

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>	Spracúvanie osobných údajov na účely poskytovania bankových produktov a služieb zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky: 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); (vi) preverenia existencie konkurzného alebo obdobného konania; (vii) opätovnej kontroly aktuálnosti údajov pri ďalších obchodoch; (viii) kontroly údajov porovnaním s dokladom totožnosti; (ix) spracúvania biometrických údajov na identifikáciu klienta; (x) postupov týkajúcich sa zmeny údajov klienta alebo jeho zástupcu, (xi) uľahčenie overenia identity klienta alebo zástupcu klienta, ktorého identita už bola preverená v rámci KYC procesov inou bankou zo skupiny ERSTE v rámci tzv. „onboardingových“ procesov Prevádzkovateľa, čo zahŕňa využívanie zdieľaných dokumentov a prijímanie osobných údajov o dôležitých fyzických osobách pôsobiacich u korporátnych klientov Prevádzkovateľa (napr. členovia štatutárnych orgánov, koneční užívatelia výhod, spoločníci, akcionári) od členov podnikov ERSTE Group, a to najmä: Erste Group Bank AG, Erste Bank Österreich, Erste Bank Novi Sad, Erste & Steiermärkische Bank, Erste Bank Hungary, Česká spořitelňa, a.s, Banca Comercială România, ak už na ich strane bola overovaná identita zástupcov firemných klientov (ix) zdieľanie a poskytovanie osobných údajov a nevyhnutných dokladov týkajúcich sa overovania identity zástupcov firemných klientov členom podnikov zo skupiny ERSTE Group s cieľom uľahčiť KYC procesy a onboarding firemných klientov Prevádzkovateľa aj u spriaznených bánk v zahraničí. 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> 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. Overovanie nehnuteľností. Zahŕňa spracúvanie osobných údajov v rámci: (i) overenia stavu nehnuteľnosti z viacerých zdrojov a registrov, vrátane katastra nehnuteľností, ak je súčasťou bankového obchodu nehnuteľnosť (napr. založená nehnuteľnosť pri hypotéke); (ii) spracúvania osobných údajov o osobách nachádzajúcich sa na listoch vlastníctva predmetných nehnuteľností; (iii) <u>vypracovania a posúdenia znaleckých posudkov k nehnuteľnosti</u>; (iv) poznania a vyhodnotenia stavu nehnuteľnosti v internom systéme banky; (v) <u>využívania údajov o číselníkoch katastra, o administratívnych a technických jednotkách, údajov o stavbách, bytoch a nebytových priestoroch, údajov o účastníkoch právnych vzťahov, o právnych listinách, o listoch vlastníctva, o katastrálnych konaniach, a to aj prostredníctvom analýzy denných tabuliek rozdielov vybraných údajov.</u> (vi) prenesenia údajov do zmluvnej dokumentácie (úverové produkty). 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 týkajúcich sa identifikácie klientov (vyššie) v rámci digitálneho onboardingu; (iv) vytvorenia prihlasovacích a identifikačných údajov v rámci daných aplikácií; (vi) akceptácie zmluvnej dokumentácie na diaľku; (v) <u>využívanie Voicebota na identifikáciu problému, navigáciu a asistenciu pri riešení problémov týkajúcich sa aplikácie George až do jeho úspešného vyriešenia</u> (napr. pri strate prihlasovacieho mena a PIN kódu, neschopnosti klienta nájsť funkčnosť Georgea a pod.).

		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 informácií 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. Cenné papiere (Treasury). Zahŕňa spracúvanie osobných údajov v rámci: (i) získavania údajov v rámci tzv. investičných dotazníkov v rozsahu otázok stanovených Vyhláškou Ministerstva financií SR z 19. decembra 2017; (ii) získavanie ďalších údajov podľa zákona o cenných papieroch (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) vnútrobankových prevodov; (ix) 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 nahlásovania 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) predchádzania podvodom a podvodným operáciám na finančnom trhu; (vii) podávania 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 podpory klienta prostredníctvom call centra, pobočky alebo osobného bankára, prípadne komunikácie prostredníctvom chatbota, (ii) poskytovania klientskej podpory a starostlivosti prostredníctvom asistenčného systému schopného na základe softvéru s integrovanou technológiou umelej inteligencie (AI) využívať rozpoznávanie hlasových pokynov (ďalej len „Voicebot“) zamestnancov pri proaktívnej hlasovej odchádzajúcej komunikácii smerovanej na klientov (napr. pri rôznych zmenách) a hlasových pokynov klientov pri prichádzajúcej komunikácii pri vyriešení klientskej požiadavky alebo jej presmerovaní na definovanú skupinu riešiteľov, (iii) využívania Voicebota pri evidovaní prichádzajúcich volaní zákazníkov a dôvodov ich volania do určeného interného systému banky a na poskytovanie typizovaných klientskych FAQs (odpovedí na často kladené otázky) a typizovaných odpovedí týkajúcich sa konkrétnych bankových produktov alebo služieb, (iv) využívania Voicebota v rámci asistenčných služieb pri blokovaní platobných kariet, vydávaní nových platobných kariet, aktivovaní platobných kariet a bezhotovostných platieb, (v) využívania Voicebota pri manažmente organizácie stretnutí klientov s internými znalcami banky na oceňovanie nehnuteľností a poskytovaní katastrálnych údajov o relevantných nehnuteľnostiach zahrnutých do obchodu banky interným znalcom banky, (vi) využívania Voicebota pri vykonávaní proaktívnych notifikácií a pripomienok adresovaných klientom vyžadujúcich doplnenie chýbajúcich informácií a podkladov potrebných pre riadne poskytovanie bankových produktov a služieb a kontroly ich úplnosti (napr. vyžiadanie podkladových dokumentov k žiadosti o úver, ktoré neboli odovzdané), (vii) využívanie asistencie Voicebota pri riešení klientskych požiadaviek na odblokovanie bezpečnostných predmetov, (viii) využívanie Voicebota na aktívne informovanie klientov o výsledkoch vybavenia ich požiadaviek a reklamácií po ich uzatvorení v príslušnom internom systéme banky, (ix) využívanie Voicebota na dohodnutie termínu pre zavolanie klientovi na najbližší voľný termín podľa dát z pracovných kalendárov zamestnancov banky v prípade, ak počas klientskeho volania nie je k dispozícii žiadny voľný poverený pracovník banky (x) nahrávania telefonической komunikácie a overovania identity klienta; (xi) riešenia všeobecných podnetov, sťažností alebo reklamácií klientov; (xii) agendy ombudsmana banky, na ktorého sa môžu klienti banky obrátiť v akejkoľvek veci; (xiii) akejkoľvek poštovej, elektronickej telefonической alebo osobnej komunikácie súvisiacej s vyššie uvedenými spracovateľskými operáciami a zasielania tzv. servisných správ; (xiv) spracovania a vyúčtovania akýchkoľvek poplatkov banky v zmysle platného cenníka alebo pripísania akéhokoľvek zhodnotenia (napr. úroky alebo výnosy) na účet klienta; (xvi) prípravy, uzatvárania a vykonávania obchodov a zmluvných vzťahov s klientmi; (xvi) správy a kontroly záväzkového vzťahu medzi klientom a bankou; (xvii) poskytovania doplnkových služieb s pridanou hodnotou pre klienta banky, vrátane poskytovania tzv. voliteľných doplnkov v rámci aplikácie Goerge ako je napr. finančný manažér a mesačný prehľad, ktoré dotknutej osobe pomáhajú získať lepší prehľad o kategóriách jej finančných príjmov a výdavkov; (xviii) vnútorných administratívnych činností banky alebo skupiny Erste, vrátane prenosu osobných údajov v rámci skupiny Erste na vnútorné administratívne účely vrátane spracúvania osobných údajov klientov, externých partnerov alebo zamestnancov; (xix) využívanie Voicebota pri podpore a poskytovaní asistenčných služieb pre autentizovaných externých partnerov v rámci rozmanitých interných procesov banky, (xx) získavania spätnej väzby od klientov pre potreby skvalitňovania a prispôsobovania bankových produktov a služieb potrebám, požiadavkám a preferenciám klientov a novým trendom v bankovníctve (xxi) asistenčných úkonov pri podpore „onboardingu“ potenciálnych klientov, ktorí prerušia a nedokončia potrebný „onboardingový“ proces, vrátane využitia už poskytnutých kontaktných údajov, (xxi) na generovania a zobrazovania rád konkrétnym skupinám segmentovaných (profilovaných) a výlučne plnoletých klientov (napr. rady k aktivácii, či blokácii karty, zvyšovaniu bezpečnosti online „bankovania“, nastavenia trvalých príkazov, stiahnutia apky George (web George), nastaveniam základných servisných úkonov ako je zriadenie novej platby, skenovanie údajov pre platbu), poskytovanie odkazov na konkrétnejšie video-návody a pod., (xxii) vytváranie a vyhodnocovanie spôsobu interakcií používateľov so zobrazenými radami v aplikácii George z dôvodu zefektívňovania a zvyšovania používateľského komfortu a zákazníckej starostlivosti. Spracúvanie môže zahŕňať aj ďalšie spracovateľské operácie, oblasti alebo postupy, ktoré budú nevyhnutné pre splnenie účelu poskytovania bankových produktov a služieb.

Zdieľanie a využívanie údajov v skupine ERSTE pri cezhraničných platobných operáciách. Zahŕňa spracúvanie osobných údajov počas poskytovania údajov v rámci Skupiny ERSTE pri cezhraničných platbách z dôvodu zdieľania spoločnej IT infraštruktúry, ktorá je platformou pre platobné systémy niektorých bánk zo skupiny ERSTE Group (vrátane

		Prevádzkovateľa). Takéto zdieľané využívanie údajov umožňuje Prevádzkovateľovi voči klientom vykonávať efektívnejšie a ľahšie platby na účty klientov vedené v tretích krajinách v bankách mimo skupiny ERSTE Group, napr. z vlastných zdrojov skupiny ERSTE Group, ktoré sa nachádzajú na účtoch bánk mimo skupiny Erste Group v takýchto tretích krajinách. <u>Využívanie analytických nástrojov a dát skupiny ERSTE pri ochrane pred legalizáciou príjmov z trestnej činnosti.</u> Zahŕňa spracúvanie osobných údajov v rámci: (i) zdieľania osobných údajov rámci skupiny ERSTE Group prostredníctvom skupinovej softvérovej platformy „CAPS – Compliance Advanced Analytics Platform and Services“ (CAPS) pre vývoj modelov strojového učenia, vyšetovania a analýzy klientskeho portfólia, analýzy rizika finančnej kriminality a podávania súvisiacich automatizovaných správ s cieľom optimalizovať účinnosť a efektívnosť plnenia regulačných požiadaviek týkajúcich sa finančnej kriminality v sektore bánk. Táto spracovateľská operácia nebude v sebe zahŕňať žiadne aktívne poskytovanie osobných údajov zahrnutých do AML hlásení od Prevádzkovateľa iným bankám zo skupiny ERSTE Group, (ii) využívanie CAPS pri vyhodnocovaní a rozpoznávaní neobvyklých obchodných operácií na základe analýzy klientskych dát. <u>Zefektívňovanie produktivity a kreativity poskytovania bankových služieb pomocou AI technológií.</u> Zahŕňa spracúvanie osobných údajov v rámci: (i) akéhokoľvek spracúvanie osobných údajov klientov, ku ktorému dochádza pri využívaní umelej inteligencie Copilot integrovanej v MS Office 365 pri zvyšovaní kreativity, analytickosti a produktivity používateľov aplikácií ako sú napr. Word, Excel, Powerpoint, Outlook, Teams fungujúcich v prostredí cloudových služieb MS Office 365. Typicky sa to týka hlavne realizácie úkonov, ktoré sa vykonávajú s asistenciou Copilota, pri vyhodnocovaní zavádzania rôznych opatrení s dopadom na klientov, pri segmentácii klientov, reorganizáciách a súvisiacich analýzach kvality poskytovaných služieb a vhodnosti produktov, či pri vyhodnocovaní efektívnosti interných štandardov a vnútorných procesov súvisiacich s poskytovaním bankových služieb. <u>Poskytovanie údajov o adrese platiteľov poskytovateľovi platobných služieb príjemcu platby v rámci prevodov akýchkoľvek finančných prostriedkov v celej EÚ aj mimo EÚ.</u> Zahŕňa spracúvanie osobných údajov v rozsahu meno platiteľa, číslo platobného účtu platiteľa a adresa platiteľa pri všetkých prevodoch finančných prostriedkov bez ohľadu na ich výšku poskytovateľovi platobných služieb príjemcu platby usadenému v EÚ aj mimo EÚ, pričom údaj o adrese platiteľa sa poskytuje aj nad rámec minimálneho rozsahu údajov podľa povinností podľa čl. 5 ods. 2 a čl. 6 ods. 2 Nariadenia Európskeho parlamentu a Rady (EÚ) 2015/847 z 20. mája 2015 o údajoch sprevádzajúcich prevody finančných prostriedkov, ktorým sa zrušuje nariadenie (ES) č. 1781/2006. <u>Rizikový model banky – SIMS – klienti.</u> Predmetné spracúvanie sa týka existujúcich klientov Prevádzkovateľa - právnických osôb alebo subjektov, ktoré sú v súvislosti s jednaním o poskytnutí bankovej služby preverovaní. Napr. štatutárni zástupcovia klientov, ktorí sú právnickými osobami. Spracovateľská operácia zahŕňa spracúvanie údajov získaných od spoločnosti Slovenská informačná a marketingová spoločnosť, a. s. ("SIMS"), ktorá je spravodajskou agentúrou poskytujúcou špecializovaný, analytický a štruktúrovaný spravodajský servis zameraný na ekonomické, obchodné a faktografické spravodajstvo. Osobné údaje v rozsahu zákonne zverejnených údajov SIMS získava z oficiálnych verejne dostupných zdrojov, ako sú štatistický úrad a štátne a iné verejné registre. Základná časť spracovateľských operácií Prevádzkovateľa, ktorá súvisí s rizikovým modelom banky, prebieha súčasne aj na právnom základe plnenia zákonných povinností podľa čl. 6 ods. 1 písm. c) GDPR. Banka musí mať podľa zákona č. 483/2001 Z. z. o bankách svoj vlastný rizikový model, ktorý kontroluje a schvaľuje NBS, a ktorý musí prispôbovať svojmu podnikaniu. Z tohto dôvodu je uplatňovanie rizikového modelu banky nevyhnutnou súčasťou spracúvania údajov v rámci poskytovania bankových produktov a služieb. Širším kontextom tohto spracúvania je, že rizikový model chráni integritu finančného sektora tým, že nedovolí banke (najmä vo vzťahu k úverovým alebo hypotekárnym produktom) také operácie, ktoré by boli rizikové. Spracúvanie údajov v súvislosti s uplatňovaním rizikového modelu banky však predstavuje vo vzťahu k vyššie uvedeným spracovateľským operáciám oprávnený záujem banky.
2. Právne a zmluvné účely	Plnenie zmluvy a <u>oprávnený záujem</u>	Spracúvanie osobných údajov na účely preukazovania, uplatňovania a obhajovania právnych nárokov zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky:

Vymáhanie pohľadávok. Zahŕňa spracúvanie osobných údajov v rámci: (i) zasielania výziev a upomienok k neuhradeným platbám; (ii) 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 urovaní alebo splátkových kalendárov, (viii) využívania Voicebota na aktívne informovanie klientov o splatných pohľadávkach v omeškaní a riešenie spôsobu najrýchlejšieho splatenia, čo zahŕňa zistenie a využitie relevantných informácií o pohľadávke a zároveň zistenie možnosti úhrady a dôvody vzniknutého omeškania na strane klienta, ktoré zaeviduje do príslušných interných systémov banky, a to aj vrátane klientskych vyjadrení vrátane žiadostí o splátkové kalendáre a požiadaviek na zmenu dátumov splátok, (ix) využívania Voicebota na spracovanie a vybavenie požiadavky klienta - dlžníka komunikovať v rámci procesu mimosúdneho vymáhania pohľadávky emailom.

Súdne spory, konania a dopyty. Zahŕňa spracúvanie osobných údajov v rámci: (i) 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 urovaní; (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.

Zmluvná agenda. Zahŕňa spracúvanie osobných údajov v rámci: (i) uzatvárania a plnenia akejkoľvek zmluvy medzi bankou a tretou stranou; (ii) schvaľovania a revízie zmlúv právnym oddelením (iii) komunikácie zmluvných strán vrátane spracúvania údajov o kontaktných osobách a štatutároch 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).

Správa majetku. Zahŕňa spracúvanie osobných údajov v rámci: (i) správy, údržby a zhodnocovania nehnuteľného a hnutelného majetku banky; (ii) uzatvárania a evidencie nájomných a iných zmlúv k nehnuteľnostiam; (iii) vysporiadania majetkovo-právnych záležitostí týkajúcich sa nehnuteľností.

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; (iv) oznamovania a dokumentovania porušení ochrany osobných údajov; (v) vedenia záznamov o poučení alebo informovaní, (iv) konvalidácie už udelených súhlasov so spracúvaním osobných údajov po uplynutí dlhšej doby, ak je to primerané alebo žiadosť o opätovné udelenie súhlasu so spracúvaním osobných údajov v prípadoch, ak v minulosti dotknutá osoba neudelila súhlas a s ohľadom na okolnosti je to primerané (napr. uplynula dlhšia doba, príp. očakávanie dotknutej osoby týkajúce sa spracúvania by sa mohli zmeniť, pretože ide o špecifickejšiu žiadosť Prevádzkovateľa a pod.) (vii) využívania Voicebota na čítanie povinných právnych informácií (napr. v rámci telefonátov s klientami), získavanie súhlasov so spracúvaním osobných údajov a ich zaevidovanie do príslušného interného systému banky a prípadné dopĺňovanie vysvetlení k nadväzným otázkam klienta.

Právna agenda. Zahŕňa spracúvanie osobných údajov v rámci: (i) typickej agendy právneho oddelenia, napr. pripomienkovanie zmlúv, vymáhanie pohľadávok či spisovanie žalôb a návrhov na začatie súdnych konaní; (ii) kontroly právnych záležitostí a interného právneho poradenstva; (iii) nahlasovania rôznych skutočností orgánom verejnej moci (vrátane hlásenia o deliktoch, trestných činoch alebo škodových/poistných udalostiach); (iv) využívania právneho zastúpenia a právneho poradenstva advokátskych kancelárií; (v) vykonávania auditu (due diligence), vrátane poskytovania údajov potenciálnym kupujúcim a ich poradcom napr. pri predaji podniku, akcií alebo portfólia banky; (vi) vedenia korporátnej agendy a plnenia všetkých povinností v zmysle Obchodného zákonníka (napr. valné zhromaždenia a pozvánky, výročné správy); (vii) získavania, obnovy a evidencie akýchkoľvek licencií, súhlasov, potvrdení o odbornej spôsobilosti alebo o dosiahnutom vzdelaní v rámci bežného súladu banky s právnymi predpismi (viii) využívania Voicebota na čítanie povinných právnych informácií (napr. v rámci telefonátov s klientami), získavanie dôkazov o právnych úkonoch (prejavoch vôle) klienta a ich zaevidovanie do príslušného interného systému banky a prípadné dopĺňovanie právnych vysvetlení k nadväzným otázkam klienta. .

3. Vykonávanie bezpečnostných opatrení na prevenciu pred podvodmi	Splnenie zákonnej povinnosti a <u>oprávnený záujem</u>	Spracúvanie osobných údajov na účely vykonávania bezpečnostných opatrení na prevenciu pred podvodmi zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky: 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 napodporu silnej autentizácie používateľa elektronických bankových služieb vychádzajúcich z definovania a analýzy signálov odzrkadľujúcich spôsob využívania a správanie používateľa bankových aplikácií a systémov; (iii) analýzy a využívania rizikových signálov v rámci identifikácie, autentizácie a autorizácie prístupov dotknutej osoby k definovaným službám a funkcionalitám elektronického bankovníctva a pri vyhodnocovaní stupňa bezpečnosti pri autorizácii platieb. 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. Bezpečnosť a vývoj IT. Ide o kombinovanie a využívanie dát spracúvaných na tento účel, vrátane rizikových signálov aj nazlučiteľné 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.
4. Bezpečnosť a vývoj IT	Splnenie zákonnej povinnosti a <u>oprávnený záujem</u>	Spracúvanie osobných údajov na účely bezpečnosti a vývoja IT zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky: Riadenie prístupových práv. Ide o spracúvanie osobných údajov najmä v súvislosti s (i) prideľovaním, zmenami a odobieraním 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) dátovou integráciou a posilňovaním autorizácie prístupov používateľov a klientov cez technologické riešenia na báze IAM (Identity Access Management), (iii) prideľovaním, zmenami, obnovovaním zabudnutých alebo kompromitovaných hesiel do interných systémov banky alebo bankových aplikácií určených pre klientov, (iv) uchovávaním údajov neaktívneho (disabled) používateľa po určité obdobie po odobratí jeho prístupových práv z hľadiska prevencie pred pokusmi o zneužitie jeho prihlasovacej identity, (v) využívaním 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) využívaním osobných údajov za účelom odlišenia a verifikácie ľudského konania od útokov tzv. botov integrovaným do služieb internetového bankovníctva, (vii) 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 využívanie 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 forenznnej analýzy preskúmajúcej 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 údaje, 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 úrovni aplikáčnych vrstiev využívaných informačno-komunikačných technológií banky, počítačových sietí, elektronických komunikačných metadát atď.), (ii) porovnávanie osobných údajov používateľov IT banky s 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 a pod.) 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 zadefinovaných 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 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) v rámci umelej inteligencie začleňovanej do niektorých externých softvérových bezpečnostných riešení, ktoré banka využíva pri analýze dát a rôznych udalostí sledovaných v interných systémoch.

Trénovanie umelej inteligencie. Ide o spracúvanie osobných údajov, ktoré typicky zahŕňa: (i) poskytovanie vstupných údajov získaných pôvodne na zlučiteľné účely ich spracúvania do systémov s integrovanou umelou inteligenciou (napr. Keboola, Azure Databricks), ktorá ich bude následne analyzovať a využívať v kontexte zadaných školiacich úloh a vopred stanovených účelov s cieľom vytvárania funkčných dátových modelov aplikujúcich správne väzby a logické odvodenia z hľadiska definovaných kritérií a dosahovania cieľov pre svoje vlastné zdokonaľovanie sa a efektívnejšie plnenie zadávaných úloh, (ii) testovacie overovanie korektnosti a spoľahlivosti tréningových dátových modelov vytvorených v simulovaných podmienkach umelou inteligenciou.

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. 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 vývoja IT pri plnení zákonných povinností banky ako prevádzkovateľa podľa čl. 32 GDPR. 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).
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 uchovávania 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 (Foreign Account Tax Compliance Act) vrátane jeho 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) priestorov prístupných verejnosti v definovaných objektoch banky, vrátane siete pobočiek banky a (ii) bankomatov a zmenárenských miest (§ 93a ods. 7 Zákona o bankách) prostredníctvom kamerových systémov.

		Systémy na kontrolu a evidenciu vstupov do definovaných priestorov banky. 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 GPS monitoring firemných vozidiel. Ide o monitorovanie geo-lokalizácie 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/á) a zároveň udelí banke na takéto monitorovanie osobitný špecifický informovaný súhlas so spracúvaním osobných údajov, ktorého neudelenie nemá na zamestnanca žiadny negatívny vplyv. Využívanie súkromných bezpečnostných služieb. 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 zabezpečovaním ochrany osôb a majetku v mene banky (napr. sprevádzanie zamestnancov banky na dražby, exekúcie, rizikové súdne pojednávania či vykonávanie strážnej službyv definovaných objektoch banky).
8. Marketingové a PR účely	Súhlas a <u>oprávnený záujem</u>	Spracúvanie osobných údajov na marketingové účely a PR účely zahŕňa okrem iného nasledovné operácie, oblasti a postupy banky: Cielená reklama (priamy marketing). Zahŕňa spracúvanie osobných údajov v rámci: (i) tvorby a prispôsobovania obsahu, času a spôsobu marketingového oslovenia pred odoslaním marketingovej elektronickej pošty (e-mail, SMS, push-notifikácie, správy v Georgovi) alebo vykonaním marketingového volania; (ii) tvorby a prispôsobovania obsahu letákov alebo tlačených marketingových materiálov; (iii) profilovania správania klienta v rámci online marketingu, vrátane tvorby, prispôsobovania reklamy a personalizovaných ponúk v rámci bankovej aplikácie George alebo internet banking; (iv) tvorby, prispôsobovania obsahu reklamy a jej zobrazovania na sociálnych sieťach (súhlas s cookies); (v) tvorby, prispôsobovania a zobrazovania bannerovej reklamy na webstránkach (súhlas s cookies); (vi) vykonávania foriem priameho marketingového oslovenia dotknutej osoby v rámci elektronickej komunikácie (SMS, email), v rámci aplikácie George (Push-notifikácie, správy v Georgovi), či internet banking alebo telefonicky výlučne k existujúcim klientom v súvislosti s ponukou obdobných tovarov a služieb a pri dodržaní všetkých právnych obmedzení nevyžadanej komunikácie podľa § 116 Zákona o elektronických komunikáciách; (vii) vykonávania foriem priameho marketingového oslovenia dotknutej osoby v rámci elektronickej komunikácie (SMS, email), v rámci aplikácie George (Push-notifikácie, správy v Georgovi), či internet banking alebo telefonicky (bežný súhlas), (viii) realizácie marketingových prieskumov a ankiet spokojnosti (bežný súhlas), a to aj vrátane využívania Voicebota realizujúceho prieskum spokojnosti a zaznamenávanie odpovedí klientov . Využívanie marketingových nástrojov. Zahŕňa spracúvanie osobných údajov v rámci: (i) profilovania vykonávaného analýzou návštevnosti, úspešnosti a konverzie, prípadne vytvárania iných marketingových analýz v rámci segmentácie klientov a používateľov elektronických služieb (napr. prostredníctvom nástrojov Google Analytics, Facebook Ads Manager, SAS Customer Intelligence 360 a pod.); (ii) využívania pluginov sociálnych sietí alebo tretích strán (ako napr. FB/Google Login); (iii) identifikácie klienta pri prihlásení sa do Georga a promo-zón chránenej zóny; (iv) používania rôznych analytických nástrojov, ktoré využívajú aj cookies, pixely, SDK, web beacons a pod., tak ako sú vysvetlené v rámci „cookies policy“ banky a za podmienky, že marketingové a štatistické cookies boli získané po udelení súhlasu s cookies, (v) profilovania vykonávaného analyzovaním a využívaním rôznych transakčných a behaviorálnych é dát o správaní používateľov Georga alebo webstránok SLSP a a rozmanitých osobné údaje týkajúce sa využívania bankových produktov a služieb, ktorými

		banka disponuje vo vzťahu k existujúcimi klientom s cieľom zefektívňovať podporu predaja bankových produktov a služieb. (vi) profilovania vykonávaného analyzovaním a vyhodnocovaním interakcií dotknutých osôb so zobrazovanou reklamou a priamou elektronickou marketingovou komunikáciou (napr. notifikácie v Georgovi, emaily). Všetky opísané spracovateľské operácie spojené s využívaním marketingových nástrojov sa vykonávajú najmä s cieľom zefektívňovať podporu predaja bankových produktov a služieb alebo merať a vyhodnocovať účinnosť a vhodnosť oslovenia relevantných okruhov dotknutých osôb s konkrétnou ponukou produktov a služieb. Zvyšovanie povedomia a dobrého mena (PR). Zahŕňa spracúvanie osobných údajov v rámci: (i) vedenia profilov banky / skupiny SLSP na sociálnych sieťach a súvisiacej interakcie s užívateľmi; (ii) organizovania podujatí, vrátane vyhotovovania foto a video záznamov (môže sa využívať aj v kombinácii so súhlasom dotknutej osoby podľa povahy konkrétnej situácie); (iii) zverejňovania obsahu, foto alebo video záznamov v rámci sociálnych sietí (môže sa využívať aj v kombinácii so súhlasom dotknutej osoby podľa povahy konkrétnej situácie); (iv) zvyšovania povedomia a dobrého mena (PR účely); (v) organizovania spotrebiteľských súťaží vrátane partnerských súťaží (môže sa využívať aj v kombinácii so zmluvou alebo súhlasom ako právnym základom).
9. Štatistické 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).

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