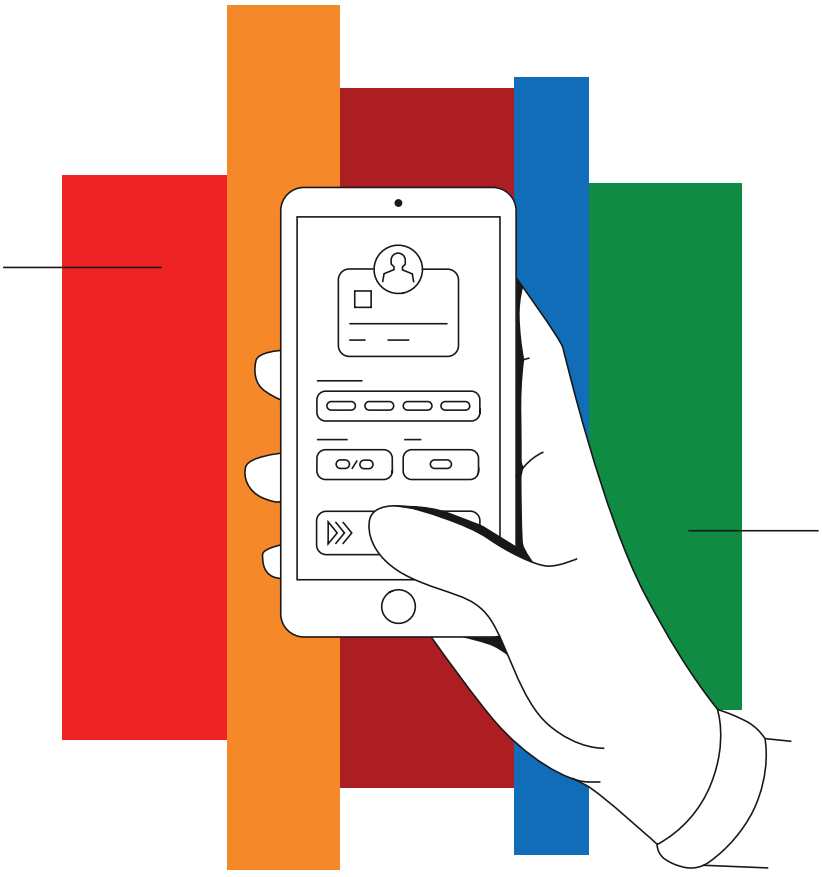
Zásady ochrany osobních údajů pro mobilní aplikace



mBank.cz

mBank S.A. koná s maximální péčí o ochranu soukromí současných i potenciálních zákazníků využívajících bankovní mobilní aplikace. Tento dokument popisuje zásady ochrany osobních údajů mobilních aplikací mBank S.A. se sídlem ve Varšavě (dále jen „banka“).

Jaké definice používáme?

Naše aplikace

- Verze pro iOS - aplikace je k dispozici pro mobilní zařízení s operačním systémem iOS.
- Verze pro Android - aplikace je k dispozici pro mobilní zařízení s operačním systémem Android a službami Google nebo Android a HMS (Huawei Mobile Services).

Systémová nastavení

Individuální konfigurace mobilního zařízení a použitých mobilních aplikací nainstalovaných v mobilním zařízení uživatele.

Token JWT

Webový token JSON je standard, který definuje způsob bezpečné výměny údajů mezi stránkami prostřednictvím objektu JSON.

I. Co ukládáme na mobilních zařízeních?

1. V našich aplikacích jsou uloženy tyto identifikátory:
- **1.1** šifrovaný jedinečný identifikátor naší aplikace (parametr se vytváří v procesu registrace naší aplikace na straně banky) - uložený v mobilním zařízení, dokud z něj naši aplikaci neodstraníte.
- **1.2** UUID s tokenem JWT, který umožňuje sledovat události prováděné v našich aplikacích - uložené v mobilním zařízení, dokud z mobilního zařízení neodstraníme naši aplikaci.

2. identifikátory našich aplikací uvedené v bodech 1.1. a 1.2. a informace o značce, modelu a hardwarovém identifikátoru mobilního zařízení se zasílají bance v procesu registrace zařízení v naší aplikaci a používají se na jednoznačnou identifikaci naší aplikace, mobilního zařízení a uživatele.

II. Je komunikace mezi aplikací a mBank bezpečná?

1. Komunikace mezi našimi aplikacemi a bankou probíhá pomocí šifrovacích mechanismů.

2. Za účelem splnění bezpečnostní požadavky vyplývající z PSD2 (směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65 / ES, 2009/110 / ES, 2013/36 / EU a nařízení (EU) č. 1093/2010 a zrušení směrnice 2007/64 / ES a souvisejících aktů), které souvisí s tzv. silná autentifikace, banka uplatňuje mechanismy zaměřené na zvýšení bezpečnosti zákazníků využívajících naše aplikace, to znamená:
1 / kontrola, zda se v mobilním zařízení během spuštění nenachází malware. Pokud se takový software zjistí, naše aplikace budou z bezpečnostních důvodů zablokovány. V takové situaci se do banky předávají informace o detekci malwaru v mobilním zařízení (ale do banky se neposílají informace o názvu softwaru, který zablokoval naše aplikace).
2 / kontrola, zda došlo k narušení továrního nastavení zabezpečení (tzv. Root nebo Jailbreak) na mobilním zařízení. V takové situaci naše aplikace odesílají tyto informace do banky, kterou analyzujeme z hlediska bezpečnosti transakcí.

III. K jakým prostředkům zařízení mají naše aplikace přístup?

Po udělení souhlasu uživatele mají naše aplikace přístup k:

1. informacím o poloze mobilního zařízení při vyhledávání bankomatů nebo poboček
2. kontaktním údajům v případě uskutečnění převodu na telefonní číslo,
3. kamera a paměť v případě skenování QR kódu,
4. paměť v případě ukládání PDF dokumentu s potvrzením transakce,
5. telefon (pro účely spojení s mLinky).

IV. Jak zablokovat přístup ke zdrojům zařízení pro naše aplikace?

V závislosti na verzi mobilní aplikace lze povolení aplikace zrušit změnou nastavení systému na daném mobilním zařízení nebo odinstalováním našich aplikací.

V. Jaké informace shromažďují naše aplikace a s jakými nástroji?

1. Naše aplikace využívají sadu nástrojů Firebase společnosti Google, které získávají anonymní informace, jako například:
- operační systém mobilního zařízení,
- typ mobilního zařízení,
- verze naší mobilní aplikace,
- jazyk používaný v mobilním zařízení,
- kliknutí na prvky naší mobilní aplikace,
- zobrazování obrazovek mobilní aplikace,
- přibližná poloha mobilního zařízení, které banka používá na vylepšení, diagnostiku chyb a optimalizaci fungování našich aplikací.

2. Naše aplikace se službami Google používají nástroj Synerise od společnosti Syner S.A. Nástroj funguje v modelu On Premise (na serverech banky), což zajišťuje bezpečnost shromážděných údajů. Díky tomuto řešení je banka schopna přizpůsobit marketingové nabídky v rámci našich aplikací konkrétnímu příjemci. Údaje jako:
- operační system mobilního zařízení
- typ mobilního zařízení,
- verze mobilní aplikace,
- jazyk používaný v mobilním zařízení,
- kliknutí na prvky mobilní aplikace,
- zobrazování obrazovek mobilní aplikace,

- poloha mobilního zařízení, získané díky tomuto nástroji lze kombinovat s dalšími uživatelskými údaji našich aplikací v závislosti na digitálních kanálů, které používají (informační web www.mbank.cz, system žádostí form.mbank.cz a internet banking online.mbank.cz).

VII. Nesouhlasím s politikou ochrany osobních údajů mobilních aplikací. Co mohu dělat?

Pokud nesouhlasíte s těmito zásadami ochrany osobních údajů, neinstalujte naši aplikaci nebo ji odinstalujte. Také vám doporučujeme navštívit www.mbank.cz/gdpr, kde jsme popsali, jak zpracováváme údaje a jaká jsou vaše práva.

mBank S.A., se sídlem ul. Prosta 18, 00-850 Varšava, Polská republika, zapsaná ve Vnitrostátním soudním rejstříku (KRS) Rejstříku podnikatelů vedeném u Obvodního soudu hl. m. Varšavy, XIII. hospodářské oddělení, pod číslem KRS0000025237, REGON: 001254524, s úplně splaceným základním kapitálem, jehož výška k 1.1.2021 je 169.468.160 PLN, vykonávající bankovní činnost na území České republiky prostřednictvím pobočky banky mBank S.A., organizační složka, se sídlem Pernerova 691/42, 186 00 Praha 8 – Karlín, IČO: 27943445, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze sp. zn. A 58319.