

# Zásady ochrany osobných údajov pre mobilné aplikácie



**mBank.sk**

mBank S.A. koná s maximálnou starostlivosťou o ochranu súkromia súčasných aj potenciálnych zákazníkov využívajúcich bankové mobilné aplikácie. Tento dokument popisuje zásady ochrany osobných údajov mobilných aplikácií mBank S.A. so sídlom vo Varšave (ďalej len „banka“).

## Aké definície používame?

### Naše aplikácie

- Verzia pre iOS - aplikácia je k dispozícii pre mobilné zariadenia s operačným systémom iOS.
- Verzia pre Android - aplikácia je k dispozícii pre mobilné zariadenia s operačným systémom Android a službami Google alebo Android a HMS (Huawei Mobile Services).

### Systémové nastavenia

Individuálna konfigurácia mobilného zariadenia a použitých mobilných aplikácií nainštalovaných v mobilnom zariadení používateľa.

### Token JWT

Webový token JSON je štandard, ktorý definuje spôsob bezpečnej výmeny údajov medzi stránkami prostredníctvom objektu JSON.

## I. Čo ukladáme na mobilných zariadeniach?

1. V našich aplikáciách sú uložené tieto identifikátory:
  - 1.1 šifrovaný jedinečný identifikátor našej aplikácie (parameter sa vytvára v procese registrácie našej aplikácie na strane banky) - uložený v mobilnom zariadení, kým z neho našu aplikáciu neodstránite.
  - 1.2 Identifikátor UUID s tokenom JWT, ktorý umožňuje sledovať udalosti vykonávané v našich aplikáciách - uložené v mobilnom zariadení, kým z mobilného zariadenia neodstránime našu aplikáciu.
2. identifikátory našich aplikácií uvedené v bodoch 1.1. a 1.2. a informácie o značke, modeli a hardvérovom identifikátore mobilného zariadenia sa zasielajú banke v procese registrácie zariadenia v našej aplikácii a používajú sa na jednoznačnú identifikáciu našej aplikácie, mobilného zariadenia a používateľa.

## II. Je komunikácia medzi aplikáciou a mBank bezpečná?

1. Komunikácia medzi našimi aplikáciami a bankou prebieha pomocou šifrovacích mechanizmov.
2. S cieľom splniť bezpečnostné požiadavky vyplývajúce z PSD2 (smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65 / ES, 2009 / 110 / ES, 2013/36 / EÚ a nariadenia (EÚ) č. 1093/2010 a zrušenia smernice 2007/64 / ES a súvisiacich právnych aktov), ktoré súvisia s tzv. silná autentifikácia, banka uplatňuje mechanizmy zamerané na zvýšenie bezpečnosti zákazníkov využívajúcich naše aplikácie, to znamená:
  - 1 / kontrola, či sa v mobilnom zariadení počas spustenia nenachádza malware. Ak sa takýto softvér zistí, naše aplikácie budú z bezpečnostných dôvodov zablokované. V takejto situácii sa do banky zasielajú informácie o detekcii malvéru v mobilnom zariadení (ale do banky sa neposielajú informácie o názve softvéru, ktorý zablokoval naše aplikácie).
  - 2 / kontrola, či došlo k narušeniu továrenského nastavenia zabezpečenia (tzv. Root alebo Jailbreak) na mobilnom zariadení. V takejto situácii naše aplikácie odosielajú tieto informácie do banky, ktorú analyzujeme z hľadiska bezpečnosti transakcií.

## III. K akým prostriedkom zariadenia majú naše aplikácie prístup?

Po udelení súhlasu používateľa majú naše aplikácie prístup k:

1. informáciám o polohe mobilného zariadenia pri vyhľadávaní bankomatov, alebo pobočiek
2. kontaktným údajom v prípade uskutočnenia prevodu na telefónne číslo,
3. kamera a pamäť v prípade skenovania QR kódu,
4. pamäť v prípade ukladania PDF dokumentu s potvrdením transakcie,
5. telefón (na účely spojenia s mLinkou).

## IV. Ako zablokovať prístup k zdrojom zariadení pre naše aplikácie?

V závislosti od verzie mobilnej aplikácie je možné povolenia aplikácie zrušiť zmenou nastavení systému na danom mobilnom zariadení alebo odinštalovaním našich aplikácií.

## V. Aké informácie zhromažďujú naše aplikácie a s akými nástrojmi?

1. Naše aplikácie využívajú sadu nástrojov Firebase spoločnosti Google, ktoré získavajú anonymné informácie, ako napríklad:
  - operačný systém mobilného zariadenia,
  - typ mobilného zariadenia,
  - verzia našej mobilnej aplikácie,
  - jazyk používaný v mobilnom zariadení,
  - kliknutia na prvky našej mobilnej aplikácie,
  - zobrazovanie obrazoviek mobilnej aplikácie,
  - približná poloha mobilného zariadenia, ktoré banka používa na vylepšenie, diagnostiku chýb a optimalizáciu fungovania našich aplikácií.
2. Naše aplikácie so službami Google používajú nástroj Synerise od spoločnosti Synerise S.A. Nástroj funguje v modeli On Premise (na serveroch banky), čo zaisťuje bezpečnosť zhromaždených údajov. Vďaka tomuto riešeniu je banka schopná prispôbiť marketingové ponuky v rámci našich aplikácií konkrétnemu príjemcovi. Údaje ako:
  - operačný systém mobilného zariadenia
  - typ mobilného zariadenia,
  - verzia mobilnej aplikácie,
  - jazyk používaný v mobilnom zariadení,
  - kliknutia na prvky mobilnej aplikácie,
  - zobrazovanie obrazoviek mobilnej aplikácie,

- poloha mobilného zariadenia, získané vďaka tomuto nástroju je možné kombinovať s ďalšími používateľskými údajmi našich aplikácií v závislosti od digitálnych kanálov, ktoré používajú (informačný web [www.mbank.sk](http://www.mbank.sk), systém žiadostí [form.mbank.sk](http://form.mbank.sk) a internet banking [online.mbank.sk](http://online.mbank.sk)).

## VII. Nesúhlasím s politikou ochrany osobných údajov mobilných aplikácií. Čo môžem robiť?

Ak nesúhlasíte s týmito zásadami ochrany osobných údajov, neinštalujte našu aplikáciu, alebo ju odinštalujte.

Tiež vám odporúčame navštíviť [www.mbank.sk/gdpr](http://www.mbank.sk/gdpr), kde sme opísali, ako spracovávame údaje a aké sú vaše práva.