Informácie o spracúvaní osobných údajov v mobilnej aplikácii Dôchodok

Článok I — Úvodné ustanovenia a vzťah k hlavným informáciám

- Tieto Informácie o spracúvaní osobných údajov v mobilnej aplikácii Dôchodok (ďalej len „**Informácie o aplikácii**“) poskytujú doplňujúce informácie o spracúvaní osobných údajov pri používaní mobilnej aplikácie **Dôchodok** (dôchodOK) dostupnej pre operačné systémy iOS a Android (ďalej len „**mobilná aplikácia**“).
- Tieto Informácie o aplikácii nadväzujú na hlavné **Informácie o spracúvaní osobných údajov pre klientov VÚB Generali dôchodková správcovská spoločnosť, a.s.** (ďalej len „**Hlavné informácie**“), ktoré sú v aktuálnom znení zverejnené na webovom sídle prevádzkovateľa https://www.vubgenerali.sk/o-nas/ochrana-osobnych-udajov/.
- Pre otázky, ktoré nie sú výslovne upravené v týchto Informáciách o aplikácii (najmä všeobecný rámec spracúvania zmluvnej dokumentácie, dedičské konanie, plnenie zákonných daňových a účtovných povinností, inštitucionálne audity a podrobnosti o výkone všetkých práv dotknutých osôb), sa v plnom rozsahu uplatňujú ustanovenia Hlavných informácií.
- Dokumenty vytvorené alebo doručené prostredníctvom aplikácie, ktoré tvoria súčasť registratúry DSS, sa evidujú, ukladajú a vyraďujú aj podľa zákona č. 395/2002 Z. z. a registratúrneho plánu DSS. Uplynutie lehoty uloženia pri dokumentoch podliehajúcich vyraďovaciemu konaniu neznamená automatické zničenie; dokumenty posúdené ako archívne dokumenty sa odovzdávajú príslušnému štátnemu archívu na trvalé uchovávanie. Toto pravidlo automaticky nepredlžuje dobu uchovávania všetkých technických údajov ani biometrických šablón, pre ktoré platia osobitné účely a lehoty uvedené nižšie.

Článok II — Identifikačné a kontaktné údaje prevádzkovateľa a zodpovednej osoby

1. Prevádzkovateľ

VÚB Generali dôchodková správcovská spoločnosť, a. s.

Mlynské nivy 1, 820 04 Bratislava

IČO: 35 903 058

Všeobecný kontakt: 0850 111 110, info@vubgenerali.sk.

2. Zodpovedná osoba (Data Protection Officer – DPO)

Prevádzkovateľ vymenoval zodpovednú osobu, ktorú môžete v súvislosti so spracúvaním Vašich osobných údajov a uplatňovaním práv podľa Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 (ďalej len „**GDPR**“) kontaktovať:

- **E-mailom:** osobne.udaje@vubgenerali.sk
- **Písomne poštou:** na adresu sídla prevádzkovateľa s označením „*Zodpovedná osoba (DPO)*“.

Článok III — Účely, právne základy, rozsah a doby uchovávania osobných údajov v mobilnej aplikácii

Mobilná aplikácia umožňuje sporiteľom bezpečný elektronický prístup k ich osobnému dôchodkovému účtu, správu zmluvy o starobnom dôchodkovom sporení (II. pilier), overovanie totožnosti a komunikáciu s DSS. Spracúvanie osobných údajov v mobilnej aplikácii prebieha na nasledovné konkrétne účely:

1. Prihlasovanie do mobilnej aplikácie a lokálna (on-device) biometria

Účel spracúvania: Rýchle, komfortné a bezpečné prihlásenie používateľa do aktivovanej mobilnej aplikácie a odomknutie jej rozhrania na koncovom zariadení.

Lokálna biometria zariadenia (Touch ID / Face ID / odtlačok prsta):

- Mobilná aplikácia podporuje využitie systémových biometrických funkcií Vášho zariadenia (napr. Touch ID, Face ID na zariadeniach Apple alebo biometrické overenie odtlačkom prsta či tvárou na zariadeniach so systémom Android).
- **Prevádzkovateľ nemá prístup k Vašim biometrickým údajom uloženým v zariadení.**
- Samotné overenie biometrie prebieha výlučne lokálne na Vašom mobilnom zariadení v rámci jeho chráneného hardvérového modulu (tzv. *Secure Enclave* / *Android Keystore* pod správou operačného systému).
- Mobilná aplikácia od operačného systému dostáva iba informáciu o tom, či bolo lokálne overenie úspešné alebo neúspešné. Pri tomto lokálnom prihlasovaní prevádzkovateľ biometrické vzory ani šablóny zariadenia na svojich serveroch nezhromažďuje, nespracúva ani neukladá. Ide o odlišný postup od vzdialeného biometrického overenia podľa bodu 2.

Právny základ: Oprávnený záujem DSS (čl. 6 ods. 1 písm. f) GDPR) na poskytnutí bezpečného a používateľsky jednoduchého spôsobu prístupu k elektronickým službám. Využitie lokálnej biometrie zariadenia je plne dobrovoľné; alternatívou je prihlasovanie pomocou zvoleného číselného PIN kódu alebo hesla.

Rozsah údajov: Identifikátor zariadenia, stav aktivácie biometrického prihlasovania v aplikácii (príznak zapnuté/vypnuté), čas prihlásenia.

Doba uchovávania: Lokálne nastavenie trvá do odinštalovania aplikácie, odhlásenia používateľa alebo vypnutia funkcie v nastaveniach aplikácie.

Táto doba sa týka iba lokálneho biometrického nastavenia, nie samostatného PIN, hesla alebo ich prihlasovacieho overovacieho údaja. Desaťročná lehota zmluvnej dokumentácie sa na samotné prihlasovacie údaje automaticky nevzťahuje; odlišný potrebný nebiometrický dôkaz konkrétneho zmluvného úkonu sa posudzuje samostatne.

2. Vzdialené biometrické overenie totožnosti (Remote Biometrics) pri aktivácii a zmenách údajov zmluvy

Účel spracúvania: Zriadenie vzdialeného prístupu k osobnému dôchodkovému účtu, aktivácia aplikácie a bezpečná autorizácia zásadných zmien zmluvy o starobnom dôchodkovom sporení (najmä aktualizácia identifikačných, kontaktných a adresných údajov sporiteľa priamo cez aplikáciu) bez nutnosti osobnej návštevy pobočky, vrátane spracovania údajov z predloženého dokladu totožnosti a ochrany pred podvodným konaním a zneužitím identity.

Priebeh vzdialeného overenia:

- Nasnímanie prednej a zadnej strany platného úradného dokladu totožnosti (občiansky preukaz, cestovný pas, doklad o pobyte) fotoaparátom mobilného zariadenia a automatizované vyťaženie údajov z dokladu (OCR);
- Nasnímanie série fotografií tváre sporiteľa (selfie);
- Vykonanie testu živosti (*liveness check*) na overenie prítomnosti živej osoby v reálnom čase (predchádzanie použitiu statickej fotografie, masky alebo videozáznamu);
- Biometrické porovnanie podobizne tváre zhotovenej počas overenia s fotografiou tváre vyťaženej z predloženého dokladu totožnosti a vyhodnotenie miery zhody (*similarity score*).

Upozornenie: Pri procese vyhotovujeme statické snímky vrátane snímok pohybových testov, centrálnych snímok tváre a výrezu fotografie z dokladu totožnosti a spracúvame ich matematické biometrické vektory.

Videozáznam sa nevyhotovuje ani neuchováva. Vzdialené overenie vykonáva DSS vo vlastnom riešení s využitím softvérových komponentov s otvoreným zdrojovým kódom.

Právny základ:

- **Výslovný súhlas dotknutej osoby** podľa čl. 6 ods. 1 písm. a) a čl. 9 ods. 2 písm. a) GDPR na spracúvanie osobitnej kategórie osobných údajov (biometrické údaje – snímky tváre, biometrický vektor tváre, skóre testu živosti a zhody);
- **Splnenie zákonných povinností DSS** podľa čl. 6 ods. 1 písm. c) GDPR v spojení so zákonom č. 43/2004 Z. z. o starobnom dôchodkovom sporení a zákonom č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o financovaní terorizmu (povinná identifikácia a overenie totožnosti klienta);
- **Oprávnený záujem DSS** podľa čl. 6 ods. 1 písm. f) GDPR na bezpečnosti elektronických služieb, predchádzaní neoprávnenému prístupu, zamedzení podvodom a preukazovaní právnych nárokov.

Rozsah údajov: Titul, meno, priezvisko, rodné priezvisko, rodné číslo, dátum a miesto narodenia, pohlavie, štátna príslušnosť, údaje o doklade totožnosti (druh, séria, číslo, platnosť, vydávajúci orgán), adresa trvalého pobytu, kópia/snímka prednej a zadnej strany dokladu totožnosti, snímky tváre, matematické biometrické šablóny (vektory), skóre živosti, skóre zhody, celkový výsledok overenia, dátum a čas overenia, IP adresa a identifikátor požiadavky/relácie.

Dobrovoľnosť a alternatívny postup: Využitie vzdialeného biometrického overenia je pre sporiteľa **plne dobrovoľné**. Ak sporiteľ súhlas neudelí alebo ho odvolá, môže totožnosť overiť alebo zmenu zmluvy vykonať nebiometrickým spôsobom – **osobne na pobočke VÚB banky alebo Generali poisťovne**.

Vekové obmedzenie: Vzdialené biometrické overenie poskytujeme len sporiteľovi, ktorý **dovŕšil 16 rokov** a predloží platný doklad totožnosti. Sporiteľ, ktorý 16 rokov nedovŕšil, vrátane sporiteľa vo veku 15 rokov, nemôže využiť vzdialené biometrické overenie v mobilnej aplikácii; totožnosť overí nebiometrickým spôsobom, najmä osobne na pobočke VÚB banky alebo Generali poisťovne. Toto obmedzenie nemá vplyv na možnosť sporiteľa uzatvoriť zmluvu o starobnom dôchodkovom sporení alebo využívať mobilnú aplikáciu po riadnom overení totožnosti.

Automatizované vyhodnotenie a záruky: Systém vyhodnocuje zhodu tváre a test živosti automatizovane. Neúspešný výsledok automatizovaného overenia nepredstavuje definitívne zamietnutie žiadosti ani stratu prístupu k službe. Klient má v súlade s čl. 22 ods. 3 GDPR právo na preskúmanie výsledku poverenou osobou DSS, právo vyjadriť svoje stanovisko a právo napadnúť výsledok overenia (prostredníctvom infolinky 0850 111 110 alebo e-mailu osobne.udaje@vubgenerali.sk).

Doba uchovávania:

Nedokončené overenie: Obrazové vstupy a technické výstupy spracúvané iba na základe súhlasu vymažeme najneskôr do 30 dní od posledného úkonu. Ide o internú lehotu; konkrétny podklad, ktorý patrí do povinnej AML alebo zmluvnej dokumentácie, má osobitný režim uvedený nižšie.

Úspešné overenie totožnosti: Biometrické šablóny a vektory používame iba počas jednorazového porovnania a po jeho ukončení ich vymažeme. Samostatné obrazové vstupy spracúvané výlučne na základe súhlasu vymažeme najneskôr do 30 dní od ukončenia overenia. Kópiu dokladu totožnosti a nebiometrický záznam o vykonanom AML overení uchovávame počas vzťahu a päť rokov od jeho skončenia podľa § 19 zákona č. 297/2008 Z. z. Na písomnú žiadosť Finančnej spravodajskej jednotky sa lehota v určenom rozsahu môže predĺžiť najviac o ďalších päť rokov.

Oprávnené a nevyhnutné nebiometrické klientske doklady môžu podliehať internému desaťročnému režimu spoločnej zložky sporiteľa opísanému v bode 7 *Informácie o spracúvaní osobných údajov pre klientov VÚB Generali dôchodková správcovská spoločnosť, a.s.* iba v právne odôvodnenom rozsahu. Nejde o zákonnú desaťročnú AML lehotu a samotné uloženie do tejto zložky nestačí na predĺženie zákonnej AML lehoty.

Osobitný AML režim: Ak konkrétny obrazový podklad patrí medzi údaje alebo doklady získané pri zákonnej AML starostlivosti, uplatní sa naň zákonný režim uchovania, nie automatický výmaz po 30 dňoch. Osem obrazových vstupov ani biometrické šablóny neuchovávame plošne päť rokov len preto, že vznikli pri overovaní. Pri prípadnom uchovávaní osobitných kategórií údajov musia byť samostatne splnené aj podmienky čl. 9 GDPR; samotné označenie podkladu ako AML tento základ nevytvára.

Ani interný desaťročný režim zložky sporiteľa neoprávňuje plošne uchovávať všetkých osem obrazových vstupov, selfie, šablóny alebo surové biometrické údaje. Pri každom ponechanom obraze musí existovať konkrétny prípustný účel a nevyhnutnosť.

Odvolanie biometrického súhlasu: Súhlas môžete kedykoľvek odvolať e-mailom na osobne.udaje@vubgenerali.sk alebo písomne na adresu sídla DSS. Odvolanie nemá vplyv na zákonnosť predchádzajúceho spracúvania. Na odvolanom súhlase nevykonávame ďalšie biometrické porovnanie a bez zbytočného odkladu, najneskôr do jedného mesiaca od doručenia odvolania, vymažeme zostávajúce samostatné snímky tváre, výrezy, šablóny a vektory spracúvané výlučne na súhlase; kratšie lehoty zostávajú zachované. Zákonne uchovávaná kópia dokladu vrátane fotografie v doklade a nebiometrické AML alebo zmluvné dôkazy zostávajú uchované v príslušnom rozsahu. Konkrétny ďalší obrazový podklad ponecháme iba na základe skutočnej zákonnej povinnosti a pri splnení príslušných podmienok GDPR.

Dokumentácia o zmene zmluvy: Pokiaľ vygenerovaný záznam o zmene údajov zmluvy tvorí súčasť zmluvného spisu, uchováva sa v režime zložky sporiteľa podľa Hlavných informácií: počas zmluvného vzťahu a do 31. decembra desiateho kalendárneho roka nasledujúceho po roku, v ktorom zmluvný vzťah zanikol alebo bola zmluva právoplatne vyhlásená za neplatnú alebo nevznikla, majetok bol vysporiadaný a zložka sporiteľa bola uzatvorená. Táto lehota automaticky nepredlžuje osobitné lehoty biometrických údajov ani technických záznamov.

3. Viacfaktorová autentifikácia (MFA) prostredníctvom jednorazových SMS a e-mailových kódov (OTP)

Účel spracúvania: Zabezpečenie dvojstupňového / viacfaktorového overenia identity sporiteľa pri prihlasovaní, potvrdzovaní operácií a overovaní kontaktných údajov pred vykonaním zmien v zmluve.

Právny základ: Plnenie zmluvy (čl. 6 ods. 1 písm. b) GDPR), splnenie zákonnej povinnosti DSS (čl. 6 ods. 1 písm. c) GDPR) a oprávnený záujem DSS (čl. 6 ods. 1 písm. f) GDPR) na bezpečnosti elektronickej komunikácie a prevencii podvodov.

Rozsah údajov: Telefónne číslo, e-mailová adresa, vygenerovaný OTP kód, čas vygenerovania a expirácie (TTL), počet pokusov o zadanie kódu, stav overenia (úspešné/neúspešné), identifikátor relácie.

Doba uchovávania: OTP kód je platný len počas určenej časovej lehoty (spravidla niekoľko minút). Kód alebo jeho overovací údaj odstránime po použití alebo uplynutí platnosti; samotný kód neuchovávame ako dlhodobý auditný dôkaz. Samostatný technický záznam o odoslaní, čase, výsledku overenia, počte pokusov a identifikátore požiadavky, bez obsahu kódu, uchovávame 12 mesiacov od udalosti. Bežný OTP audit neukladáme do dlhodobého SIEM archívu. Nebiometrický záznam preukazujúci autorizáciu konkrétneho zmluvného úkonu môže byť súčasťou príslušnej zmluvnej dokumentácie; neobsahuje OTP kód ani biometrické šablóny. Osobitne vyčlenené záznamy ku konkrétnemu incidentu alebo sporu majú režim uvedený v bode 7.

4. Správa zmluvy o SDS a osobných dôchodkových účtov cez mobilnú aplikáciu

Účel spracúvania: Poskytovanie plnej funkcionality elektronickej správy starobného dôchodkového sporenia, najmä:

- Zobrazovanie stavu osobného dôchodkového účtu, aktuálnej hodnoty majetku, počtu a hodnoty dôchodkových jednotiek;
- Zobrazovanie histórie pripísaných povinných a dobrovoľných príspevkov;
- Generovanie a sprístupňovanie ročných výpisov z dôchodkového účtu a potvrdení;

- Zobrazovanie a výpočet prognóz dôchodku a dôchodkového veku;
- Realizácia zmeny dôchodkového fondu, pomeru sporenia a rozloženia majetku (investičnej stratégie);
- Realizácia aktualizácie kontaktných údajov (telefón, e-mail, korešpondenčná adresa);
- Určenie a zmena oprávnených osôb pre prípad úmrtia sporiteľa;
- Podávanie žiadostí o výplatu dôchodku, programový výber alebo vyplácanie výnosu z investovania.

Právny základ: Plnenie zmluvy o starobnom dôchodkovom sporení (čl. 6 ods. 1 písm. b) GDPR) a splnenie zákonných povinností DSS vyplývajúcich zo zákona č. 43/2004 Z. z. o starobnom dôchodkovom sporení (čl. 6 ods. 1 písm. c) GDPR).

Rozsah údajov: Identifikačné a kontaktné údaje sporiteľa, číslo zmluvy, údaje o osobnom dôchodkovom účte, zmluvné nastavenia, zvolené fondy, finančné údaje o transakciách a príspevkoch, prognostické údaje, identifikačné údaje oprávnených osôb (ak boli určené), obsah podaných žiadostí a elektronicky generované dodatky/dokumenty.

Doba uchovávania: Počas trvania zmluvného vzťahu a do 31. decembra desiateho kalendárneho roka nasledujúceho po roku, v ktorom zmluvný vzťah zanikol alebo bola zmluva právoplatne vyhlásená za neplatnú alebo nevznikla, majetok bol vysporiadaný a zložka sporiteľa bola uzatvorená, v súlade s Hlavnými informáciami.

5. Push notifikácie a servisné upozornenia

Účel spracúvania: Doručovanie servisných informácií o stave žiadosti, zmluve alebo osobnom dôchodkovom účte a prípadných bezpečnostných upozornení priamo na mobilné zariadenie sporiteľa. Push notifikácie prostredníctvom mobilnej aplikácie nepoužívame na priamy marketing.

Právny základ: Plnenie zmluvy (čl. 6 ods. 1 písm. b) GDPR) v rozsahu doručovania informácií súvisiacich s poskytovaním zmluvnej služby a oprávnený záujem DSS (čl. 6 ods. 1 písm. f) GDPR) v rozsahu zabezpečenia účtu a predchádzania zneužitiu.

Rozsah údajov: Registračný token zariadenia pre push notifikácie, identifikátor inštalácie alebo aplikácie, text push správy vrátane informácií o stave žiadosti, zmluve alebo účte obsiahnutých v konkrétnom upozornení a technické údaje súvisiace s odoslaním a doručovaním správy. Google/Firebase pri prevádzke služby spracúva aj IP adresu získanú zo sieťovej komunikácie. Spracúvanie teda nie je obmedzené iba na technický údaj o doručení.

Príjemca a doba uchovávania: Na doručovanie push notifikácií používame Firebase Cloud Messaging od spoločnosti Google, ktorej sa na tento účel odovzdáva aj text správy. Registračný token a súvisiace identifikátory uchovávame v systémoch DSS po dobu, počas ktorej sú potrebné na doručovanie notifikácií na príslušné zariadenie; po zániku tejto potreby sa odstránia. Správy čakajúce na doručenie sa uchovávajú počas ich nastavenej technickej platnosti. Na strane Firebase sa identifikátor inštalácie uchováva do vykonania technickej požiadavky na jeho vymazanie; podľa podmienok Google následné odstránenie z aktívnych a záložných systémov prebehne do 180 dní od tejto požiadavky.

Správa notifikácií: Zobrazovanie push notifikácií závisí od systémových nastavení a príslušného povolenia v operačnom systéme Vášho zariadenia. Klient môže zobrazovanie push notifikácií kedykoľvek vypnúť v nastaveniach mobilného telefónu.

6. Priamy marketing a propagačné informácie v aplikácii

Účel spracúvania: Informovanie o novinkách, produktoch a službách DSS a v prípade udelenia osobitného súhlasu aj o produktoch akcionárov a zmluvných partnerov DSS. Tento účel sa uskutočňuje prostredníctvom obsahu a komunikačných kanálov aplikácie; nezahŕňa push notifikácie podľa bodu 5.

Právny základ:

- **Oprávnený záujem DSS** podľa čl. 6 ods. 1 písm. f) GDPR pri priamom marketingu vlastných podobných produktov a služieb DSS voči existujúcim klientom;

- **Súhlas dotknutej osoby** podľa čl. 6 ods. 1 písm. a) GDPR pri ponukách finančných produktov a služieb akcionárov (VÚB, a.s., Generali Česká pojišťovna a.s.) alebo partnerov (napr. Generali Slovenská Distribúcia, a.s.).

Rozsah údajov: Meno, priezvisko, e-mailová adresa, telefónne číslo, klientsky segment, história reakcií na marketingové oznámenia a zaznamenané preferencie/námietky.

Právo namietať a odvolať súhlas:

- **Voči spracúvaniu na účely priameho marketingu na základe oprávneného záujmu má klient právo kedykoľvek bezplatne namietať.** Po vznesení námietky DSS okamžite ukončí zasielanie marketingových správ.
- Udelený súhlas je možné kedykoľvek odvolať v profile v aplikácii, kliknutím na odkaz v správe alebo e-mailom na osobne.udaje@vubgenerali.sk.

Doba uchovávania: Údaje na aktívny marketing používame iba počas príslušného marketingového účelu a v dovolenom rozsahu, najdlhšie do odvolania potrebného súhlasu alebo uplatnenia námietky. Na nevyhnutný klientsky dôkaz súhlasu, odvolania alebo námietky a na evidovanú dokumentáciu kampane sa vzťahuje bod 12 Hlavných informácií. Samostatná história reakcií, segmentácia a operatívna evidencia blokovania sa neposudzujú automaticky podľa desaťročnej lehoty zložky sporiteľa.

7. Technická prevádzka, kybernetická bezpečnosť a auditné logy

Účel spracúvania: Zabezpečenie technického chodu aplikácie, stability, dostupnosti serverovej infraštruktúry, odhaľovanie a vyšetrovanie kybernetických bezpečnostných incidentov, predchádzanie podvodným pokusom a zabezpečenie preukázateľnosti vykonaných právnych úkonov.

Technické nástroje tretích strán: Analytický zber prostredníctvom Firebase Analytics je v mobilnej aplikácii vypnutý. Firebase Analytics nepoužívame na meranie používania aplikácie ani otvorenia alebo reakcií na push notifikácie. Firebase Cloud Messaging používame na doručovanie servisných a prípadných bezpečnostných push notifikácií podľa bodu 5, nie na marketing ani profilovanie používateľov DSS. Tým nie je dotknuté spracúvanie prevádzkových údajov spoločnosťou Google pri poskytovaní, správe a zabezpečení služby podľa jej podmienok.

Právny základ: Oprávnený záujem DSS (čl. 6 ods. 1 písm. f) GDPR) na bezpečnosti sietí a informačných systémov a splnenie zákonných povinností v oblasti kybernetickej bezpečnosti.

Rozsah údajov: IP adresa, typ a model zariadenia, verzia operačného systému, verzia aplikácie, jedinečný identifikátor relácie (session ID), časové pečiatky úkonov, záznamy o chybových stavoch a bezpečnostných udalostiach.

Doba uchovávania: Technické a bezpečnostné logy, ktoré sa neukladajú do systému SIEM, uchovávame spravidla 12 až 24 mesiacov podľa ich povahy. Logy ukladané do SIEM uchovávame 12 mesiacov v aktívnom úložisku a následne ďalších päť rokov na archívnych páskach. Osobitne vyčlenený nevyhnutný dôkaz sa riadi lehotou konkrétneho vecného spisu: päť kalendárnych rokov po roku uzatvorenia sťažnostného alebo samostatného zvyškového compliance spisu, päť rokov po ukončení súdneho sporu alebo desať kalendárnych rokov po roku uzatvorenia auditu. Pri pracovnoprávnom spore sa uplatní jeho osobitná desaťročná lehota po roku uzatvorenia. Tým sa nepredlžuje uchovávanie celého zdrojového logu ani bežného OTP auditu.

Článok IV — Kategórie príjemcov a sprostredkovateľov

Osobné údaje spracúvané v súvislosti s mobilnou aplikáciou môžu byť v nevyhnutnom rozsahu sprístupnené nasledovným kategóriám príjemcov:

- **Sprostredkovatelia a technickí dodávatelia DSS:**
- Poskytovatelia vývoja, údržby, technickej podpory a hostingu mobilnej aplikácie a súvisiacich webových služieb;

- Poverené osoby DSS pri vývoji, prevádzke a kontrole vlastného riešenia vzdialeného overenia; samotné využitie softvérových komponentov s otvoreným zdrojovým kódom neznamená existenciu externého poskytovateľa biometrického overovania ani odovzdanie údajov autorovi komponentu;
- Poskytovatelia SMS brán a komunikačných e-mailových infraštruktúr na distribúciu OTP kódov;
- Poskytovatelia cloudovej, dátovej a serverovej infraštruktúry; primárna aplikačná infraštruktúra DSS je umiestnená v EÚ/EHP, pričom spracúvanie prostredníctvom Firebase Cloud Messaging môže prebiehať v rámci globálnej infraštruktúry Google;
- Poskytovatelia distribučných platforiem mobilných aplikácií a služieb push notifikácií, najmä Apple a Google/Firebase.
- **Spoločnosti finančnej skupiny:** Spoločnosti skupiny Intesa Sanpaolo a skupiny Generali v rozsahu nevyhnutnom na zabezpečenie kybernetickej bezpečnosti, IT architektúry a plnenie zákonných dohľadových a compliance štandardov.
- **Orgány verejnej moci a inštitúcie:** Národná banka Slovenska (NBS), Sociálna poisťovňa, Finančná spravodajská jednotka (FSJ), orgány činné v trestnom konaní, súdy a exekútori, a to v rozsahu ustanovenom všeobecne záväznými právnymi predpismi.

Článok V — Prenos osobných údajov do tretích krajín

- Spracúvanie osobných údajov v mobilnej aplikácii prebieha primárne na území Slovenskej republiky a v členských štátoch Európskej únie / Európskeho hospodárskeho priestoru (EÚ/EHP).
- Pri doručovaní push notifikácií prostredníctvom Firebase Cloud Messaging môžu byť údaje uvedené v článku III bode 5 vrátane textu push správy spracúvané aj mimo EÚ/EHP v rámci globálnej infraštruktúry Google. Pri tejto službe nie je zaručené spracúvanie výlučne v EÚ/EHP.
- Ak dochádza k prenosu osobných údajov mimo EÚ/EHP, DSS zabezpečuje splnenie podmienok kapitoly V GDPR použitím príslušného mechanizmu prenosu a primeraných technických a organizačných ochranných opatrení. Informácie o uplatnených zárukách možno získať kontaktovaním zodpovednej osoby DSS.

Článok VI — Práva dotknutých osôb a spôsob ich uplatnenia

Ako dotknutá osoba máte podľa nariadenia GDPR vo vzťahu k osobným údajom spracúvaným v mobilnej aplikácii nasledovné práva:

Právo na prístup k osobným údajom (čl. 15 GDPR): Máte právo získať potvrdenie, či o Vás osobné údaje spracúvame, a právo na prístup k týmto údajom a podrobným informáciám o ich spracúvaní.

Právo na opravu (čl. 16 GDPR): Máte právo na bezodkladnú opravu nepresných alebo doplnenie neúplných osobných údajov (väčšinu údajov môžete skontrolovať a aktualizovať priamo prostredníctvom mobilnej aplikácie).

Právo na vymazanie („právo na zabudnutie“) (čl. 17 GDPR): Máte právo požadovať vymazanie osobných údajov, ak už nie sú potrebné na účely, na ktoré sa získali, ak odvoláte súhlas a neexistuje iný právny základ, alebo ak boli údaje spracúvané nezákonne. Právo na výmaz sa neuplatní, pokiaľ je spracúvanie potrebné na splnenie zákonnej povinnosti (napr. archivácia podľa zákona o SDS a AML zákona) alebo preukazovanie a obhajobu právnych nárokov.

Právo na obmedzenie spracúvania (čl. 18 GDPR): Máte právo požadovať obmedzenie spracúvania, ak napadnete správnosť údajov, spracúvanie je protiprávne a odmietnete výmaz, alebo ak DSS už údaje nepotrebuje, ale potrebujete ich Vy na uplatnenie právnych nárokov.

Právo na prenosnosť údajov (čl. 20 GDPR): Máte právo získať osobné údaje, ktoré ste nám poskytli na základe súhlasu alebo zmluvy a ktoré spracúvame automatizovane, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte.

Právo namietať (čl. 21 GDPR): Máte právo kedykoľvek namietať proti spracúvaniu osobných údajov vykonávanému na základe oprávneného záujmu DSS (čl. 6 ods. 1 písm. f) GDPR). Ak vznesiete námietku proti spracúvaniu na účely priameho marketingu, Vaše osobné údaje na tento účel okamžite prestaneme spracúvať.

Právo odvolať súhlas: Ak je spracúvanie založené na Vašom súhlase (napr. biometrické overenie totožnosti alebo marketing tretích strán), máte právo svoj súhlas kedykoľvek odvolať. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania vychádzajúceho zo súhlasu pred jeho odvolaním.

- **Práva pri automatizovanom vyhodnocovaní (čl. 22 GDPR):** Pri automatizovanom vyhodnocovaní zhody tváre a testu živosti máte právo na preskúmanie výsledku poverenou osobou DSS, právo vyjadriť svoje stanovisko a právo napadnúť výsledok vyhodnotenia za podmienok uvedených v článku III bode 2.

Ako môžete uplatniť svoje práva:

Svoje žiadosti o uplatnenie práv môžete zaslať:

- **E-mailom:** na adresu osobne.udaje@vubgenerali.sk;
- **Písomne:** na adresu sídla: *VÚB Generali dôchodková správcovská spoločnosť, a. s., Mlynské nivy 1, 820 04 Bratislava*.

V prípade, ak sa domnievate, že pri spracúvaní Vašich osobných údajov došlo k porušeniu platných právnych predpisov o ochrane osobných údajov, máte právo podať sťažnosť alebo návrh na začatie konania dozornému orgánu:

Úrad na ochranu osobných údajov Slovenskej republiky

Galvaniho Business Centrum II

Galvaniho 7/B, 821 04 Bratislava

https://dataprotection.gov.sk/.

Článok VII — Bezpečnosť spracúvania údajov v aplikácii

- DSS priebežne vyhodnocuje riziká spracúvania osobných údajov v aplikácii, určuje potrebné technické a organizačné opatrenia a zabezpečuje ich realizáciu a kontrolu účinnosti. Osobitne posudzuje ochranu dokladov totožnosti a obrazových záznamov z overovania.
- Bezpečnostné opatrenia sa týkajú najmä ochrany komunikácie a uložených údajov, riadenia prístupov, evidencie bezpečnostných udalostí, minimalizácie uchovávaných podkladov a bezpečného vymazávania. Konkrétne nastavenia sa vyhodnocujú podľa povahy spracúvania a zistených rizík.
- Informácie o spracúvaní údajov a uplatňovaní práv možno získať od zodpovednej osoby na kontaktoch uvedených v článku II. Opis bezpečnosti v týchto informáciách nenahrádza priebežné posúdenie rizík ani internú dokumentáciu prijatých opatrení.

Článok VIII — Záverečné ustanovenia

Tieto Informácie o aplikácii podliehajú pravidelnému prehodnocovaniu a v prípade zmien vo funkcionalitách aplikácie, zavedenia nových technológií alebo legislatívnych zmien budú primerane aktualizované. O podstatných zmenách budú používatelia informovaní prostredníctvom mobilnej aplikácie alebo webového sídla DSS.

V Bratislave 13.11.2026