

Učel spracúvania	Právny základ	Bližšie vysvetlenie účelu, súvisiacich spracovateľských operácií a sledovaných oprávnených záujmov ¹
1. Poskytovanie bankových produktov a služieb	Plnenie zmluvy, splnenie zákonnej povinnosti, súhlas a <u>oprávnený záujem</u>	<p>Spracúvanie osobných údajov na účely poskytovania bankových produktov a služieb zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky:</p> <p>Identifikácia klientov a ich zástupcov. Zahŕňa spracúvanie osobných údajov v rámci: (i) vyplnenia úvodných dotazníkov klienta vrátane základných identifikačných a kontaktných údajov klienta alebo jeho zástupcu; (ii) získavania údajov kopírovaním dokladov totožnosti klienta alebo jeho zástupcu; (iii) založenia klienta alebo aj jeho zástupcu v centrálnom systéme banky; (iv) vyžiadania a preverenia ďalších skutočností (napr. doklad preukazujúci oprávnenie zástupcu konať v mene klienta); (v) špecifikácie typu klienta (napr. FO, FO-podnikateľ, PO, maloletý klient, prípadne FO nespôsobilá na právne úkony); (v) preverenia existencie konkurzného alebo obdobného konania; (vi) opätovnej kontroly aktuálnosti údajov pri ďalších obchodoch; (vii) kontroly údajov porovnaním s dokladom totožnosti; (ix) spracúvania biometrických údajov na identifikáciu klienta; (x) postupov týkajúcich sa zmeny údajov klienta alebo jeho zástupcu.</p> <p>Bankové účty (depozitné produkty). Zahŕňa spracúvanie osobných údajov v rámci: (i) akceptácie všeobecných obchodných podmienok a uzatvorenia zmluvy viažucej sa na daný depozitný produkt; (ii) prípravy, uzatvárania a vykonávania obchodov medzi bankou a klientom, ktoré sa týkajú depozitných produktov; (iii); vytvorenia, vedenia a správy bankového účtu; (iv) <u>servisu a technickej podpory k bankovým účtom.</u></p> <p>Úverové produkty. Zahŕňa spracúvanie osobných údajov v rámci: (i) posudzovania žiadostí o úver alebo o kreditnú kartu získaných priamo od klienta alebo finančného sprostredkovateľa; (ii) preverenie klienta prostredníctvom dopytov v rámci bankových a nebankových registrov vrátane registrov tretích strán (napr. Sociálna poisťovňa); (iii) dopytovanie klienta o jeho príjme (séria otázok podľa Vyhlášky Ministerstva spravodlivosti SR); (iv) preverenie bonity klienta (jeho schopnosti splácať úver) na základe schváleného rizikového modelu banky; (v) <u>schválenie maximálneho úverového rámca na základe rizikového modelu banky;</u> (vi) uzatvárania zmluvy o úvere, hypotéke alebo kreditnej karte, vrátane akceptácie všeobecných obchodných podmienok banky; (vii) správy úverového produktu vrátane jeho načerpania a následného splácania.</p> <p>Overovanie nehnuteľností. Zahŕňa spracúvanie osobných údajov v rámci: (i) <u>overenia stavu nehnuteľnosti z viacerých zdrojov a registrov, ak je súčasťou bankového obchodu nehnuteľnosť (napr. založená nehnuteľnosť pri hypotéke);</u> (ii) <u>spracúvania osobných údajov o osobách nachádzajúcich sa na listoch vlastníctva predmetných nehnuteľností;</u> (iii) <u>vypracovania a posúdenia znaleckých posudkov k nehnuteľnostiam;</u> (iv) <u>poznania a vyhodnotenia stavu nehnuteľnosti v internom systéme banky;</u> (v) prenesenia údajov do zmluvnej dokumentácie (úverové produkty).</p> <p>Elektronické bankovníctvo. Zahŕňa spracúvanie osobných údajov v rámci: (i) bankových aplikácií a internet bankingu, a to najmä aplikácií George Slovensko, George GO Slovensko, SLSP mToken a Business 24; (ii) poskytovania bankových produktov a služieb akýmkoľvek iným vzdialeným / elektronickým spôsobom, vrátane webstránky www.slsp.sk a elektronického obchodu; (iii) postupov týkajúce sa identifikácie klientov (vyššie) v rámci digitálneho onboardingu; (iv) vytvorenia prihlasovacích a identifikačných údajov v rámci daných aplikácií; (vi) akceptácie zmluvnej dokumentácie na diaľku.</p> <p>Kolektívne investovanie (Asset Management). Zahŕňa spracúvanie osobných údajov v rámci: (i) poskytovania osobných údajov správcovskej spoločnosti Asset Management Slovenskej sporiteľne, správ. spol., a. s.; (ii) vytvorenia majetkového účtu klienta alebo zoznamu podielnikov u správcovskej spoločnosti; (iii) zadávania pokynov klienta správcovskej spoločnosti; (iv) výmeny a povinných notifikácií údajov s depozitármi cenných papierov a burzami; (v) vedenia evidencie majiteľov cenných papierov a záložných práv pre podielové listy; (vi) podpisovania dokumentácie na pobočke banky.</p> <p>Cenné papiere (Treasury). Zahŕňa spracúvanie osobných údajov v rámci: (i) získavania údajov v rámci tzv. investičných</p>

¹ Podčiarknuté časti textu predstavujú spracovateľské činnosti / operácie / oblasti, ktoré sú vykonávané v rámci sledovaných oprávnených záujmov.

dotazníkov v rozsahu otázok stanovených Vyhláškou Ministerstva financií SR z 19. decembra 2017; (ii) získavanie ďalších údajov podľa zákona o cenných papierov (napr. vrátane rodného listu); (iii) poskytovanie poradenstva klientom vo vzťahu k obchodu s cennými papiermi; (iv) evidencie obchodov klienta s cennými papiermi; (v) uchovávanie komunikácie s klientom podľa zákona o cenných papieroch; (vi) riešenia sporov s klientami podľa nariadenia EMIR; (vii) dodržiavania štandardov ISDA pri derivátových obchodoch; (viii) vedenia registra krytých dlhopisov; (iv) vykonávania pokynov klientov na zrealizovanie obchodov.

Rizikový model banky. Zahŕňa spracúvanie osobných údajov v rámci: (i) štatistického spracúvania údajov o klientoch a ich splácaní úverových produktov; (ii) vyhodnocovania rizikovosti jednotlivých obchodov; (iii) využívania štandardných a nadstavbových služieb úverových registrov; (iv) sledovania vestníkov (konkurzy, bankrotu a hlásenia); (v) generovania unikátnych identifikačných a autentifikačných kódov klienta; (vi) výpočtov a prispôbení ponúk pre konkrétnych klientov;

Platobný styk. Zahŕňa spracúvanie osobných údajov v rámci: (i) realizácie a spracovania tuzemských a zahraničných platieb vrátane kontroly správnosti zúčtovania; (ii) nevyhnutnej výmeny sprievodných údajov o platbách s bankami, poskytovateľmi platobných služieb a kartovými spoločnosťami v rámci systémov SEPA a SWIFT; (iii) vybavovania reklamácií týkajúcich sa spracovania platobných operácií; (iv) poskytovania a vyžiadania informácií o omylných platbách; (v) poskytovania platobných služieb; (vi) povinného sprístupnenia údajov tretím stranám (tzv. TPP resp. „third party providers“) v režime PSD2 (vii) povinného poskytovania údajov Národnej banke Slovenska; (viii) poskytovania údajov v rámci Skupiny Erste pri cezhraničných platbách; (ix) vnútrobankových prevodov; (x) výroby a personalizácie platobných kariet.

Finančné sprostredkovanie. Zahŕňa spracúvanie osobných údajov v rámci: (i) sprostredkovania poistenia bankových produktov a služieb (napr. poistenie úveru alebo platobnej karty), pri ktorom banka vystupuje ako finančný agent oprávnený na základe bankovej licencie; (ii) výmeny údajov so zazmluvnenými poisťovňami, ktoré poskytujú poisťné služby pre klientov banky; (iii) plnenia zákonných povinností finančného agenta v zmysle zákona o finančnom sprostredkovaní a finančnom poradenstve a ďalších predpisov.

Registre. Zahŕňa spracúvanie osobných údajov v rámci: (i) poskytovania a využívania údajov v registri bankových úverov a záruk NBS podľa § 38 zákona o bankách; (ii) vedenia vlastného registra klientov v zmysle § 92 ods. 7 zákona o bankách vrátane poskytovania údajov z tohto registra iným bankám; (iii) poskytovania a využívania údajov v rámci spoločného bankového registra podľa § 92a zákona o bankách (SBCB – Slovak Banking Credit Bureau, s.r.o.); (iv) poskytovania a využívania údajov v rámci spoločného registra spotrebiteľov základného bankového produktu v zmysle § 92b zákona o bankách; (v) poskytovania a využívania údajov v rámci registrov vytvorených podľa zákona o úveroch na bývanie a zákona o spotrebiteľských úveroch; (vi) aktualizácie, opravy a výmazu údajov v daných registroch.

Compliance. Zahŕňa spracúvanie osobných údajov v rámci: (i) vykonávania starostlivosti o zákazníka v zmysle predpisov AML; (ii) identifikácie, verifikácie a overovania skutočností podľa predpisov AML; (iii) odhaľovania a nahlasovania podozrivých finančných operácií Finančnej spravodajskej jednotke alebo iným orgánom; (iv) prijímania opatrení ako zablokovanie finančných prostriedkov alebo zdržanie platobnej operácie; (v) porovnávanie dát z rôznych medzivládnych sankčných alebo iných zoznamov; (vi) predchádzanie podvodom a podvodným operáciám na finančnom trhu; (vii) podávanie trestných oznámení alebo poskytovania súčinnosti orgánom verejnej moci v súvislosti s podozrením alebo dokazovaním podvodného konania; (viii) agregovaného spracúvania dát o škodových udalostiach v rámci kvantifikácie operačného rizika; (ix) dopytov orgánov činných v trestnom konaní; (x) zdokumentovania činnosti banky; (xi) vytvorenia systému vnútornej kontroly a vykonávania pravidelného vnútorného alebo externého auditu banky;

Starostlivosť o klienta. Zahŕňa spracúvanie osobných údajov v rámci: (i) poskytovania bežnej technickej a informačnej

		<p><u>podpory klienta prostredníctvom call centra, pobočky alebo osobného bankára; (ii) nahrávania telefonnickej komunikácie a overovania identity klienta; (iii) riešenia všeobecných podnetov, sťažností alebo reklamácií klientov; (iv) agendy ombudsmana banky, na ktorého sa môžu klienti banky obrátiť v akejkoľvek veci; (v) akejkoľvek poštovej, elektronickej telefonnickej alebo osobnej komunikácie súvisiacej s vyššie uvedenými spracovateľskými operáciami a zasielania tzv. servisných správ; (vi) spracovania a vyúčtovania akýchkoľvek poplatkov banky v zmysle platného cenníka alebo pripísania akéhokoľvek zhodnotenia (napr. úroky alebo výnosy) na účet klienta; (vii) prípravy, uzatvárania a vykonávania obchodov a zmluvných vzťahov s klientmi; (viii) správy a kontroly záväzkového vzťahu medzi klientom a bankou; (ix) poskytovania doplnkových služieb s pridanou hodnotou pre klienta banky; (x) vnútorných administratívnych činností banky alebo skupiny Erste, vrátane prenosu osobných údajov v rámci skupiny Erste na vnútorné administratívne účely vrátane spracúvania osobných údajov klientov alebo zamestnancov; (xi) získavanie spätnej väzby od klientov pre potreby skvalitňovania a prispôsobovania bankových produktov a služieb potrebám, požiadavkám a preferenciám klientov a novým trendom v bankovníctve.</u></p> <p>Prípadne dané spracúvanie zahŕňa akéhokoľvek ďalšie spracovateľské operácie, oblasti alebo postupy, ktoré banka vyhodnotí ako nevyhnutné pre splnenie účelu poskytovania bankových produktov a služieb.</p>
<p>2. Právne a zmluvné účely</p>	<p>Plnenie zmluvy a <u>oprávnený záujem</u></p>	<p>Spracúvanie osobných údajov na účely preukazovania, uplatňovania a obhajovania právnych nárokov zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky:</p> <p>Vymáhanie pohľadávok. Zahŕňa spracúvanie osobných údajov v rámci: (i) zasielania výziev a upomienok k neuhradeným platbám; (ii) <u>začatia exekučného konania; (iii) začatia súdneho konania (platobný rozkaz alebo žaloba o plnenie); (iv) postúpenia pohľadávok tretej strane; (v) právneho zastúpenia banky v daných veciach; (vi) výkonu záložného alebo zádržného práva; (vii) uzatvárania zmierov, uznaní dlhu, dohôd o urovnaní alebo splátkových kalendárov.</u></p> <p>Súdne spory, konania a dopyty. Zahŕňa spracúvanie osobných údajov v rámci: (i) <u>akýchkoľvek súdnych konaní bez ohľadu na procesné postavenie banky; (ii) akýchkoľvek správnych, trestných, priestupkových alebo iných konaní a kontrol bez ohľadu na procesné postavenie banky; (iii) poskytovania súčinnosti súdom, orgánom činným v trestnom konaní, správnym orgánom, arbitrážnym tribunálom alebo mediátorom (viď najmä § 91 ods. 4 zákona o bankách); (iv) overovania skutočností pred notárom; (v) mimosúdneho riešenia sporov (napr. arbitráž alebo mediácia); (vi) uzatvárania zmierov, uznaní dlhu, dohôd o urovnaní; (vii) zabezpečovania dôkazov pri preukazovaní právnych nárokov; (viii) komunikácie so súdmi, orgánmi verejnej moci, procesnými stranami a ich zástupcami; (ix) právneho zastúpenia a poradenstva advokátskymi kancelármi; (x) zabezpečovania znaleckých posudkov.</u></p> <p>Zmluvná agenda. Zahŕňa spracúvanie osobných údajov v rámci: (i) uzatvárania a plnenia akejkoľvek zmluvy medzi bankou a treťou stranou; (ii) schvaľovania a revízie zmlúv právnym oddelením (iii) komunikácie zmluvných strán vrátane spracúvania údajov o kontaktných osobách a štatútoch zmluvných strán; (iv) centrálnej evidencie interných aj externých plnomocenstiev; (v) centrálnej evidencie dodávateľsko-odberateľských zmluvných vzťahov medzi bankou ako podnikateľom a tretími stranami (t.j. mimo poskytovania bankových produktov a služieb).</p> <p>Správa majetku. Zahŕňa spracúvanie osobných údajov v rámci: (i) <u>správy, údržby a zhodnocovania nehnuteľného a hnutel'ného majetku banky; (ii) uzatvárania a evidencie nájomných a iných zmlúv k nehnuteľnostiam; (iii) vysporiadania majetkovo-právnych záležitostí týkajúcich sa nehnuteľností.</u></p> <p>GDPR. Zahŕňa spracúvanie osobných údajov v rámci: (i) vybavovania žiadostí dotknutých osôb a súvisiacej komunikácie; (ii) evidencie súhlasov, námietok alebo odvolaní súhlasov; (iii) získavania názorov dotknutých osôb napr. pri posúdení vplyvu;</p>

		<p>(iv) oznamovania a dokumentovania porušení ochrany osobných údajov; (v) vedenia záznamov o poučení alebo informovaní.</p> <p>Právna agenda. Zahŕňa spracúvanie osobných údajov v rámci: (i) <u>typickej agendy právneho oddelenia</u>; (ii) <u>kontroly právnych záležitostí a interného právneho poradenstva</u>; (iii) <u>nahlasovania rôznych skutočností orgánom verejnej moci (vrátane hlásenia o deliktach, trestných činoch alebo škodových/poistných udalostiach)</u>; (iv) <u>využívania právneho zastúpenia a právneho poradenstva advokátskych kancelárií</u>; (v) <u>vykonávania auditu (due dilingence) vrátane poskytovania údajov potenciálnym kupujúcim a ich poradcom napr. pri predaji podniku, akcií alebo portfólia banky</u>; (vi) <u>vedenia korporátnej agendy a plnenia všetkých povinností v zmysle obchodného zákonníka (napr. valné zhromaždenia a pozvánky, výročné správy)</u>; (vii) <u>získavania, obnovy a evidencie akýchkoľvek licencií, súhlasov, potvrdení o odbornej spôsobilosti alebo o dosiahnutom vzdelaní v rámci bežného súladu banky s právnymi predpismi.</u></p>
<p>3. Vykonávanie bezpečnostných opatrení na prevenciu pred podvodmi</p>	<p>Splnenie zákonnej povinnosti a <u>oprávnený záujem</u></p>	<p>Spracúvanie osobných údajov na účely vykonávania bezpečnostných opatrení na prevenciu pred podvodmi zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky:</p> <p>Silná autentizácia prístupov. Zahŕňa spracúvanie osobných údajov v rámci tzv. FPS systému (<i>fraud prevention system</i>): (i) implementácie a využívania silnej autentifikácie klientov (<i>SCA – strong customer authentication</i>) pri ich vstupe do desktopovej alebo mobilnej aplikácie George, internet bankingu, do vyhradeného API rozhrania umožňujúceho prepojenie s treťou stranou (<i>TPP – third party providers</i>), pri zadávaní alebo potvrdzovaní platobných príkazov alebo pri iných úkonoch na diaľku, ktoré predstavujú vysoké riziko podvodu; (ii) vytvárania, analyzovania a využívania behaviorálnych profilov klientov na podporu silnej autentizácie používateľa elektronických bankových služieb vychádzajúce z definovania a analýzy signálov odzrkadľujúcich spôsob využívania a správanie používateľa bankových aplikácií a systémov; (iv) analýzy a využívania rizikových signálov v rámci identifikácie, autentizácie a autorizácie prístupov dotknutej osoby k definovaným službám a funkcionalitám elektronického bankovníctva.</p> <p>Vykonávanie automatizovaného individuálneho rozhodovania. Ide o súbory plne automatizovaných spracovateľských operácií FPS systému, ktorých dôsledkom je povolenie alebo zamietnutie prístupu do internet bankingu alebo do mobilnej aplikácie George alebo rozhodnutie o osobitnom rizikovom posúdení a prešetrení iniciovanej transakcie, príp. zastavenie iniciovanej transakcie.</p> <p>Bezpečnosť a vývoj IT. Ide o kombinovanie a využívanie dát spracúvaných na tento účel, vrátane rizikových signálov aj na zlučiteľné účely bezpečnosti a vývoja IT pri plnení zákonných povinností podľa čl. 32 GDPR, RTS nariadenia, PSD2 smernice a zákona o bankách alebo v situáciách, keď prevažuje oprávnený záujem banky na takom spracúvaní.</p>
<p>4. Bezpečnosť a vývoj IT</p>	<p>Splnenie zákonnej povinnosti a <u>oprávnený záujem</u></p>	<p>Spracúvanie osobných údajov na účely bezpečnosti a vývoja IT zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky:</p> <p>Riadenie prístupových práv: Ide o spracúvanie osobných údajov najmä v súvislosti s (i) pridelovaním, zmenami a odoberaním prístupových práv a rolí v rámci jednotlivých systémov a aplikácií banky, čo zahŕňa využívanie „Service desk“ alebo ticketovacieho systému aj na správu interných IT záležitostí, (ii) dátová integrácia a posilňovanie autorizácie prístupov používateľov a klientov cez technologické riešenia na báze IAM (Identity Access Management), (iii) pridelovanie, zmeny, obnovovanie zabudnutých alebo kompromitovaných hesiel do interných systémov banky alebo bankových aplikácií určených pre klientov, (iv) uchovávanie údajov neaktívneho (disabled) používateľa po určité obdobie po odobratí jeho prístupových práv z hľadiska prevencie pred pokusmi o zneužitie jeho prihlasovacej identity, (v) využívanie tzv. dvojfaktorovej autentizácie prístupu dotknutej osoby v prípade potvrdzovania klientskych transakcií, či pripájania zamestnancov do internej siete banky cez VPN z cudzieho prostredia mimo banky alebo iných rizikovejších činností, (vi) využívanie osobných údajov za účelom odlišenia a verifikácie ľudského konania od útokov tzv. botov integrované do služieb internetového bankovníctva, (vii)</p>

uplatňovanie procesov viažucich sa k overovaniu stavu

Manažment bezpečnostných incidentov a vyhodnocovanie podozrivých hlásení: Ide o spracúvanie osobných údajov najmä v súvislosti s (i) manažmentom a dokumentáciou porušení ochrany osobných údajov podľa GDPR, čo môže zahŕňať oznámenie nevyhnutných osobných údajov hlavnému dozornému orgánu alebo aj spracúvanie osobných údajov dotknutej osoby, ktorej je banka povinná oznámiť porušenie ochrany osobných údajov podľa čl. 34 GDPR, (ii) Export, zabezpečenie a využívania logovacích údajov týkajúcich sa konkrétnej udalosti a do nej zainteresovaných osôb alebo priamo logovacích údajov týkajúcich sa správania konkrétneho používateľa v rozhodnom čase v rámci forenznej analýzy preskúmavajúcej príčiny a zodpovednosť za vzniknutý bezpečnostný incident

Monitorovanie používateľov a zariadení: Ide o spracúvanie osobných údajov, ktoré typicky zahŕňa rôzne systematické monitorovanie a analýzu rozmanitých dát obsahujúcich aj osobné najmä pre: (i) využívanie súboru technológií, postupov, vyčleneného odborne kvalifikovaného personálu banky v rámci SOC (Security Operation Center) pre potreby SIEM (Security Information and Event Management), čo zahŕňa hlavne bezpečnostnú analýzu tzv. podozrivých udalostí, ktoré boli systematicky vygenerované vo forme upozornení (alertov) v dôsledku spracúvania veľkého množstva údajov pochádzajúcich z rôznych zdrojov (napr. systémov, aplikácií, externých databáz zraniteľností, logov z rôznych úrovní aplikačných vrstiev využívaných informačno-komunikačných technológií banky, počítačových sietí, elektronických komunikačných metadát atď.), (ii) porovnávanie osobných údajov používateľov IT banky z osobnými údajmi, resp. dátami ktoré boli označené ako kompromitované údaje cez dôveryhodné bezpečnostné softvérové nástroje využívané bankou a ich ďalšie využívania pre zvyšovanie bezpečnosti banky a jej klientov (napr. pre zablokovanie emailov zneužívaných na phishingové útoky, kompromitované čísla kreditných kariet využívané existujúcim klientom, kompromitované databázy údajov ponúkané na predaj na darkwebe a pod.), (iii) generovanie tzv. logovacích údajov monitorujúcich správanie používateľov IT banky do vnútra banky (napr. vo vzťahu k zamestnancom, oprávneným pracovníkom dodávateľov) ako aj navonok (napr. vo vzťahu ku klientom využívajúcim bankové služby, novým používateľom sťahujúcim bankové aplikácie apod.) na všetkých úrovniach systémov, aplikácií, sietí, ktoré to technicky umožňujú, (iv) využívanie „anti-theft“ funkcionalít umožňujúcich na základe emailového konta zamestnanca vymazanie obsahu pracovnej elektronickej pošty dostupnej v prenosnom mobilnom zariadení (smartfón) na diaľku cez internet v prípade jeho straty alebo odcudzenia, (v) monitorovanie zdieľania elektronických súborov osobitne privilegovanými používateľmi, ktorým boli zverené aj prístupové práva k externým dátovým úložiskám preverených sprostredkovateľov

Profilovanie a využívanie AI technológií: Ide o spracúvanie osobných údajov, ktoré typicky zahŕňa: (i) sprístupnenie aplikácií používateľovi na základe hodnotenia digitálnych rizík a prípadne dočasné zablokovanie zariadenia v prípade prítomnosti väčšieho množstva rizikových signálov alebo zadaných hrozieb, ktoré sa môžu v čase dynamicky meniť a prispôbovať (napr. prihlasovanie sa z neštandardnej IP adresy / krajiny, mimo pracovného času, z neznámeho zariadenia) (tzv. zero trust koncept), (ii) definovanie rizikových kritérií a udalostí spojené s automatizovaným vyhodnocovaním a analýzou veľkého objemu dát a osobných údajov s cieľom automatizovane generovať upozornenia (alerty) pre bezpečnostný personál, čo môže byť rozvíjané aj cez metódy tzv. strojového učenia (machine learning) začlenené do umelej inteligencie začleňovanej do niektorých externých softvérových bezpečnostných riešení, ktoré banka využíva.

Vývoj, vylepšovanie a testovanie IT: Ide o spracúvanie osobných údajov, ktoré typicky zahŕňa: (i) spracúvanie osobných údajov potrebné na vývoj, vylepšovanie alebo testovanie interných bankových systémov, aplikácií, ich funkcionalít vrátane vývoja, vylepšovania a testovania technických bezpečnostných opatrení s ohľadom na aktuálny stav poznania a technologický vývoj, (ii) spracúvanie osobných údajov, ktoré je nevyhnutné pre vykonávanie interných kontrolných auditov, penetračných testov, či bezpečnostných auditov pre potreby ISO certifikácie, ktoré sú určené na overovanie funkčnosti, spoľahlivosti a primeranosti aplikovaných bezpečnostných opatrení.

		<p>Využívanie dát spracúvaných FPS systémom: Ide o kombinovanie a využívanie dát spracúvaných na účel vykonávania bezpečnostných opatrení na prevenciu pred podvodmi, vrátane rizikových signálov aj na zlučiteľné účely bezpečnosti a vývoja IT pri plnení zákonných povinností banky ako prevádzkovateľa podľa čl. 32 GDPR.</p> <p>Zlučiteľné spracúvanie na účely preukazovania, obhajovania a uplatňovania právnych nárokov: ide o spracúvanie osobných údajov, ktoré typicky okrem iného pokrýva nasledovné operácie, oblasti a postupy banky: (i) nevyhnutné spracúvanie, ktoré je súčasťou preukazovania prijatých bezpečnostných opatrení a ich praktického dodržiavania vo vzťahu ku hlavnému dozornému orgánu a dotknutým dozorným orgánom vykonávajúcim dozorné aktivity pri spracúvaní osobných údajov nad skupinou našej banky, (ii) nevyhnutné spracúvanie, ktoré nastáva pri vykonávaní bezpečnostných auditov, ak je banka v postavení sprostredkovateľa a prevádzkovateľ požadoval vykonať audit, (iii) spracúvanie osobných údajov, ktoré je nevyhnutné vykonať pri bezpečnostnom preverovaní a auditoch sprostredkovateľov banky, ak to nie je možné s ohľadom na povahu, kontext a účely realizovať bez potreby spracúvania osobných údajov (iv) využívanie dát vzniknutých v dôsledku aplikovania bezpečnostných opatrení (napr. logov) pri odpovedaní na žiadosti dotknutých osôb súvisiacich s uplatňovaním ich práv podľa GDPR, (v) poskytovanie osobných údajov spracúvaných na účel bezpečnosti a vývoja IT v rámci žiadosti o poskytovanie súčinnosti iným útvarom banky, ktoré sú zodpovedné za vybavovanie žiadostí orgánov verejnej moci pri plnení ich zákonných úloh (napr. súdy, orgány činné v trestnom konaní).</p>
5. Oznamovanie protispoločenskej činnosti (tzv. whistleblowing)	Splnenie zákonnej povinnosti	Spracúvanie osobných údajov na účely oznamovania protispoločenskej činnosti zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky: (i) vykonávanie úkonov spojených s ochranou oznamovateľa protispoločenskej činnosti zamestnávateľom podľa § 7 zákona č. 54/2019 Z. z. (ii) prijímanie, vyhodnocovanie a evidovanie oznámení v rámci vnútorného systému preverovania oznámení, vrátane uchovávanie evidencie došlých oznámení po dobu 3 rokov, (iii) zaznamenávanie zvukových záznamov z telefonických hovorov došlých na osobitne zriadenú telefonickú linku určenú na oznamovanie protispoločenskej činnosti (tzv. whistleblowing hotline).
6. Účtovné a daňové účely	Splnenie zákonnej povinnosti	Spracúvanie osobných údajov na účtovné a daňové účely zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky: (i) evidencia a využívanie účtovných dokladov § 35 zákona č. 431/2002 Z. z. o účtovníctve a o zmene a doplnení niektorých zákonov; (ii) uchovávanie faktúr podľa § 76 ods. 1 zákona č. 422/2004 Z. z. o dani z pridanej hodnoty; (iii) akékoľvek spracúvanie osobných údajov potrebné pre plnenie povinností platiteľa dane podľa zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov, (iv) akékoľvek spracúvanie osobných údajov potrebné pre plnenie povinností daňového subjektu podľa zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov, (v) spracúvanie osobných údajov potrebné na plnenie zákonných povinností podľa zákona č. 359/2015 Z.z. o automatickej výmene informácií o finančných účtoch na účely správy daní, čo môže zahŕňať poskytovanie osobných údajov spojených s finančnými účtami vedenými v banke orgánom správy daní v iných členských štátoch EÚ alebo Spojených štátov Amerických na základe dohody medzi Slovenskou republikou a Spojenými štátmi americkými na zlepšenie dodržiavania medzinárodných predpisov v oblasti daní a na implementáciu zákona FATCA vrátane jej príloh
7. Ochrana majetku a osôb	<u>Oprávnený záujem</u> a splnenie zákonnej povinnosti	Spracúvanie osobných údajov na účely ochrany majetku a osôb zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky: Kamerové systémy. Ide o monitorovanie (i) <u>priestorov prístupných verejnosti v definovaných objektoch banky, vrátane siete pobočiek banky</u> (ii) bankomatov a zmenárenských miest (§ 93a ods. 7 Zákona o bankách) prostredníctvom kamerových systémov.

		<p><u>Systémy na kontrolu a evidenciu vstupov do definovaných priestorov banky.</u> Ide o (i) monitorovanie a využívanie údajov o vstupoch zamestnancov a návštevníkov banky vstupujúcich do definovaných chránených priestorov ako sú napr. vymedzené miesta na pobočkách, centrále, pokladnice, parkoviská, bankomaty, trezory alebo vyhradené priestory (budovy) banky, čo môže zahŕňať aj kontrolu fotografie zamestnanca integrovanej do čipovej karty, (ii) spracúvanie limitovaných údajov zo strojov-čitateľnej časti občianskeho preukazu (meno, priezvisko, číslo dokladu totožnosti) automatizovaným spôsobom a ich doplnenie o údaje týkajúce sa času vstupu a času odchodu vo vzťahu k návštevníkom určitých objektov banky</p> <p><u>GPS monitoring firemných vozidiel.</u> Ide o monitorovanie geolokalizácie služobných vozidiel banky využívaných v súvislosti s plnením pracovných úloh, či prevozom finančnej hotovosti, pričom je možné sledovať aj pohyb a okamžitú lokalizáciu monitorovaného vozidla v reálnom čase. Súkromné jazdy oprávnených zamestnancov môžu byť monitorované iba ak sa zamestnanec sám dobrovoľne rozhodne nezamedziť takémuto monitorovaniu (t.j. neaktivuje systémovú funkciu cez tlačidlo vo vozidle, o ktorom bol/a preukázateľne poučený) a zároveň udelí banke na takéto monitorovanie osobitný špecifický informovaný súhlas so spracúvaním osobných údajov, ktorého neudelenie nemá na zamestnanca žiadny negatívny vplyv.</p> <p><u>Využívanie súkromných bezpečnostných služieb.</u> Ide o akékoľvek spracúvanie osobných údajov, ktoré je nevyhnutné pre riadne plnenie zmluvných vzťahov medzi bankou a súkromnými bezpečnostnými službami, ktoré poskytujú banke svoje služby v oblasti bezpečnosti, čo typicky zahŕňa najmä: (i) spracúvanie osobných údajov pracovníkov SBS a overovanie ich identity pri vykonávaní úkonov spojených s manipuláciou s finančnou hotovosťou, (ii) iné poskytovanie služieb SBS, pri ktorom je nevyhnutné spracúvať osobné údaje v súvislosti so zabezpečením ochrany osôb a majetku v mene banky (napr. sprevádzanie zamestnancov banky na dražby, exekúcie, rizikové súdne pojednávania, či vykonávanie strážnej služby v definovaných objektoch banky).</p>
<p>8. Marketingové a PR účely</p>	<p>Súhlas a <u>oprávnený záujem</u></p>	<p>Spracúvanie osobných údajov na marketingové účely a PR účely zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky:</p> <p><u>Cielená reklama (priamy marketing).</u> Zahŕňa spracúvanie osobných údajov v rámci: (i) tvorby, prispôsobovania a zasielania marketingovej elektronickej pošty (e-mail, SMS, push-notifikácie); (ii) tvorby, prispôsobovania a zasielania letákov alebo tlačných adresných foriem marketingu; (iii) tvorby, prispôsobovania a zobrazovania reklamy na sociálnych sieťach; (iv) tvorby, prispôsobovania a zobrazovania bannerovej reklamy; (v) tvorby, prispôsobovania a zobrazovania ponúk v rámci aplikácie alebo internet bankingu; (vi) profilovania správania klienta v rámci online marketingu.</p> <p><u>Využívanie marketingových nástrojov.</u> Zahŕňa spracúvanie osobných údajov v rámci: (i) analýzy návštevnosti, úspešnosti a konverzie (napr. prostredníctvom nástrojov Google Analytics, Facebook Ads Manager a pod.); (ii) využívania pluginov sociálnych sietí alebo tretích strán (ako napr. FB/Google Login); (iii) identifikácie klienta pri prihlásení sa do chránenej zóny; (iv) používania rôznych analytických nástrojov na báze súborov cookies, pixelov, SDK, web beacons a pod., tak ako sú vysvetlené v rámci „cookies policy“ banky; (v) realizácie marketingových prieskumov a ankiet.</p> <p><u>Zvyšovanie povedomia a dobrého mena (PR).</u> Zahŕňa spracúvanie osobných údajov v rámci: (i) vedenia profilov banky / skupiny SLSP na sociálnych sieťach a súvisiaca interakcia s užívateľmi; (ii) organizovania podujatí, vrátane vyhotovovania foto a video záznamov; (iii) zverejňovania obsahu, foto alebo video záznamov v rámci sociálnych sietí; (iv) zvyšovania povedomia a dobrého mena (PR účely); (v) organizovania spotrebiteľských súťaží vrátane partnerských súťaží.</p>

9. Statistické účely	Právny základ pôvodných účelov v zmysle čl. 89 GDPR	Spracúvanie osobných údajov na štatistické účely zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky: (i) zostavovanie štatistických výstupov, výkazov, hlásení, správ, analýz a rôznych pracovných a analytických podkladov potrebných pre interné štatistické účely banky ako aj pre štatistické účely Národnej banky Slovenska, iných štátnych orgánov a právnických osôb, (ii) vytváranie anonymizovaných a agregovaných štatistických údajov z osobných údajov spracúvaných na iné legitímne účely spracúvania osobných údajov, ktoré majú právny základ a o ktorých boli dotknuté osoby riadne informované v súlade s recitálom 50 a čl. 89 GDPR.
10. Archivácia vo verejnom záujme	Splnenie zákonnej povinnosti, prípadne právny základ pôvodných účelov v zmysle čl. 89 GDPR	Spracúvanie osobných údajov na účely archivácie vo verejnom záujme zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky: (i) uchovávanie registratúrnych záznamov podľa lehôt uvedených v registratúrnom pláne banky (správa registratúry); (ii) uchovávanie záznamov o došlej pošte; (iii) likvidácia registratúrnych záznamov po uplynutí úložných lehôt; (iv) postupovanie archívnych dokumentov štátnym archívom; (v) vyradovacie konanie; (vi) opätovné sprístupňovanie a používanie registratúrnych alebo archívnych dokumentov za splnenia podmienok testu zlučiteľnosti (napr. na účely preukazovania, uplatňovania a obhajovania právnych nárokov).