SLOVENSKÁ sporiteľňa

Pravidlá ochrany súkromia – mobilné aplikácie (privacy policy)

(podľa článku 13 a 14 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR))

Prevádzkovateľ
Slovenská sporiteľňa, a. s., Tomášikova 48, 832 37 Bratislava, IČO 00151653, zapísaná v Obchodnom registri Okresného súdu Bratislava I, odd. Sa, vložka č. 601/B (ďalej „Banka“).
telefonický kontakt: 0850 111 888 e-mailová adresa: info@slsp.sk webové sídlo: www.slsp.sk

Zodpovedná osoba
Riaditeľ odboru právnych služieb
Korešpondenčná adresa: Odbor právnych služieb, Slovenská sporiteľňa, a. s., Tomášikova 48, 832 37 Bratislava
e-mailová adresa: osobneudaje@slsp.sk

Mobilné aplikácie
Tento dokument vysvetľuje akým spôsobom Banka spracúva osobné údaje špecificky vo vzťahu k mobilným aplikáciám:

- „George Slovensko“ (https://play.google.com/store/apps/details?id=sk.slsp.georgego)
- „George Go Slovensko“ (https://play.google.com/store/apps/details?id=sk.slsp.georgego&hl=en_US)
- „SLSP mToken“ (https://play.google.com/store/apps/details?id=com.slsp.mtoken)
- „Business24“ (https://play.google.com/store/apps/details?id=sk.slsp.business24)

prípadne vo vzťahu k akýmkoľvek iným mobilným aplikáciám, desktopovým aplikáciám, internet bankingu alebo vo všeobecnosti k elektronickým bankovým alebo finančným službám a produktom. Vlastníkom a prevádzkovateľom vyššie uvedených mobilných aplikácií je Banka.

Tento dokument dopĺňa hlavnú informáciu Banky o spracúvaní osobných údajov (klienti), ktorá je zverejnená na webovom sídle Banky v sekcii „osobné údaje“ (ďalej len „**Hlavná informácia**“) a ktorá sa naďalej vzťahuje aj na mobilné aplikácie. Dôvodom je, že prostredníctvom alebo pomocou mobilných aplikácií stále dochádza k poskytovaniu bankových produktov a služieb klientom Banky.

Používanie mobilných aplikácií je vyhradené pre klientov Banky resp. zástupcov klientov Banky, pričom na to je nevyhnutné mať s Bankou uzatvorenú zmluvu o poskytovaní bankových produktov alebo služieb (napr. zmluva o bežnom účte). Niektoré funkcionality mobilných aplikácií sú navyše podmienené uzatvorením špecifickej zmluvy (napr. zmluva o bezpečnostných predmetoch, zmluva o elektronických službách) alebo sa ne vzťahujú špecifické obchodné podmienky Banky (napr. produktové obchodné podmienky pre depozitné produkty). Aby Banka mohla plniť svoje povinnosti podľa daných zmlúv alebo podmienok, je nevyhnutne potrebné, aby dochádzalo k spracúvaniu údajov aj prostredníctvom mobilných aplikácií.

Účely a právne základy spracúvania osobných údajov
V rámci mobilných aplikácií dochádza k spracúvaniu osobných údajov primárne na účely poskytovania bankových produktov a služieb, pričom základom spracúvania osobných údajov vyššie uvedeného účelu je (podľa toho o akú spracovateľskú činnosť ide) buď:

- súhlas dotknutej osoby podľa čl. 6 ods. 1 písm. a) alebo čl. 9 ods. 2 písm. a) GDPR;
- plnenie zmluvy s dotknutou osobou podľa čl. 6 ods. 1 písm. b) GDPR;
- splnenie zákonnej povinnosti podľa čl. 6 ods. 1 písm. c) GDPR;
- oprávnený záujem podľa čl. 6 ods. 1 písm. f) GDPR.

V rámci mobilných aplikácií (ale najmä vo vzťahu k aplikácii „SLSP mToken“) takisto dochádza k spracúvaniu osobných údajov na účely (i) vykonávania bezpečnostných opatrení na prevenciu pred podvodmi na právnom základe splnenia zákonnej povinnosti podľa čl. 6 ods. 1 písm. c) GDPR a súčasne na právnom základe oprávneného záujmu podľa čl. 6 ods. 1 písm. f) GDPR.

Ďalšie relevantné účely spracúvania, právne základy spracúvania osobných údajov ako aj oprávnené záujmy sledované Bankou vyplývajú z Hlavnej informácie.

Sledované oprávnené záujmy
Pri nasledujúcich účeloch sa spoliehame aj na právny základ oprávneného záujmu podľa čl. 6 ods. 1 písm. f) GDPR. Nižšie nájdete bližšie vysvetlenie oprávnených záujmov, ktoré sledujeme.

Účel spracúvania	Vysvetlenie oprávneného záujmu
Vykonávanie bezpečnostných opatrení na prevenciu pred podvodmi	*Prijímanie a vykonávanie bezpečnostných opatrení s cieľom ochrániť Banku a jej klientov využívajúcich bankové elektronické služby pred kyber hrozbami, kyber útokmi, podvodmi, škodlivými kódmi, kompromitáciou informačnej bezpečnosti, vrátane monitoringu a analýzy podvodných operácií s finančnými prostriedkami, zabezpečovania silnej autentifikácie klientov pri ich vstupe do mobilnej aplikácie George, internet bankingu, do rozhrania tretej strany, pri zadávaní alebo potvrdzovaní platobných príkazov alebo pri iných úkonoch na diaľku, ktoré predstavujú vysoké riziko hrozby považujeme za náš oprávnený záujem.*

Poučenie: Dotknutá osoba má právo namietať proti spracúvaniu svojich osobných údajov na základe oprávneného alebo verejného záujmu ako aj proti spracúvaniu na účely priameho marketingu vrátane namietania proti súvisiacemu profilovaniu podľa čl. 21 GDPR. Ak dotknutá osoba udelila Banke súhlas so spracúvaním osobných údajov, má právo kedykoľvek ho odvolať, pričom odvolanie nemá vplyv na zákonnosť spracúvania vychádzajúceho zo súhlasu pred jeho odvolaním.

Povinnosť poskytnúť osobné údaje
Poskytnutie osobných údajov zo strany dotknutej osoby ako užívateľa mobilných aplikácií je dobrovoľné, nakoľko samotné používanie mobilných aplikácií je dobrovoľné. Avšak, bez poskytnutia niektorých osobných údajov alebo bez uzatvorenia zmluvy s Bankou nie je možné využívať všetku funkcionalitu mobilných aplikácií. Je tomu tak najmä z dôvodu, že Banka má povinnosť overiť identitu užívateľa pred jeho pripustením do chráneného prostredia bankových mobilných aplikácií. Ak klient odmietne Banke poskytnúť osobné údaje požadované na základe osobitných právnych predpisov, odmietne Banka vykonať bankový obchod. Ak klient odmietne Banke poskytnúť osobné údaje, ktoré sú zmluvnou požiadavkou, nebude môcť dôjsť k uzatvoreniu zmluvy. Ak klient odmietne Banke poskytnúť osobné údaje, ktoré sú nevyhnutné pre spracúvanie, ktoré sa zakladá sa na súhlase, nebude môcť dôjsť k danému spracúvaniu.

Údaje, ku ktorým majú aplikácie prístup
Podľa pravidiel spoločnosti Google mobilné aplikácie získavajú aj niektoré z tzv. „*personal and sensitive information*“ (tzn. osobné a citlivé informácie). Podľa spoločnosti Google medzi také informácie patria okrem iného: akékoľvek osobné údaje; finančné alebo platobné údaje; autentifikačné informácie; alebo senzorové údaje týkajúce sa fotoaparátu.

Ak mobilná aplikácia požaduje **prístup k fotoaparátu** mobilného zariadenia, robí tak buď s cieľom umožniť vykonanie platby naskenovaním napr. QR kódu, poštovej poukážky alebo čiarového kódu alebo s cieľom overenia Vašej identity napr. pri zakladaní účtu bez prítomnosti na pobočke. Zároveň sa týmto spôsobom uisťujeme, že komunikujeme so živou (skutočnou) osobou. Ak nám umožníte tento prístup, nezakladá to naše právo pristupovať k fotografiám uloženým v zariadení, o ktoré sa nemusíte obávať.

Ak mobilná aplikácie vyžaduje využitie funkcionality **FaceID** na zariadeniach Apple, Banka nemá prístup k samotnej fotografii ani k žiadnym biometrickým údajom. Tieto zostávajú spracúvané len prostredníctvom Vášho mobilného zariadenia a spoločnosťou Apple, Inc. Banka sa prostredníctvom FaceID prakticky len opýta Vášho mobilného zariadenia, či ste to naozaj Vy. Používanie FaceID môžete prostredníctvom nastavení Vášho zariadenia úplne zakázať alebo povoliť/zakázať len vo vzťahu ku konkrétnym aplikáciám. Viac informácií o FaceID ako aj o nastavení danej funkcionalite nájdete tu:

- https://support.apple.com/sk-sk/HT208108
- https://support.apple.com/sk-sk/HT208109

Ak mobilná aplikácie spracúva **GPS polohu zariadenia**, robí tak buď z dôvodu, aby zisťovala anomálie indikujúce podvodné správanie alebo iné škodlivé činnosti, aby umožnila funkcionalitu, ktorá je priamo naviazaná na polohu zariadenia (napr. ponuka menovej kalkulačky s predvolenou menou podľa lokality) alebo z dôvodu zvýšenia bezpečnosti služieb vo všeobecnosti (napr. pri podpise platieb). Užívateľ aplikácie môže kedykoľvek povoliť alebo zakázať zaznamenávanie GPS polohu zariadenia.

V prípade používania aplikácie mToken sa skúma aj **stav telefónu**. Cieľom je ochrana klienta a Banky pred podvodnými a škodlivými činnosťami. V rámci stavu telefónu za zaznamenáva a analyzuje, či iné aplikácie nemajú neprimerane silné oprávnenia alebo či sa s nimi nespájajú udalosti, ktoré by mohli indikovať prítomnosť podvodu alebo škodlivého kódu (napr. Root/Jailbrake – iOS, Android; Fingerprint – iOS, Android; SMS hijacking – Android; Overlay detection – Android; Emulatr detection – Android, Human checks – Android; Debugger detection – Android).

Okrem toho mobilné aplikácie spracúvajú prihlasovacie údaje užívateľa, identifikačné alebo overovacie údaje, údaje týkajúce sa používania aplikácií a najmä zadávania príkazov alebo pokynov vo vzťahu k platobným funkcionalitám a všetky bežne spracúvané osobné údaje v bankovom prostredí (ako napr. zostatky na účte,

pohyby, platby, a pod.).

Mobilné aplikácie ukladajú do Vášho zariadenia dva súbory cookies, jeden s dobou používania 1 rok a druhý s dobou používania 24 hodín. Tieto súbory sú ukladané do zariadenia prostredníctvom SDK (software development kit) mobilnej aplikácie alebo JAVA skriptu (tzv. snippet) webovej aplikácie (internet bankingu). V prípade, ak klient zablokuje ukladanie súborov cookies na svojom zariadení, neznamená to automaticky odmietnutie poskytnutia služby, ale chýbajúci identifikátor znamená zvýšenú mieru rizika, ktorá môže znamenať vyžiadanie dodatočného overenia. K týmto súborom má prístup iba Banka, avšak v prostredí Banky s nimi môžu pracovať s informáciami získanými prostredníctvom týchto súborov aj ďalší (preverení) dodávatelia ako napr. spoločnosť ThreatMark s.r.o. Tieto súbory slúžia výlučne len na účely vykonávanie bezpečnostných opatrení na prevenciu pred podvodmi.

Chceli by sme Vás ubezpečiť, že žiadne z vyššie uvedených súborov neslúžia na Vaše sledovanie, predaj dát tretím stranám alebo marketing. Všetky spracúvané údaje uchovávame len na nevyhnutne potrebný čas, bezpečným spôsobom a len v nevyhnutnej miere. V konečnom dôsledku tieto informácie spracúvame preto, aby sme Vás aj nás ochránili pred podvodmi a škodlivými kódmi.

Zdroj získania osobných údajov
Mobilné aplikácie získavajú údaje priamo od Vás resp. komunikáciou s Vaším zariadením.

Doba uchovávania údajov
K získavaniu vyššie uvedených údajov vo všeobecnosti dochádza len počas doby, po ktorú je mobilná aplikácia nainštalovaná a používaná a to len za predpokladu, že užívateľ získavanie citlivých informácií dovolil prostredníctvom nastavenia zariadenia. Súbory cookies týkajúce sa mobilných aplikácií majú nastavenú dobu používania 1 rok a 24 hodín. Banka však niektoré informácie získané prostredníctvom mobilných aplikácií alebo súborov cookies uchováva po dobu 12 rokov, na to na účely poskytovania bankových produktov a služieb a vykonávanie bezpečnostných opatrení na prevenciu pred podvodmi.

Príjemcovia osobných údajov
K spracúvaním údajom majú prístup poverení zamestnanci oddelenia informačnej bezpečnosti Banky a overení dodávatelia Banky v oblasti bezpečnosti (najmä spoločnosť spoločnosť ThreatMark s.r.o.).

Cezhraničný prenos osobných údajov
Cezhraničný prenos osobných údajov do tretích krajín (t.j. krajín mimo EÚ, Nórska, Islandu a Lichtenštajnska) Banka v súvislosti s mobilnými aplikáciami nerealizuje.

Práva dotknutej osoby pri spracúvaní osobných údajov
Klient ako dotknutá osoba má najmä právo žiadať od Banky ako prevádzkovateľa:
- prístup k osobným údajom podľa čl. 15 GDPR;
- opravu nesprávnych a doplnenie neúplných osobných údajov podľa čl. 16 GDPR,
- vymazanie osobných údajov spracúvaných Bankou podľa čl. 17 GDPR,
- obmedzenie spracúvania osobných údajov podľa čl. 18 GDPR,
- odovzdanie/prenosnosť údajov, ktoré poskytol Banke podľa čl. 20 GDPR v štruktúrovanom strojovo čitateľnom formáte, ktoré sú spracúvané automatizovane, a ktoré sú zároveň spracúvané na základe zmluvy alebo súhlasu.

Dotknutá osoba má tiež právo:
- namietať voči spracúvaniu osobných údajov, ktoré Banka spracúva na právnom základe ochrany oprávnených záujmov, vrátane profilovania a priameho marketingu podľa čl. 21 GDPR;
- žiadať, aby sa na ňu nevzťahovalo automatizované individuálne rozhodovania za podmienok stanovených v čl. 22 GDPR;
- odvolať udelený súhlas so spracúvaním osobných údajov
- podať sťažnosť dozornému orgánu, ktorým je Úrad na ochranu osobných údajov SR resp. návrh na začatie konania § 100 zákona č. 18/2018 Z. z., o ochrane osobných údajov.

Automatizované rozhodovanie a profilovanie
Pre účely správne cielenej ponuky bankových produktov a služieb, ako aj pre účely poskytovania a vhodných bankových produktov a služieb klientovi, tak aby zohľadňovali reálne potreby klienta ale aj jeho platobnú schopnosť a možnosti pre poskytnutie takéhoto produktu (najmä úverové produkty), pre účely vyhodnocovania rizikovosti bankových obchodov, Banka využíva v procese schvaľovania produktu ako aj v procese výberu klientov pre cielenú ponuku produktov a služieb niektoré formy automatizovaného rozhodovania a profilovania.

Klient má právo na to, aby sa naňho nevzťahovalo rozhodnutie prijaté na základe výlučne automatizovaného individuálneho rozhodovania (tzn. algoritmické rozhodnutie počítačového programu bez ľudského zásahu) a požadovať vhodné opatrenia zo strany Banky (napr. ľudský zásah zo strany Banky, možnosť vyjadrenia svojho stanoviska alebo právneho napadnutia daného rozhodnutia). Uvedené neplatí, ak je rozhodnutie povolené právom EÚ alebo Slovenskej republiky a ktorým sa zároveň stanovujú aj vhodné opatrenia zaručujúce ochranu práv a slobôd a oprávnených záujmov dotknutej osoby.

Kódex správania
Banka v súlade s článkom 40 GDPR plánuje pristúpiť (po schválení Úradom na ochranu osobných údajov SR) ku kódexu správania vypracovanému Slovenskou bankovou asociáciou pre bankový sektor, ktorého znenie bude po jeho schválení prístupné na webovom sídle Banky, na webovom sídle Slovenskej bankovej asociácie (www.sbaonline.sk), ako aj na webovom sídle Úradu na ochranu osobných údajov SR (www.uoou.sk).

Zmeny a účinnosť
Tento dokument je účinný od 13. septembra 2019 a jeho každá verzia je účinná jej zverejnením na webovom sídle Banky, v app store alebo v mobilnej aplikácii. Banka si vyhradzuje právo jednostranne zmeniť tieto informácie, pričom na podstatné zmeny Banka dotknuté osoby vhodným spôsobom upozorní napr. oznámením v mobilnej aplikácii. Ak zmeny nie sú zásadného charakteru, Banka iba zverejní novú verziu informácií na tom istom mieste ako pôvodná verzia.