyhnutné z dôvodov významného verejného záujmu na základe práva Únie alebo práva členského štátu, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu údajov a stanovujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby podľa článku 9 ods. 2 písm. g) GDPR. Takýto významný verejný záujem môže vyplývať napr. z osobitných predpisov na prechádzanie trestnej činnosti alebo inej činnosti ako napr. Zákon o ochrane pred legalizáciou z trestnej činnosti, FATCA, medzinárodných sankčných zoznamov a embárg, Trestného zákona alebo Zákona o trestnej zodpovednosti právnických osôb.

5.2.4 Banky sú oprávnené spracúvať údaje týkajúce sa zdravia, ak je to nevyhnutné na posúdenie klienta, schválenie klienta, uzatvorenie alebo plnenie zmluvy s klientom a vykonávanie platobných operácií. Tým nie je dotknutá povinnosť bánk spoliehať sa pri takom spracúvaní na jednu z podmienok uvedených v článku 9 ods. 2 GDPR alebo § 78 ods. 5 Zákona o ochrane osobných údajov.

5.2.5 Banky sú v určitých prípadoch oprávnené spracúvať o klientoch údaje týkajúce sa zdravia, najmä ak konajú ako sprostredkovatelia pre poisťovne, pobočky poisťovní z iných členských štátov alebo pobočke zahraničnej poisťovne.

5.2.6 GDPR umožňuje členským štátom zachovať alebo zaviesť ďalšie podmienky spracúvania genetických údajov, biometrických údajov alebo údajov týkajúcich sa zdravia v článku 9 ods. 4. Medzi tieto ďalšie podmienky podľa slovenského práva patrí § 78 ods. 5 Zákona o ochrane osobných údajov, ktorý umožňuje prevádzkovateľom spracúvať biometrické údaje ak tak ustanovuje osobitný predpis. Následne, Zákona o bankách výslovne dovoľuje bankám spracúvať biometrické údaje v rozsahu biometrickej charakteristiky hlasu klienta alebo zástupcu klienta banky. Osobitné predpisy môžu bankám umožniť alebo prikázať spracúvať aj iné formy biometrických údajov alebo osobitných kategórií osobných údajov bez súhlasu dotknutých osôb.

6 Práva dotknutých osôb

6.1 Vybavovanie žiadostí dotknutých osôb

6.1.1 Pri akejkoľvek žiadosti na základe práv dotknutých osôb vyplývajúcich z GDPR sú banky povinné v prvom rade identifikovať dotknutú osobu v súlade s ustanoveniami článku 12 GDPR. Banka nie je povinná konať na základe žiadosti dotknutej osoby až do kým nie je jednoznačne overená totožnosť dotknutej osoby. Dotknuté osoby sa môžu na banky obrátiť osobne na pobočke, písomne, elektronicky alebo telefonicky. V každom z týchto prípadov je však banka oprávnená požadovať poskytnutie dodatočných informácií na overenie totožnosti dotknutej osoby. Táto skutočnosť vyplýva aj z článku 12 ods. 6 GDPR, podľa ktorého ak banka má oprávnené pochybnosti v súvislosti s totožnosťou fyzickej osoby podávajúcej žiadosť môže požiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby. Banka je oprávnená v takom prípade napr. odkázať dotknutú osobu na osobné overenie prostredníctvom pobočky banky alebo na prihlásenie sa prostredníctvom aplikácie alebo internet bankingu. Tieto opatrenia na overenie totožnosti dotknutej osoby je banka povinná prijať a uplatňovať z dôvodu povinnosti chrániť bankové tajomstvo ale aj osobné údaje v zmysle GDPR.

6.1.2 Existujú situácie, kedy banky síce spracúvajú osobné údaje o dotknutých osobách, avšak spôsobom, ktorý im nedovoľuje alebo prestal dovoľovať identifikovať danú fyzickú osobu. Banky by však mali v takýchto prípadoch vyvinúť primerané úsilie na

identifikáciu dotknutej osoby, najmä ak táto osoba poskytla dodatočné informácie na overenie jej totožnosti. Ak to však nie je možné, banky sú oprávnené odmietnuť konať. Banky musia byť schopné identifikovať svojich existujúcich klientov.

6.1.3 Všeobecná lehota na vybavenie žiadosti dotknutej osoby podľa článkov 15 až 20 GDPR je jeden mesiac od doručenia žiadosti (ďalej len „mesačná lehota"). Banka je oprávnená rozhodnúť o predĺžení tejto mesačnej lehoty o ďalšie dva mesiace, pričom zohľadní komplexnosť žiadosti a celkový počet žiadostí, ktoré v danom období banka obdržala. Vždy keď banka rozhodne o predĺžení danej lehoty, je povinná informovať dotknutú osobu o každom takomto predlžení spolu s dôvodmi zmeškania lehoty v pôvodnej mesačnej lehote.

6.1.4 Ak banka neprijme opatrenia na základe žiadosti dotknutej osoby je povinná v mesačnej lehote informovať dotknutú osobu o dôvodoch nekonania a o možnosti podať sťažnosť na Úrade na ochranu osobných údajov alebo uplatniť súdny prostriedok nápravy do jedného mesiaca od doručenia žiadosti. To zahŕňa aj situácie, kedy banka neprijala opatrenia z dôvodu, že dotknutá osoba v mesačnej lehote neposkytla dodatočné informácie na overenie jej totožnosti alebo nespresnila jej príliš všeobecnú žiadosť. **Po dodatočnom poskytnutí doplňujúcich informácií zo strany dotknutej osoby začína plynúť nová mesačná lehota na vybavenie žiadosti.**

6.1.5 Banka je oprávnená z dôvodov uvedených v článku 12 ods. 5 druhej vety GDPR odmietnuť konať na základe žiadosti alebo požadovať primeraný poplatok zohľadňujúci administratívne náklady banky v súvislosti s poskytnutím informácií, oznámení alebo v súvislosti s uskutočnením požadovaného opatrenia. Primeraný poplatok zohľadňujúci administratívne náklady banky nemusí byť rovnaký u jednotlivých bánk a môže byť súčasťou cenníkov bánk. Banka môže týmto spôsobom postupovať vždy keď sú žiadosti dotknutej osoby zjavne neopodstatnené alebo neprimerané, najmä pre ich opakujúcu sa povahu. Banka je povinná v každom jednotlivom prípade posudzovať osobitne, či je žiadosť dotknutej osoby zjavne neopodstatnená alebo neprimeraná. **Odporúčaným všeobecným pravidlom ak ide o opakovanú žiadosť dotknutej osoby je, aby banka po osobitnom posúdení danej situácie uvažovala o neprimeranosti žiadosti len tam, kde medzi tými istými alebo obdobnými žiadosťami (nie doplneniami tej istej žiadosti) uplynulo menej ako 6 mesiacov.** Za zjavne neopodstatnené žiadosti dotknutej osoby sa považujú najmä také žiadosti:

i. na základe ktorých dotknutá osoba neoprávnene žiada prístup k dôverným alebo citlivým informáciám bez ohľadu na jej úmysel v súvislosti s týmito informáciami;
ii. ktoré majú výslovne šikanózny charakter voči zamestnancom banky alebo voči samotnej banke;
iii. ktoré sú vulgárne alebo obsahujú prvky rasovej, etnickej, rodovej, pohlavnej, sexuálnej alebo náboženskej nenávisti;
iv. ktoré sa týkajú informácií, ktoré banka poskytuje na základe iného všeobecne záväzného právneho predpisu (ako GDPR) alebo zmluvného vzťahu s klientom;
v. ktoré majú tak všeobecný charakter alebo sú tak nezrozumiteľné, že banka nevie z danej žiadosti posúdiť aké právo dotknutá osoba uplatňuje ani po prípadnom vyžiadaní spresnenia žiadosti;
vi. ktorými dotknutá osoba žiada informácie, oznámenia alebo na uskutočnenie opatrení, ktoré výslovne nevyplývajú z článkov 15 až 20 GDPR;
vii. ktoré smerujú opakovane k tej istej skutočnosti, ktorú banka už viacnásobne vysvetlila dotknutej osobe, pričom dotknutej osobe musí byť z okolností jasné, že odpoveď banky sa nemala prečo zmeniť;

viii. ktoré vzbudzujú podozrenie z úmyslu dotknutej osoby v súvislosti s jej žiadosťou dopustiť sa konania, ktoré by mohlo mať za následok trestnoprávnu zodpovednosť alebo škodu vzniknutú banke alebo iným osobám;

ix. pri ktorých dotknutá osoba koná agresívne, pod vplyvom alkoholu alebo omamných látok alebo ohrozuje bezpečnosť ostatných osôb nachádzajúcich sa v danom priestore.

6.1.6 Porušenie bankového tajomstva môže v osobitných prípadoch viesť k nepriaznivým dôsledkom pre práva a slobody iných, vrátane avšak nie len nepriaznivých dôsledkov pre práva a slobody klienta banky, ktorého bankové tajomstvo chráni ako aj nepriaznivých dôsledkov pre práva a slobody banky, ktorá je povinná pod hrozbou sankcie zabezpečiť, aby nedošlo k porušeniu bankového tajomstva.

6.2 Informácie poskytované dotknutým osobám

6.2.1 Banky sú oprávnené splniť si informačné povinnosti podľa článkov 13 a 14 GDPR akýmkoľvek spôsobom, bez ohľadu na formu a podobu poskytnutých informácií. Banky sa vzhľadom na okolnosti daného spracúvaniu môžu rozhodnúť pre poskytovanie týchto informácií napríklad prostredníctvom svojich webových stránok, elektronicky prostredníctvom webu, v rámci samostatného pop-up okna, fyzicky v tlačenej podobe napr. v pobočkách bánk, zverejnením vývesky alebo prostredníctvom úradnej tabule alebo nástenky, zakomponovaním do zmluvnej dokumentácie a/alebo všeobecných obchodných podmienok banky, oznámením počas telefonického rozhovoru, certifikovanými mechanizmami, značkami alebo pečaťami, zaslaním na e-mailovú alebo poštovú adresu klienta alebo ústnym alebo písomným poskytnutím zamestnancom banky, pričom zmeny týchto informácií sú banky oprávnené komunikovať akýmkoľvek uvedeným spôsobom. **Banky sú však povinné v každom prípade zverejniť aspoň základné informácie podľa článkov 13 a 14 GDPR na svojich webových sídlach, čím nie je dotknutá možnosť bánk uviesť niektoré informácie iným vhodnejším spôsobom vzhľadom na okolnosti daného prípadu bez potreby ich duplikovania na svojom webovom sídle.**

6.2.2 Informácie, ktoré majú banky poskytovať dotknutým osobám podľa článkov 13 a 14 GDPR sa neuplatňujú v situácii, kedy o dané informácie žiada dotknutá osoba na základe práva na prístup. Zásada transparentnosti si vyžaduje, aby všetky informácie a komunikácia súvisiace so spracúvaním osobných údajov boli ľahko prístupné a ľahko pochopiteľné a formulované jasne a jednoducho. Uvedená zásada sa týka najmä informácií pre dotknuté osoby o identite prevádzkovateľa a účeloch spracúvania, a ďalších informácií na zabezpečenie spravodlivého a transparentného spracúvania.

6.2.3 Na preukázanie splnenia povinnosti informovať dotknutú osobu podľa článkov 13 GDPR je rozhodujúce, či dotknutá osoba mala možnosť pri získavaní osobných údajov oboznámiť sa s týmito informáciami a nie je skutočnosť, či tak dotknutá osoba skutočne urobila, nakoľko dotknuté osoby nie sú povinné oboznamovať sa alebo čítať tieto informácie. Banka preukáže splnenie tejto povinnosti najmä existenciou interných pravidiel poskytovania daných informácií dotknutým osobám prijatých v čase získavania osobných údajov ako aj zverejnením základných informácií o spracúvaní osobných údajov podľa článkov 13 a 14 GDPR na svojom webovom sídle v zmysle bodu 6.2.1 tohto Kódexu vyššie. Nie je potrebné, aby poskytnutie základných informácií dotknutá osoba potvrdzovala napr. označením alebo podpisom.

6.2.4 Časový okamih pre splnenie informačnej povinnosti podľa článku 13 GDPR je definovaný ako "získavanie" osobných údajov resp. "pri získavaní" osobných údajov. Nie je preto potrebné splniť všetky informačné povinnosti "pred" získaním akýchkoľvek osobných údajov ale je možné tak urobiť aj počas získavania osobných údajov. Je

v súlade s GDPR posudzovať splnenie informačnej povinnosti v súlade so zavedenými procesmi bánk. Ak určitý proces banky trvá dlhšie (t.j. nie je okamžitý) a získavanie osobných údajov sa viaže na tento proces, banka by mala mať možnosť splniť svoju informačnú povinnosť podľa článku 13 GDPR kedykoľvek počas tohto procesu. Je v záujme dotknutých osôb aby mali dostatok času na oboznámenie sa s informáciami podľa článku 13 GDPR. Ak sa napríklad dotknutá osoba rozhodne otvoriť účet fyzicky v pobočke banky, je postačujúce ak má dotknutá osoba možnosť oboznámiť sa s týmito základnými informáciami kedykoľvek počas procesu otvárania účtu, napr. počas svojej prítomnosti v pobočke banky, prostredníctvom oboznámenia sa s dokumentami zaslanými na email dotknutej osoby alebo prostredníctvom webovej stránky banky. Rozhodujúca je možnosť dotknutej osoby oboznámiť sa s týmito informáciami v prípade, ak má taký záujem. Skutočnosť, že dotknutá osoba bola upovedomená o existencii a dostupnosti týchto informácií pri získavaní jej osobných údajov a dotknutá osoba sa rozhodla neoboznámiť sa s nimi nemôže byť posudzovaná ako porušenie informačnej povinnosti banky. Z tejto povinnosti existuje výnimka, a to v situácii, ak dotknutá osoba už dané informácie má.

6.2.5 Časový okamih pre splnenie informačnej povinnosti podľa článku 14 GDPR je stanovený neskoršie ako podľa článku 13 GDPR. Túto informačnú povinnosť môže banka splniť najneskôr do jedného mesiaca prípadne skorej, a to v čase prvej komunikácie banky s dotknutou osobou alebo pred prvým poskytnutím osobných údajov ďalšiemu príjemcovi. Splnenie tejto informačnej povinnosti banky môžu takisto realizovať ktorýmkoľvek spôsobom uvedeným vyššie.

6.2.6 Špecifické požiadavky vyplývajúce z § 78 ods. 6 Zákona o ochrane osobných údajov sa nepoužijú, ak je právnym základom plnenie zákonných povinností vyplývajúcich z osobitných predpisov (napr. Zákon o bankách). V prípade, kedy banka získava osobné údaje o dotknutej osoby od inej fyzickej osoby (napr. klient), aplikuje sa podľa § 78 ods. 6 Zákona o ochrane osobných údajov podmienka získať na takéto poskytnutie údajov písomný súhlas dotknutej osoby. Táto podmienka sa však neuplatňuje, ak poskytovaním týchto údajov banke klient (i) chráni svoje práva alebo právom chránené záujmy; (ii) oznamuje skutočnosti, ktoré od odôvodňujú uplatnenie právnej zodpovednosti dotknutej osoby alebo (iii) osobné údaje o danej dotknutej osobe sú spracúvané na základe osobitného predpisu (napr. Zákon o ochrane pred legalizovaním trestnej činnosti, Zákon o bankách, Zákon o platobných službách, Zákon o cenných papieroch a pod.).

6.2.7 Banka nie je povinná poskytovať základné informácie v prípadoch a situáciách predpokladaných v článku 14 ods. 5 GDPR. V bankovom sektore sa tieto prípady a situácie uplatňujú najmä vo vzťahu k neklientom. Napr., ak sú osobné údaje získavané o neklientoch na základe osobitného právneho predpisu vzťahujúceho sa na banku, banka nie je povinná oznamovať neklientom žiadne informácie podľa článku 14 GDPR. Banka je oprávnená voči neklientom argumentovať aj tým, že osobné údaje musia zostať dôverné na základe povinnosti zachovávania profesijného tajomstva (bankového tajomstva), ktoré má banka voči klientovi. Ak by banka poskytla niektoré informácie podľa článku 14 GDPR (napr. zdroj údajov o neklientovi), mohlo by tým dôjsť k porušeniu bankového tajomstva, nakoľko neklient by sa dozvedel identitu klienta. Tým nie sú dotknuté ďalšie výnimky upravené v článku 14 ods. 5 GDPR. Banka nie je povinná oznamovať informácie podľa článku 14 GDPR ani neklientom, ktorí sú odosielatelia alebo prijímatelia platobných prevodov a transakcií klientov bánk, nakoľko takéto informovanie je v zmysle článku 14 ods. 5 písm. b) GDPR nemožné alebo by si vyžadovalo neprimerané úsilie. S poukazom na druhú vetu článku 14 ods. 5 písm. b) GDPR sú banky v takýchto prípadoch povinné prijať vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby vrátane sprístupnenia daných

informácií verejnosti, čo banky zabezpečujú zverejnením základných informácií na svojich webových sídlach v zmysle bodu 6.2.1 vyššie tohto Kódexu. Týmto odsekom nie sú dotknuté situácie, kedy banka získava osobné údaje priamo od dotknutej osoby. V takom prípade platí režim článku 13 GDPR, ktorý bližšie vysvetľuje najmä bod 6.2.4 vyššie.

6.2.8 Ak sú splnené podmienky týkajúce sa možnosti oboznámenia sa dotknutých osôb so základnými informáciami aj vo vzťahu k tomuto Kódexu napríklad tým, že banky na tento Kódex výslovne odkážu v rámci základných informácií poskytovaných podľa článkov 13 a 14 GDPR a je pritom zachovaná možnosť dotknutej osoby oboznámiť sa s týmto Kódexom v rovnakej forme (písomná / elektronická) ako so základnými informáciami, banky sú oprávnené spoliehať sa pri spracúvaní osobných údajov na obsah tohto Kódexu ako na informácie, ktoré už dotknutá osoba má dispozícii.

6.2.9 Informačnou povinnosťou bánk podľa článkov 13 a 14 GDPR nie sú dotknuté povinnosti bánk poskytovať niektoré ďalšie informácie klientom alebo zástupcom klientov napr. podľa Zákona o bankách.

6.2.10 V rámci informačných povinností banky môžu spadať pod povinnosť poskytnúť informáciu o príjemcoch alebo kategóriách príjemcov osobných údajov. Podľa článku 4 ods. 9 GDPR sa za príjemcu považuje osoba, ktorej sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania sa však nepovažujú za príjemcov. Banky si splnia informačnú povinnosť podľa článku 13 a 14 GDPR tým, ak poskytnú generické informácie o kategóriách príjemcov bez uvádzania úplného zoznamu daných osôb (napr. prevádzkovatelia spoločných bankových registrov vrátane ich zamestnancov).

6.3 Právo na prístup k osobným údajom

6.3.1 Dotknutá osoba má právo žiadať banku o prístup k osobným údajov v súlade s podmienkami podľa článku 15 GDPR bližšie vysvetlenými v tomto Kódexe. Zmyslom práva na prístup je možnosť dotknutej osoby preveriť aké osobné údaje o nej spracúva banka. Právo na prístup v prvom rade zahŕňa právo dotknutej osoby získať od banky potvrdenie, či o nej banka spracúva osobné údaje. Len v prípade, že banka spracúva osobné údaje o dotknutej osoby má dotknutá osoba právo žiadať (aj v rámci jednej žiadosti aj postupne) ďalšie práva patriace pod právo na prístup, konkrétne:

i. právo na poskytnutie informácií podľa článku 15 ods. 1 a 2 GDPR;
ii. právo získať prístup[9] k osobným údajom spracúvaných bankou;
iii. právo na poskytnutie kópie spracúvaných osobných údajov.

6.3.2 Ak zo žiadosti dotknutej osoby nevyplýva, že dotknutá osoba žiada aj poskytnutie informácií podľa článku 15 ods. 1 a 2 GDPR, získanie prístupu k osobným údajom, alebo poskytnutie kópie osobných údajov podľa bodov i., ii. a iii. vyššie, je banka oprávnená takú všeobecnú žiadosť podľa článku 15 GDPR považovať len za žiadosť o potvrdenie, či sú osobné údaje o dotknutej osobe spracúvané. Ak je odpoveď banky na žiadosť o potvrdenie podľa predchádzajúcej vety pozitívna, je odporúčaným postupom bánk podľa tohto Kódexu poskytnúť dotknutej osobe spolu s odpoveďou aj odkaz na základné informácie o spracúvaní osobných údajov zverejnené na svojom webom sídle v zmysle bodu 6.2.1 tohto Kódexu vyššie.

[9] Pre odstránenie pochybností, dané právo tento Kódex označuje ako právo „získať" prístup, pričom ak tento Kódex spomína len právo na prístup, myslí tým vo všeobecnosti právo na prístup podľa článku 15 GDPR v plnom rozsahu. Právo „získať" prístup je preto významovo užší pojem ako právo na prístup.

6.3.3 Pri poskytovaní informácií podľa článku 15 ods. 1 GDPR sú banky oprávnené použiť ten istý spôsob a metódu poskytovania informácií, aký sa uplatňuje na poskytovanie informácií podľa článkov 13 a 14 GDPR. Informácie podľa článku 15 GDPR však musia byť prispôsobené okolnostiam týkajúcim sa konkrétnej dotknutej osoby (pokiaľ sa neuplatňujú výnimky z danej povinnosti). Napr. ak banky poskytujú všeobecné informácie o spracúvaní osobných údajov podľa článkov 13 a 14 GDPR, poskytujú nikomu neadresovaný prehľad účelov spracúvania, ku ktorým môže dochádzať, ale nedeklarujú, že vo vzťahu ku každej dotknutej osobe v skutočnosti dochádza k spracúvaniu osobných údajov na všetky tieto účely. Pri práve na prístup naopak banky upresňujú tieto informácie vo vzťahu ku konkrétnej dotknutej osobe a teda poskytujú informácie o účeloch spracúvania, ktoré sa týkajú tejto konkrétnej dotknutej osoby.

6.3.4 Právo získať prístup k osobným údajov v bankovom sektore je realizované najmä prostredníctvom internet bankingu a bankových aplikácií, prostredníctvom ktorých má klient banky možnosť získať prístup k jeho osobným údajom spracúvaných bankou. Banky však spracúvajú o klientoch aj ďalšie informácie, ktoré nemusia byť súčasťou internet bankingu alebo bankových aplikácií. Banky majú právo pri žiadosti o získanie prístupu odkázať dotknuté osoby na primárne tieto prostriedky prístupu, pričom ak dotknutá osoba požaduje ďalšie alebo iné osobné údaje spracúvané o nej bankou, ktoré sa nenachádzajú v týchto prostriedkoch, banky majú právo požadovať o spresnenie akých informácií alebo spracovateľských činností sa žiadosť dotknutej osoby týka.[10] Banky nemajú povinnosť poskytovať internet banking alebo bankové aplikácie, pričom v takom prípade sú povinné zabezpečiť právo získať prístup iným spôsobom, za podmienok stanovených týmto Kódexom. Ak banky spoplatňujú internet banking alebo bankové aplikácie v súlade so zmluvnými podmienkami alebo cenníkom, neznamená to, že banky sú povinné na účely zabezpečenia práva na prístup začať poskytovať dané služby zadarmo.

6.3.5 Právo získať prístupu nie je absolútnym právom dotknutej osoby a zároveň nepredstavuje právo na získanie prístupu do informačných systémov banky. Právo získať prístup podlieha výnimkám a obmedzeniam vyplývajúcim z článku 15 GDPR, ktorých uplatnenie musí banka pri každej žiadosti posúdiť individuálne. Právo na prístup a výnimky z neho bližšie vysvetľuje recitál 63 GDPR:

„*Ak je to možné, prevádzkovateľ by mal môcť poskytnúť prístup na diaľku k bezpečnému systému, ktorý by dotknutej osobe zabezpečil priamy prístup k jej osobným údajom. Uvedené právo by sa nemalo nepriaznivo dotknúť práv alebo slobôd iných osôb, ani obchodného tajomstva alebo práv duševného vlastníctva a najmä autorských práv týkajúcich sa softvéru. Výsledkom zohľadnenia týchto prvkov by však nemalo byť odmietnutie poskytnutia akýchkoľvek informácií dotknutej osobe.*“

6.3.6 Právo na poskytnutie kópie osobných údajov podľa článku 15 ods. 3 GDPR predstavuje doplnkové právo dotknutej osoby v rámci práva na prístup. Uplatnením práva na poskytnutie informácií podľa článku 15 ods. 1 GDPR banka poskytne dotknutej osobe len kategórie dotknutých osobných údajov, ktoré spracúva o konkrétnej dotknutej osobe (napr.: meno, vek). Právom na poskytnutie kópie osobných údajov podľa článku 15 ods. 3 GDPR dotknutá osoba uplatňuje právo na poskytnutie konkrétnej „hodnoty“ týchto osobných údajov (napr.: Jozef, 41). Kópie osobných údajov nemusia byť poskytované v žiadnom špecifickom štruktúrovanom formáte. Banky môžu tieto kópie poskytovať v akejkoľvek bežne používanej elektronickej podobe, pričom na žiadosť

[10] Recitál 63 GDPR: „*Ak prevádzkovateľ spracúva v súvislosti s dotknutou osobou veľké množstvo informácií,* ***mal by môcť požadovať, aby pred doručením informácií dotknutá osoba spresnila, ktorých informácií alebo spracovateľských činností sa žiadosť týka.***“

dotknutej osoby odpovedajú písomne alebo elektronicky – podľa toho ako o kópie osobných údajov žiada dotknutá osoba. Primeraný poplatok zohľadňujúci administratívne náklady banky v zmysle článku 15 ods. 3 GDPR nemusí byť rovnaký u jednotlivých bánk a môže byť súčasťou cenníkov bánk. Právo na poskytnutie kópie osobných údajov neznamená, že banka je povinná poskytovať napr. náhradné výpisy z účtov, potvrdenia k produktom alebo kópie zmlúv a dodatkov.

6.3.7 GDPR vyvažuje práva dotknutých osôb s inými často protichodnými právami iných osôb tým, že spája viaceré výnimky z práv dotknutých osôb s nepriaznivými dôsledkami na práva a slobody iných.[11] Medzi „iných" je možné v tomto zmysle zaradiť banku, iné spoločnosti patriace do skupiny danej banky, iné dotknuté osoby alebo iné osoby ako je dotknutá osoba uplatňujúca žiadosť. Banka je povinná pri každej žiadosti o prístup individuálne posúdiť, či vyhovenie žiadosti nemôže viesť k nepriaznivým dôsledkom na práva a slobody iných. To by mohlo nastať napríklad v prípade, ak by danú žiadosť uplatňoval neklient a banka by bola povinná v zmysle článku 15 GDPR poskytnúť informácie spôsobom vedúcim k porušeniu bankového tajomstva v zmysle bodu 6.1.6 tohto Kódexu vyššie.

6.3.8 Banky sú oprávnené v zmysle Zákona o platobných službách poskytovať klientom službu výpisov z účtu, pričom sú oprávnené účtovať za túto službu administratívny poplatok v zmysle platných cenníkov bánk. Skutočnosť, že zákazník má právo na prístup podľa článku 15 GDPR neznamená, že služby výpisov z účtu sú banky povinné poskytovať zadarmo.

6.4 Právo na opravu a vymazanie („zabudnutie")

6.4.1 Dotknutá osoba má právo žiadať banku o opravu nesprávnych osobných údajov, ktoré sa jej týkajú a má právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia. O tom, či sú osobné údaje neúplné z pohľadu účelov spracúvania však rozhoduje banka ako prevádzkovateľ. Banka nie je povinná doplniť osobné údaje podľa žiadosti klienta ak ich nepovažuje za potrebné pre dané účely, nakoľko banka má všeobecnú povinnosť spracúvať len tie osobné údaje, ktoré sú nevyhnutné na dané účely. Právo na opravu podľa článku 16 GDPR musí byť vykladané v súlade so zásadou správnosti podľa bodu 4.5 tohto Kódexu.

6.4.2 Právo na vymazanie osobných údajov býva verejnosťou mylne vnímané ako absolútne právo, ktorým je možné kedykoľvek dosiahnuť vymazanie všetkých osobných údajov. V skutočnosti sa právo na vymazanie aplikuje len v prípadoch vymedzených v článku 17 GDPR, ktoré nemajú všeobecnú alebo absolútnu povahu. Ak zo žiadosti dotknutej osoby ani z okolností a kontextu daného prípadu nie je zrejmé na základe akých dôvodov má prísť k požadovanému vymazaniu osobných údajov, banky sú oprávnené nevyhovieť takej žiadosti o vymazanie, čím nie je dotknutá povinnosť podľa článku 12 ods. 4 GDPR informovať dotknutú osobu o dôvodoch nekonania a možnosti podať sťažnosť dozornému orgánu a uplatniť súdny prostriedok nápravy. Banky zároveň môžu žiadať doplnenie informácií zo strany dotknutej osoby tým, že poučia v odpovedi dotknutú osobu o dôvodoch na vymazanie osobných údajov podľa článku 17 GDPR, pričom bod 6.1.4 tohto Kódexu vyššie sa použije primerane. Banky sú zároveň oprávnené odmietnuť konať na základe žiadosti o vymazanie osobných údajov, ak platí niektorý z dôvodov uvedených v článku 17 ods. 3 GDPR.

6.5 Právo na obmedzenie spracúvania

[11] Recitál 63 GDPR: „***Uvedené právo by sa nemalo nepriaznivo dotknúť práv alebo slobôd iných osôb, ani obchodného tajomstva alebo práv duševného vlastníctva a najmä autorských práv týkajúcich sa softvéru***."

Dotknutá osoba má právo žiadať u banky obmedzenie spracúvania v situáciách predpokladaných v článku 18 GDPR, pričom obsah naplnenia týchto povinností sa posudzuje primeraným spôsobom ako pri posudzovaní dôvodov na vymazanie osobných údajov vysvetlených v bode 6.4.2 vyššie. Ak sú splnené podmienky na obmedzenie spracúvania, banka je povinná pristúpiť k obmedzeniu spracúvania v primeranej lehote podľa článku 12 GDPR. Banka by mala mať možnosť v tejto lehote posúdiť, či je žiadosť opodstatnená.

6.6 Právo na prenosnosť

6.6.1 Dotknutá osoba má právo žiadať o poskytnutie osobných údajov podľa článku 20 ods. 1 GDPR len vo vzťahu k osobným údajom, ktoré:

i. sú spracúvané automatizovaným prostriedkami (t.j. elektronicky);
ii. sú spracúvané na právnom základe súhlasu alebo plnenia zmluvy (podľa článkov 6 ods. 1 písm. a) alebo b) alebo článku 9 ods. 2 písm. a) GDPR); a
iii. poskytla banke samotná dotknutá osoba.

6.6.2 Právo na prenosnosť sa nevzťahuje na osobné údaje, ktoré banky spracúvajú na iných právnych základoch ako je súhlas alebo plnenie zmluvy.[12] Pod kategórie údajov, ktoré nespadajú pod právo prenosnosť sa vzťahujú predovšetkým všetky osobné údaje spracúvané na právom základe vyplývajúcom z osobitných predpisov alebo oprávnených záujmov banky vysvetlených vyššie.

6.6.3 V súlade so stanoviskom Európskej bankovej federácie k právu na prenosnosť[13], za osobné údaje poskytnuté dotknutou osobou sa môžu považovať len tzv. surové (raw) údaje aktívne poskytnuté dotknutou osobou. Opakom takýchto údajov sú akékoľvek obohatené alebo odvodené údaje, ktoré už prešli ďalším spracúvaním bankou ako napr. verifikáciu, interným spracúvaním, bezpečnostnou kontrolou alebo analýzou. Obohatené alebo odvodené údaje – aj keď stále môžu predstavovať osobné údaje – by nepatria pod právo na prenosnosť, nakoľko tieto údaje vznikajú na základe investície bánk do sofistikovaných systémov ich spracúvania, ktorými banky poskytujú surovým dátam, ktoré poskytuje dotknutá osoba, oveľa vyššiu pridanú hodnotu a celkovo kvalitu dát. V mnohých prípadoch sa tak deje priamo v súvislosti s povinnosťami bánk podľa osobitných predpisov.

6.6.4 Na základe vyššie uvedeného, pod právo na prenosnosť nespadajú napr.:

i. údaje spracúvané na základe osobitných predpisov ako napr. Zákon o ochrane pred legalizáciou príjmov z trestnej činnosti, FATCA, Zákona o bankách, Zákon o úveroch na bývanie, Zákon o spotrebiteľských úveroch, Zákon o cenných papieroch a osobné údaje spracúvané na základe medzinárodných sankcií a tzv. čiernych listov;
ii. manuálne spracúvané osobné údaje ako napr. fotokópie dokladov totožnosti alebo písomná dokumentácia;
iii. transakčné dáta (t.j. údaje o platobných transakciách);
iv. biometrické údaje, ktoré predstavujú odvodené údaje; alebo
v. iné údaje, ktoré predstavujú odvodené údaje.

---

[12] Recitál 68 GDPR: „*Nemalo by sa uplatňovať, ak je spracúvanie založené na inom právnom základe, než je súhlas alebo zmluva. Zo samotnej povahy uvedeného práva vyplýva, že by sa nemalo uplatňovať voči prevádzkovateľom, ktorí spracúvajú osobné údaje pri výkone svojich verejných úloh.* ***Nemalo by sa preto uplatňovať, ak je spracúvanie osobných údajov potrebné na plnenie zákonnej povinnosti, ktorá sa na prevádzkovateľa vzťahuje,*** *alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi.*“

[13] Dostupné na: http://www.ebf.eu/wp-content/uploads/2017/04/EBF_025448E-EBF-Comments-to-the-WP-29-Guidelines_Right-of-data-portabi.._.pdf

6.6.5 Nakoľko osobitné predpisy môžu pojem súhlas používať aj v inom zmysle ako GDPR, za súhlas podľa článku 20 ods. 1 GDPR sa považuje len súhlas so spracúvaním osobných údajov podľa článku 6 ods. 1 písm. a) GDPR alebo podľa článku 9 ods. 2 písm. a) GDPR a nie žiadny iný typ alebo zmysel súhlasu.

6.7 Právo namietať

6.7.1 Dotknuté osoby majú právo namietať z dôvodov týkajúcich sa ich konkrétnej situácie proti spracúvaniu osobných údajov bankami na právnom základe verejného alebo oprávneného záujmu. Po prijatí žiadosti dotknutej osoby je banka povinná v lehote podľa článku 12 GDPR preukázať dotknutej osobe nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov. V prípade ak banka nie je schopná v danej lehote preukázať tieto dôvody spracúvania, nesmie od momentu uplynutia tejto lehoty ďalej osobné údaje spracúvať.

6.7.2 Dotknuté osoby majú právo namietať proti spracúvaniu osobných údajov na účely priameho marketingu, pričom v tomto prípade sú banky povinné čo najskôr v rámci svojich interných procesov a v súlade reálnymi možnosťami ukončiť namietané spracúvanie osobných údajov na daný účel.

6.8 Automatizované individuálne rozhodovanie vrátane profilovania

6.8.1 Dotknutá osoba má právo, aby sa na ňu nevťahovalo rozhodnutie banky, ktoré napĺňa nasledovné kumulatívne podmienky podľa článku 22 ods. 1 GDPR:

i. rozhodnutie je založené na výlučne automatizovanom rozhodnutí, ktoré môže zahŕňať profilovanie (t.j. nejde o rozhodnutie človeka); a
ii. rozhodnutie má právne účinky, ktoré sa dotknutej osoby týkajú alebo iné ako právne účinky, ktoré sa dotknutej osoby týkajú alebo ju podobne významne ovplyvňujú.

6.8.2 Na to, aby určité automatizované rozhodnutie dotknutú osobu významne ovplyvnilo v zmysle článku 22 GDPR, musia byť účinky spracúvania na dotknutú osobu dostatočne veľké alebo dôležité, aby boli hodné pozornosti. Inými slovami, automatizované rozhodnutie musí mať potenciál:

i. významne ovplyvniť okolnosti, správanie alebo voľby dotknutej osoby;
ii. mať dlhodobý alebo trvalý vplyv na dotknutú osobu; alebo
iii. v najextrémnejších prípadoch viesť k vylúčeniu alebo diskriminácii dotknutej osoby.[14]

6.8.3 Právo dotknutej osoby aby sa na ňu nevzťahovalo rozhodnutie napĺňajúce vyššie uvedené podmienky neznamená, že banky nemôžu obsahovo rovnaké rozhodnutie prijať voči dotknutej osobe spôsobom, ktorý nenapĺňa vyššie uvedené podmienky. Napr., ak recitál č. 71 GDPR ako príklad spadajúci pod dané rozhodovanie uvádza automatické zamietnutie online žiadosti o úver, právo dotknutej osoby podľa článku 22 GDPR neznamená, že banka je povinná dotknutej osobe úver poskytnúť. Zmyslom tohto ustanovenia je zabezpečiť, aby k automatizovanému individuálnemu rozhodovaniu podľa článku 22 ods. 1 GDPR dochádzalo iba na základe výslovného súhlasu dotknutej osoby, na základe osobitného predpisu alebo na základe plnenia zmluvy s dotknutou osobou, pričom v prípade súhlasu výslovného súhlasu a plnenia zmluvy by banky mali

[14] Usmernenia WP 29 k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679, WP 251, str. 21.

navyše zabezpečiť právo na ľudský zásah zo strany prevádzkovateľa, právo vyjadriť svoje stanovisko a právo napadnúť rozhodnutie.

6.8.4 Ako vysvetlila Európska banková federácia k pojmu automatizované individuálne rozhodovanie[15], profilovanie je bežne používané v bankovom sektore s cieľom chrániť spotrebiteľov a zabezpečiť súlad s právnymi predpismi vrátane zabezpečenia súladu so Zákonom o ochrane pred legalizovaním príjmov z trestnej činnosti, Zákonom o cenných papieroch, Zákonom o úveroch na bývanie alebo Zákonom o spotrebiteľských úveroch. Zmyslom týchto predpisov je okrem iného zabezpečiť zodpovedné poskytovanie úverov/pôžičiek takým spôsobom, aby sa jednotlivci nestávali predĺženými a zároveň predchádzať na finančnom trhu podozrivým operáciám, podvodom a financovaniu terorizmu. V týchto prípadoch sú banky oprávnené prijímať rozhodnutia spadajúce pod automatizované individuálne rozhodovanie podľa článku 22 ods. 1 GDPR a dotknutá osoba nemá právo, aby sa na ňu také rozhodnutia nevzťahovali s poukazom na výnimku uvedenú v článku 22 ods. 2 písm. b) GDPR. Vhodné opatrenia zaručujúce ochranu práv a slobôd a oprávnených záujmov dotknutej osoby podľa článku 22 ods. 2 písm. b) GDPR vyplývajú zo samotnej povahy daných predpisov, ktorých účelom je ochrana osôb, voči ktorým automatizované individuálne rozhodovania smerujú.

6.8.5 Za automatizované individuálne rozhodovanie podľa článku 22 GDPR sa nepovažuje spracúvanie osobných údajov, ktoré síce napĺňa znaky profilovania podľa článku 4 bodu 4 GDPR alebo výlučne automatizovaného spracúvania ale nemá právne účinky, ktoré sa týkajú dotknutej osoby alebo iné účinky, ktoré ju podobne významne ovplyvňujú. Takisto sa za automatizované individuálne rozhodovanie nepovažujú procesy a rozhodovania bánk, ktorých súčasťou sú aspoň čiastočne ľudské rozhodnutia alebo individuálne ľudské prehodnotenie, posúdenie alebo zásah.

7 Posúdenie vplyvu a predchádzajúca konzultácia

7.1 Posúdenie vplyvu

7.1.1 Posúdenie vplyvu predstavuje špecifickú povinnosť bánk vo vzťahu k určitým typom spracúvania osobných údajov, pri ktorých pravdepodobne hrozí vysoké riziko pre práva a slobody fyzických osôb. Zmyslom danej povinnosti je posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Banky majú všeobecnú povinnosť podľa GDPR zabezpečiť primeranú úroveň ochrany osobných údajov najmä podľa článku 32 GDPR, ktorá predstavuje všeobecný (primeraný) prístup k riadeniu rizík. Riadenie rizík však typicky smeruje k riadeniu rizík organizácie, jej aktivít a aktív. Posúdenie vplyvu je potrebné odlišovať od všeobecného riadenia rizík, nakoľko posúdenie vplyvu sa týka rizík hroziacich pre práva a slobody fyzických osôb.[16] Z týchto dôvodov nie je možné vytvoriť jednotný a všeobecný model posudzovania vplyvu pre bankový sektor, nakoľko posúdenie vplyvu môže zahŕňať skutkové posúdenia špecifické pre konkrétnu situáciu a banku, ktoré nie je možné vopred predpokladať. Banky sú preto oprávnené vykonávať posúdenie akýmkoľvek spôsobom, ktorý spĺňa požiadavky uvedené v článku 35 ods. 7 GDPR. Prístup k posudzovaniu vplyvu môže byť objektívne rozdielny medzi jednotlivými bankami aj vzhľadom na ich príslušnosť do rôznych skupín, ktoré môžu mať záujem vykladať povinnosť posúdenia vplyvu v súlade s očakávaniami

[15] Dostupné na: http://www.ebf.eu/wp-content/uploads/2017/12/EBF_029539-EBF-comments-on-WP29-guidelines-on-automated-decision-making-and-profiling.pdf

[16] Usmernenia WP 29 týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“, WP 248 rev. 01, str. 20.

hlavného dozorného orgánu a vzhľadom na rôzne metodológie posudzovania rizík, ktoré GDPR umožňuje.

7.1.2 Povinnosť vykonať posúdenie vplyvu vyplýva pre banku v prípadoch, ak sú splnené podmienky podľa článku 35 GDPR.

7.1.3 Povinnosť posúdenia vplyvu sa podľa článku 35 ods. 10 GDPR nevzťahuje na situácie, kedy banky spracúvajú osobné údaje v rámci plnenie zákonných povinností alebo verejného záujmu vyplývajúcich z práva Únie alebo členského štátu, ktoré sa nich vzťahuje, ak dané právo upravuje konkrétnu spracovateľskú operáciu alebo ich súbor a posúdenie ochrany údajov sa už vykonalo v rámci všeobecného posúdenia vplyvu v súvislosti s prijatím daného právneho základu. Banky sú oprávnené spoliehať sa minimálne na to, že primárne a sekundárne právo EÚ vrátane implementujúcich národných predpisov spĺňajú túto požiadavku. Ide predovšetkým o právo EÚ týkajúce sa ochrany finančného spotrebiteľa a integrity finančných trhov ako AML, MiFID, CCD a MCD.

7.2 Predchádzajúca konzultácia s Úradom na ochranu osobných údajov

V prípade, ak výsledkom posúdenia vplyvu je, že spracúvanie by viedlo k vysokému riziku v prípade, ak by neboli prijaté opatrenia na zmiernenie daného rizika, sú banky povinné požiadať Úrad na ochranu osobných údajov o predchádzajúcu konzultáciu.

8 Bezpečnosť osobných údajov

8.1 Primeranosť bezpečnostných opatrení

8.1.1 Tento Kódex, rovnako ako GDPR, neslúži ako technologický alebo technický štandard alebo norma bankového sektora v oblasti bezpečnosti osobných údajov alebo riadenia bezpečnosti a rizík. Táto skutočnosť je daná prierezovým charakterom GDPR ako všeobecného predpisu na ochranu osobných údajov aplikujúcim sa na širokú škálu adresátov. Pre posúdenie toho, či prevádzkovateľ poskytuje osobných údajom primeranú úroveň ochrany v súlade s GDPR je kľúčové posúdenie primeranosti prijatých bezpečnostných opatrení so zreteľom na nasledujúce okolnosti:

i. najnovšie poznatky (v angličtine: *state of the art*);
ii. náklady na vykonanie (implementáciu) opatrení;
iii. na povahu, rozsah, kontext a účely spracúvania;
iv. riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb;
(tzv. „okolnosti“).

8.1.2 Vyššie uvedené okolnosti posudzovania primeranosti prijatých bezpečnostných opatrení neprešli z pohľadu predchádzajúcej úpravy Smernice 95/46/ES žiadnymi zmenami. GDPR príkladne spomína nasledovné bezpečnostné opatrenia, ktoré môžu byť použité na preukázanie primeranej úrovne bezpečnosti osobných údajov:

i. pseudonymizáciu a šifrovanie osobných údajov;
ii. schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;
iii. schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;
iv. proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

8.1.3 Vyššie uvedené okolnosti posudzovania primeranosti ako aj príklady bezpečnostných opatrení však neznamenajú, že každá banka musí mať prijaté tie isté bezpečnostné

opatrenia. Výsledkom aplikácie týchto pravidiel GDPR môžu byť odlišné bezpečnostné opatrenia prijaté bankami, ktoré zohľadňujú konkrétne okolnosti jednotlivých bánk.

8.1.4 Banky historicky postupujú v súlade s medzinárodnými normami a štandardmi bezpečnosti (ako napr. ISO/EIS normy), ktoré sú považované za súčasť primeraných bezpečnostných opatrení. Na bankový sektor sa však vzťahujú aj pravidlá, ktoré na rozdiel od GDPR majú technickú povahu. Ide predovšetkým o technické opatrenia, ktoré sa môžu na banky vzťahovať podľa Zákona o kybernetickej bezpečnosti, Zákona o platobných službách alebo iných predpisov. Splnením týchto špecifických štandardov je vo všeobecnosti splnená aj požiadavka primeranosti bezpečnostných opatrení podľa GDPR.

8.1.5 Banky zabezpečujú primeranú úroveň bezpečnosti osobných údajov aj prispôsobovaním prostriedkov a možností spracúvania osobných údajov najnovším technologickým trendom. Používanie cloudových technológií, mobilných aplikácií, využívanie biometrie, technológie *blockchain* alebo najnovších poznatkov v oblasti spracúvania veľkých dát neznamená automaticky vyššie riziko pre dotknuté osoby. V mnohých prípadoch nové technológie poskytujú vyššiu úroveň bezpečnosti, transparentnosti a kontroly nad osobnými údajmi. Tým nie sú dotknuté povinnosti bánk súvisiace napr. s posúdením vplyvu, ak sú splnené požiadavky na uplatnenie daných povinností. Samotná skutočnosť, že použitá technológia je nová však nepredstavuje riziko pre dotknuté osoby, pričom riziko musí vyplývať z konkrétnych okolností daného prípadu. Vzhľadom na to, že spracúvanie osobných údajov by malo byť podľa recitálu č. 4 GDPR určené na to, aby slúžilo ľudstvu, GDPR ani tento Kódex nemôžu byť vykladané spôsobom, ktorý bráni technologickému vývoju bankového sektora v situáciách, kedy neexistujú riziká pre dotknuté osoby súvisiace s použitím nových technológií. Použitie najnovších poznatkov je súčasťou preukázania zásady integrity a dôvernosti osobných údajov.

8.2 Oznamovanie porušení ochrany osobných údajov

8.2.1 Banky sú povinné oznamovať porušenia ochrany osobných údajov v lehote 72 hodín. Rozhodujúcou skutočnosťou pre začiatok tejto lehoty je moment, kedy banka overí, či nastalo porušenie ochrany osobných údajov a aké môže predstavovať riziká pre práva a slobody fyzických osôb a nie zistenie, že porušenie ochrany osobných údajov mohlo nastať alebo nastalo. Banky sú povinné vykonávať overenie podľa predchádzajúcej vety bezodkladne po zistení, že porušenie ochrany osobných údajov mohlo nastať. Hodnotenie pravdepodobnosti a výšky rizika pre práva a slobody fyzických osôb prebieha na základe metodológie prijatou bankou, pričom jednotlivé banky môžu oprávnene používať iné metodológie aj vzhľadom na ich príslušnosť do rôznych skupín, ktoré môžu mať záujem používať metodológie v súlade s očakávaniami hlavného dozorného orgánu a vzhľadom na rôzne metodológie posudzovania rizík, ktoré GDPR umožňuje.

8.2.2 Pokiaľ banka nevie v danom momente oznámiť Úrad na ochranu osobných údajov všetky náležitosti porušenia súčasne, podľa článku 33 ods. 4 GDPR tak môže robiť postupne vo viacerých etapách v závislosti od objektívneho zistenia týchto informácií.

8.2.3 Ak by si oznamovanie porušenia ochrany osobných údajov dotknutým osobám vyžadovalo neprimerané úsilie (napr. veľký počet dotknutých osôb), banky môžu informovať dotknuté osoby napr. zverejnením oznámenia na svojom webovom sídle, hromadným zaslaním e-mailov alebo prostredníctvom hromadného oznamu v internet bankingu alebo bankovej aplikácii.

9 Ďalšie subjekty zapojené do spracúvania osobných údajov

9.1 Poskytovanie osobných údajov

9.1.1 V bankovom sektore bežne dochádza k poskytovaniu osobných údajov bankami ako prevádzkovateľmi iným subjektom. Vzhľadom na to, že GDPR ani Zákon o ochrane osobných výslovne nepodmieňujú poskytnutie osobných údajov inému subjektu súhlasom dotknutej osoby platí, že poskytovanie osobných údajov je spracovateľskou operáciou, ktorá môže prebiehať na akomkoľvek právnom základe dovolenom GDPR. Tým však nie sú dotknuté osobitné povinnosti podľa Zákona o bankách.

9.1.2 Banky sú v niektorých prípadoch povinné podľa osobitných predpisov poskytovať osobné údaje iným subjektom. K osobným údajom spracúvaným bankami môže mať prístup Národná banka Slovenska, Úrad na ochranu osobných údajov a ďalšie subjekty. Napr. podľa Zákona o bankách sú banky povinné na písomné vyžiadanie podať správu o záležitostiach týkajúcich sa klienta, ktoré sú predmetom bankového tajomstva (vrátane osobných údajov) bez súhlasu klienta viacerým orgánom verejnej moci.

9.2 Použitie sprostredkovateľov

9.2.1 Banky môžu použiť na spracúvanie osobných údajov sprostredkovateľov, ktorí spracúvajú osobné údaje v mene bánk. Použitie sprostredkovateľov nepodlieha súhlasu dotknutej osoby. Banky sú povinné uzatvoriť so sprostredkovateľmi zmluvu podľa článku 28 GDPR, ktorá môže byť uzatvorená akýmkoľvek preukázateľným spôsobom vrátane písomnej alebo elektronickej dohody alebo akceptáciou zmluvných podmienok zverejnených online.

9.2.2 Medzi sprostredkovateľov bánk môžu patriť aj poskytovatelia cloudových riešení. Poprední poskytovatelia cloudových riešení môžu poskytovať aj vyšší štandard bezpečnosti ako je možné dosiahnuť pri vlastnom serverovom riešení. Banky sú však povinné postupovať svedomito pri výbere poskytovateľov cloudových riešení. Pri rozhodovaní o tomto výbere by banky mali zohľadniť aj pristúpenie poskytovateľa ku kódexom správania týkajúcich sa ochrany osobných údajov, a to najmä tých kódexov správania, ktoré boli alebo budú schválené v režime GDPR. Pristúpenie ku schválenému kódexu správania zo strany poskytovateľov cloudových služieb môže byť bankami posúdené ako jeden z viacerých možných z prvkov preukazujúcich súlad daných poskytovateľov s GDPR. Bez ohľadu na vyššie uvedené, banky nesmú jednať s poskytovateľmi cloudových riešení, ktorí vykazujú výrazné znaky nesúladu s GDPR alebo nevenujú ochrane osobných údajov dostatočnú pozornosť. Banky sú v každom prípade oprávnené podľa článku 28 GDPR žiadať vykonanie auditu a poskytnutie technickej a právnej dokumentácie pre posúdenie schopnosti poskytovateľa cloudového riešenia poskytovať dostatočné záruky podľa GDPR.

9.3 Zdieľanie osobných údajov v rámci registrov

9.3.1 Zákon o bankách, Zákon o úveroch na bývanie a Zákon o spotrebiteľských úveroch dovoľujú bankám vytvoriť viaceré alebo používať bankové registre obsahujúce osobné údaje o klientoch a iných fyzických osobách a zároveň dovoľuje sprístupňovanie a poskytovanie údajov z týchto registrov medzi bankami a inými subjektami. Primárnym účelom spracúvania osobných údajov v tomto kontexte je najmä posudzovanie schopnosti klienta splácať úver. Tieto osobné údaje môžu byť spracúvané bankami aj na iné účely ako napr. prevencia podvodov v bankovom sektore, plnenie zmluvných povinností, plnenie AML povinností, na účely týkajúce sa ochrany oprávnených záujmov bánk alebo iných osôb alebo na iné účely vyplývajúce z právnych predpisov.

9.3.2 Každá banka je podľa Zákona o bankách oprávnená viesť register klientov, ktorí riadne a včas neplnia povinnosti zo zmluvných vzťahov, dopustili sa určitého konania podľa Zákona o ochrane pred legalizáciou príjmov z trestnej činnosti alebo sa na nich vzťahujú

medzinárodné sankcie. Banky sú oprávnené navzájom si vymieňať informácie z týchto registrov. Na spracúvanie osobných údajov v týchto registroch ani na poskytnutie informácií z týchto registrov iným bankám nie je potrebný súhlas dotknutej osoby so spracúvaním jej osobných údajov.

9.3.3 Banky zároveň používajú tzv. spoločný bankový register, ktorý prevádzkuje ako prevádzkovateľ spoločnosť SBCB – Slovak Banking Credit Bureau, s.r.o. ako spoločný podnik bankových služieb. Za podmienok stanovených v Zákone o bankách majú do spoločného bankového registra prístup banky ale aj iné subjekty. Medzi tieto podmienky patrí aj povinnosť získať súhlas s poskytnutím údajov do tohto registra podľa § 91 ods. 1 Zákona o bankách. Uvedený súhlas však predstavuje osobitný súhlas slúžiaci výlučne na účely prelomenia bankového tajomstva. Tento súhlas nepredstavuje právny základ spracúvania osobných údajov podľa článku 6 ods. 1 psím. a) alebo článku 9 ods. 2 písm. a) GDPR. Banky sú preto oprávnené získavať uvedený súhlas bez splnenia dodatočných povinností, ktoré na súhlas so spracúvaním osobných údajov kladie GDPR avšak za súčasnej existencie iného vhodného právneho základu spracúvania osobných údajov.

9.3.4 Banky sú v zmysle Zákona o bankách oprávnené vytvoriť aj tzv. spoločný register spotrebiteľov, ktorým bol poskytnutý základný bankový produkt. V rámci tohto registra sú banky oprávnené bez súhlasu klienta sprístupňovať a poskytovať informácie o poskytnutom základom bankovom produkte a o spotrebiteľoch vrátane ich osobných údajov.

9.3.6 Banky môžu používať na účely uvedené vyššie aj informácie z iných registrov prevádzkovaných na tieto účely zriadenými prevádzkovateľmi. Títo prevádzkovatelia sú povinní pri zbieraní osobných údajov zabezpečiť súlad s GDPR vrátane informovania dotknutých osôb o základných informáciách podľa článkov 13 alebo 14 GDPR, medzi ktoré patrí aj informácia o príjemcoch alebo kategóriách príjemcov osobných údajov. Vzhľadom na to, že prevádzkovatelia týchto registrov nie sú vo vzťahu k bankám v postavení sprostredkovateľov, banky nezodpovedajú za porušenia predpisov na ochranu osobných údajov zo strany týchto prevádzkovateľov.

10 Zodpovedná osoba

10.1 Vzhľadom na charakter spracovateľských operácií v bankovom sektore banky vo všeobecnosti spadajú pod povinnosť vymenovať zodpovednú osobu. Táto povinnosť môže byť splnená aj poverením zodpovednej osoby materskou alebo inej spoločnosťou patriacej do tej istej skupiny, ktorá dohliada aj na činnosti banky alebo pobočky banky na Slovensku. Banky sú povinné zverejniť na svojom webovom sídle kontaktné údaje zodpovednej osoby v rozsahu pozícia, email a korešpondenčná adresa avšak nie sú povinné zverejniť aj meno a priezvisko zodpovednej osoby. Banky môžu mať vymenovaných súčasne viac zodpovedných osôb, pričom funkcia zodpovednej osoby môže byť rozdelená medzi viaceré fyzické alebo právnické osoby.

10.2 Banky sú povinné vytvoriť pre zodpovedné osoby prostredie, ktoré zodpovedá postaveniu zodpovednej osoby podľa článku 38 GDPR a umožňuje plnenie úloh zodpovednej osoby podľa článku 39 GDPR. Zodpovedná osoba okrem iného poskytuje poradenstvo v oblasti ochrany osobných údajov, monitoruje súlad prevádzkovateľa s predpismi na ochranu osobných údajov, poskytuje poradenstvo v súvislosti s posúdením vplyvu, zvyšuje povedomie a odbornú prípravu personálu a je kontaktným bodom bánk v oblasti týkajúcej sa ochrany súkromia a ochrany osobných údajov vo vzťahu k dotknutým osobám a Úradu na ochranu osobných údajov.

11 Monitorovanie súladu s Kódexom

11.1 Monitorujúci subjekt

Funkciu monitorovacieho subjektu vo vzťahu k tomuto Kódexu môže vykonávať iba Slovenská banková asociácia alebo iný subjekt s jej výslovným písomným súhlasom, ktorý získal akreditáciu podľa § 87 Zákona o ochrane osobných údajov (ďalej len „**Monitorujúci subjekt**"). Banky sa musia vo Vyhlásení o pristúpení ku Kódexu zaviazať, že sa podrobia monitorovaniu dodržiavania tohto Kódexu zo strany Monitorujúceho subjektu. Vzor Vyhlásenia o pristúpení ku Kódexu, opis práv a povinností bánk v rámci daného monitorovania ako aj opis postupu Monitorujúceho subjektu pri uplatňovaní sťažností fyzických osôb sú upravené v pravidlách Monitorovacieho subjektu, ktoré musia byť schválené zo strany Úradu v rámci konania o udelení akreditácie Monitorujúcemu subjektu. Banky nie sú povinné podrobiť sa monitorovaniu dodržiavania tohto Kódexu zo strany iného monitorovacieho subjektu, ako je uvedený v tomto bode 11.[17]

11.2 Mechanizmy monitorovania

11.2.1 Každá fyzická osoba, ktorá sa cíti byť dotknutá na svojich právach v súvislosti so spracúvaním jej osobných údajov bankou sa môže kedykoľvek obrátiť na Monitorujúci subjekt so sťažnosťou.

11.2.2 Fyzické osoby nie sú oprávnené obrátiť sa na Monitorujúci subjekt so sťažnosťou v prípade, ak už podali podnet alebo návrh na začatie konania na Úrad na ochranu osobných údajov alebo na príslušný súd. V takom prípade Monitorujúci subjekt nesmie na dané podnety reagovať. Možnosť obrátiť sa na Monitorujúci subjekt nenahrádza žiadosti dotknutých osôb podľa GDPR, ktoré Monitorujúci subjekt nie je oprávnený v mene bánk vybavovať.

11.2.3 Monitorujúci subjekt je oprávnený ale nie povinný reagovať na všetky jednotlivé sťažnosti fyzických osôb. Ak sa rozhodne Monitorujúci subjekt reagovať na sťažnosť, vyjadruje sa vo všeobecnej rovine k výkladu tohto Kódexu a môže sprostredkovať fyzickej osobe kontakt na zodpovednú osobu danej banky. Odpovede, stanoviská, názory a reakcie Monitorujúceho subjektu však nie sú právne záväzné a nenahrádzajú žiadnym spôsobom povinnosti bánk voči dotknutým osobám, pričom na tieto sa nevzťahujú podmienky upravené v článku 12 GDPR.

11.2.4 Monitorovanie súladu s Kódexom zahŕňa vypracovanie a zverejnenie výročných správ Monitorujúceho subjektu týkajúcich sa dodržiavania Kódexu. V týchto výročných správach môže Monitorujúci subjekt okrem iného poukazovať na anonymné štatistické počty sťažností dotknutých osôb, spôsoby ich vybavenia a predmet týchto sťažností. Týmto spôsobom je sledovaná transparentnosť a vývoj bankového sektora z pohľadu zabezpečovania ochrany osobných údajov dotknutých osôb.

11.2.5 Týmto bodom nie sú dotknuté ďalšie povinnosti a oprávnenia Monitorujúceho subjektu vyplývajúce z GDPR, Zákona o ochrane osobných údajov prípadne z interných predpisov Monitorujúceho subjektu schválenej Úradom na ochranu osobných údajov v rámci akreditácie Monitorujúceho subjektu.

11.2.6 Ďalšie podrobnosti o mechanizmoch monitorovania upravia interné predpisy Monitorovacieho subjektu, ktoré budú v rozsahu v akom sú adresované dotknutým

[17] Ustanoveniami týkajúcimi sa monitorovania dodržiavania Kódexu správania nie sú dotknuté povinnosti Slovenskej bankovej asociácie ako prevádzkovateľa pri vybavovaní žiadostí dotknutých osôb. Opis daného postupu je upravený v interných predpisoch Slovenskej bankovej asociácie, pričom základné informácie o spracúvaní osobných údajov zo strany Slovenskej bankovej asociácie sú uvedené na jej webovom sídle.

osobám zverejnené transparentným spôsobom na webovom sídle Monitorujúceho subjektu.

12 Záverečné ustanovenia

12.1 Pre účely tohto Kódexu majú pojmy alebo skratky s veľkým začiatočným písmenom význam uvedený v Prílohe č. 1. Všetky pojmy definované v GDPR používané v tomto Kódexe sa používajú v identickom význame, ak tento Kódex výslovne neustanovuje inak. V prípade rozporu má prednosť tento Kódex. Pokiaľ kontext nevyžaduje inak, slová v jednotnom čísle obsahujú aj množné číslo a naopak.

12.2 Tento Kódex a všetky vzťahy z neho vyplývajúce sa riadia slovenským právom. Počítanie času podľa tohto Kódexu sa riadi Občianskym zákonníkom. Spory týkajúce sa tohto Kódexu je sú oprávnené rozhodovať slovenské súdy.

12.3 Znenie Kódexu bolo vypracované v súlade s GDPR a v nevyhnutnom rozsahu s osobitnými právnymi predpismi.

12.4 Akýkoľvek odkaz na GDPR znamená zároveň aj odkaz na zodpovedajúce ustanovenie Zákona o ochrane osobných údajov (a naopak) vždy podľa toho, aký právny režim sa vzťahuje na danú situáciu.

Príloha č. 1
Zoznam definícií

„**AnaCredit**“ znamená „analytical credit datasets" - analytická úverová databáza a predstavuje projekt ECB, národných centrálnych bánk krajín eurozóny a niekoľkých krajín mimo eurozóny vyhádzajúci z nariadenia Európskej centrálnej banky o zbere podrobných údajov o úveroch a kreditnom riziku (ECB/2016/13), ktorým sa vytvorí nová databáza s harmonizovanými podrobnými informáciami o jednotlivých bankových úveroch vo všetkých zúčastnených členských štátoch;

„**AML**“ znamená Anti-Money Laundering, implementáciu smernice Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorou sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 a zrušuje smernica Európskeho parlamentu a Rady 2005/60/ES a smernica Komisie 2006/70/ES;

„**CCD**“ znamená Consumer Credit Directive a implementáciu Smernice Európskeho parlamentu a Rady č. 2008/48/ES z 23. apríla 2008 o zmluvách o spotrebiteľskom úvere a o zrušení smernice Rady 87/102/EHS;

„**CRD**“ znamená Capital Requirements Directive a implementáciu Smernice Európskeho parlamentu a Rady č. 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES;

„**Civilný mimosporový poriadok**“ znamená Zákon č. 161/2015 Z. z., Civilný mimosporový poriadok;

„**Civilný sporový poriadok**“ znamená zákon č. 160/2015 Z. z., Civilný sporový poriadok;

„**EBA**“ znamená Európska banková asociácia (European Bank Association);

„**ECB**“ znamená Európska centrálna banka (European Central Bank);

„**EIOPA**“ znamená Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov (European Insurance and Occupational Pensions Authority);

„**ESRB**“ znamená Európsky výbor pre systémové riziká (European Systematic Risk Board);

„**ESFS**“ znamená Európsky systém finančného dohľadu, ktorý sa skladá z ESRB, EBA, EIOPA, ESMA, Spoločného výboru európskych orgánov dohľadu a príslušných orgánov dohľadu v členských štátoch vrátane NBS;

„**ESMA**“ znamená Európsky orgán pre cenné papiere a trhy (European Securities and Markets Authority);

„**Exekučný poriadok**“ znamená zákon č. zákon č. 233/1995 Z. z., o súdnych exekútoroch a exekučnej činnosti (Exekučný poriadok), v znení neskorších predpisov;

„**e-Money**“ znamená Smernica 2009/110/ES o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva;

„**FACTA**“ znamená zákon Spojených štátov amerických známy ako „Fair and Accurate Credit Transactions Act“, ktorý sa uplatňuje na území SR na základe medzivládnej dohody;

„**GDPR**“ znamená Nariadenie EÚ č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane osobných údajov);

„**IFRS 9**“ znamená International Financial Reporting Standard vyhlásený International Accounting Standards Board.

„**Kódex**“ znamená tento kódex správania pre spracúvanie osobných údajov v bankovom sektore;

„**Občiansky súdny poriadok**“ znamená zákon č. 99/1963 Zb. Občiansky súdny poriadok, v znení neskorších predpisov;

„**Občiansky zákonník**“ znamená zákon č. 40/1964 Zb., Občiansky zákonník, v znení neskorších predpisov;

„**Obchodný zákonník**“ znamená zákon č. 513/1991 Zb., Obchodný zákonník, v znení neskorších predpisov;

„**Nariadenie o prudenciálnych požiadavkách**“ znamená Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012

„**MCD**“ znamená Mortgage Credit Directive a implementáciu Smernice Európskeho parlamentu a Rady č. 2014/17/EÚ zo 4. februára 2014 o zmluvách o úvere pre spotrebiteľov týkajúcich sa nehnuteľností určených na bývanie a o zmene smerníc 2008/48/ES a 2013/36/EÚ a nariadenia (EÚ) č. 1093/2010;

„**MiFID**“ znamená spoločne MiFID II a MiFIR;

„**MiFID II**“ znamená Smernica Európskeho parlamentu a Rady (EÚ) č. 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ;

„**MiFIR**“ znemená Nariadenie Európskeho parlamentu a Rady (EÚ) č. 600/2014 z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorým sa mení nariadenie (EÚ) č. 648/2012;

„**NBS**“ alebo „**Národná banka Slovenska**“ znamená Národná banka Slovenska;

„NIS“ znamená Smernica Európskeho parlamentu a Rady 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii;

„**PSD2“** znamená Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES;

„**Smernica 94/46/ES**“ znamená Smernica Európskeho parlamentu a Rady č. 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov;

„**SSM Nariadenie**“ znamená Nariadenie Rady (EÚ) č. 1024/2013 z 15. októbra 2013, ktorým sa Európska centrálna banka poveruje osobitnými úlohami, pokiaľ ide o politiky týkajúce sa prudenciálneho dohľadu nad úverovými inštitúciami;

„**Správny poriadok**“ znamená zákon č. 71/1967 Zb., zákon o správnom konaní (správny poriadok), v znení neskorších predpisov;

„**Správny súdny poriadok**“ znamená zákon č. 162/2015 Z. z. Správny súdny poriadok;

„**Úrad na ochranu osobných údajov**“ znamená Úrad na ochranu osobných údajov SR;

„**Výbor**“ znamená Európsky výbor pre ochranu údajov;

„**Zákon o archívoch**“ znamená zákon č. 395/2002 Z. z. o archívoch a registratúrach, v znení neskorších predpisov;

„**Zákon o automatickej výmene informácií o finančných účtoch**“ znamená zákon č. 359/2010 Z. z., o automatickej výmene informácií o finančných účtoch na účely správy daní, v znení neskorších predpisov;

„**Zákon o bankách**“ znamená zákon č. 483/2001 Z. z., o bankách, v znení neskorších predpisov;

„**Zákon o cenných papieroch a investičných službách**“ znamená zákon č. 566/2001 Z. z., o cenných papieroch a investičných službách, v znení neskorších predpisov;

„**Zákon o dohľade nad finančným trhom**“ znamená zákon č. . 747/2004 Z. z., o dohľade nad finančným trhom, v znení neskorších predpisov;

„**Zákon o elektronických komunikáciách**“ znamená zákon č. 351/2011 Z. z. o elektronických komunikáciách;

„**Zákon o konkurze a reštrukturalizácii**“ znamená zákon č. 7/2005 Z. z., o konkurze a reštrukturalizácii, v znení neskorších predpisov;

„**Zákon o kybernetickej bezpečnosti**“ znamená prijatý zákon o kybernetickej bezpečnosti;

„**Zákon o NBS**“ znamená zákon č. 566/1992 Zb., o Národnej banke Slovenska, v znení neskorších predpisov;

„**Zákon o ochrane osobných údajov**“ znamená zákon č. 18/2018 Z. z. o ochrane osobných údajov;

„**Zákon o ochrane pred legalizáciou príjmov z trestnej činnosti**“ znamená zákon č. 297/2008 Z. z., o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov;

„**Zákon o oznamovaní protispoločenskej činnosti**“ znamená zákon č. 307/2014 Z. z. o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov;

„**Zákon o platobných službách**“ znamená zákon č. 492/2009 Z. z., o platobných službách, v znení neskorších predpisov;

„**Zákon o spotrebiteľských úveroch**“ znamená zákon č. 129/2010 Z. z. o spotrebiteľských úveroch a o iných úveroch a pôžičkách pre spotrebiteľov a o zmene a doplnení niektorých zákonov;

„**Zákon o úveroch na bývanie**“ znamená zákon č. 90/2016 Z. z., o úveroch na bývanie, v znení neskorších predpisov;

„**Zákon o platobných službách**“ znamená zákon č. 492/2009 Z. z., o platobných službách, v znení neskorších predpisov;

„**Zákon o spotrebiteľských úveroch**“ znamená zákon č. 129/2010 Z. z. o spotrebiteľských úveroch a o iných úveroch a pôžičkách pre spotrebiteľov a o zmene a doplnení niektorých zákonov;

„**Zákon zmenkový a šekový**“ znamená zákon č. 191/1950 Zb., zákon zmenkový a šekový, v znení neskorších predpisov.