Privacy Policy - Mobile Applications

(under Articles 13 and 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR))

Controller
Slovenská sporiteľňa, a.s., Tomášikova 48, 832 37 Bratislava, Registration No. 00151653, incorporated in the Commercial Register of District Court Bratislava I, Section: Sa, Insert No. 601/B (hereinafter referred to as "the Bank").
Telephone number: 0850 111 888 e-mail address: info@slsp.sk website: www.slsp.sk

Responsible Person
Head of the Legal Services Division
Correspondence address: Legal Services Division, Slovenská sporiteľňa, a.s., Tomášikova 48, 832 37 Bratislava, e-mail address: osobneudaje@slsp.sk

Mobile Applications
This document explains how the Bank processes personal data specifically in relation to the following mobile applications:

- „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)

and/or in relation to any other mobile applications, desktop applications, internet banking or in general to electronic banking or financial services and products. The owner and operator of the above mentioned mobile applications is the Bank.

This document supplements the main information of the Bank on personal data processing (clients) published on the website of the Bank in section "personal data" (hereinafter referred to as "**Main Information**") and further refers also to mobile applications. The reason is that through or by the virtue of mobile applications, banking products and services are still provided to the clients of the Bank.

The use of mobile applications is reserved for the clients of the Bank and/or representatives of the Bank's clients, while it requires to have a contract on providing banking products and services (e.g. contract on current account) with the Bank. Moreover, some functionalities of the mobile applications are conditioned by the conclusion of a specific contract (e.g. contract on security objects, contract on electronic services) or are covered by the specific business terms and conditions of the Bank (e.g. product business terms and conditions for deposit products). In order for the Bank to meet its obligations under the given contracts or terms and conditions, it is necessary to perform processing of data even through the mobile applications.

Purpose and Legal Basis for Personal Data Processing
Within the framework of mobile application, personal data is processed primarily for the purposes of providing banking products and services, while the basis for personal data processing for the above mentioned purpose is (depending on what processing activity is concerned):

- consent of the data subject according to Article 6 (1) a) or Article 9 (2) a) of GDPR;
- performance of a contract with the data subject according to Article 6 (1) b) of GDPR;
- meeting a statutory obligation according to Article 6 (1) c) of GDPR;
- legitimate interest according to Article 6 (1) f) of GDPR.

In mobile applications (but mainly in relation to the application "SLSP mToken") there is also personal data processing for the purpose of (i) performing security measures to prevent frauds on the legal base of performing the statutory obligation according to Article 6 (1) c) of GDPR, and simultaneously on the legal base of legitimate interest according to Article 6 (1) f) of GDPR.

Other relevant purposes of processing, legal bases for processing of personal data, as well as legitimate interests pursued by the Bank result from the Main Information.

Legitimate Interests Pursued
In case of the following purposes, we also rely on the legal basis of the legitimate interest according to Article 6 (1)

f) of GDPR. Below you will find explanation of the legitimate interests pursued by us.

Purpose of Processing	Explanation of Legitimate Interest
Performing Security Measures to Prevent Frauds	*We consider the adoption and performance of security measures in order to protect the Bank and its clients using the banking electronic services from cyber threats, cyberattacks, frauds, malicious codes, compromising of information security, including the monitoring and analysing of fraudulent operations with funds, ensuring strong authentication of clients when entering into the mobile application George, internet banking, third-party interface, when entering or conforming payment orders or in case of other operations made remotely, which represent a high threat risk to be our legitimate interest.*

Advice: The data subject has the right to object to the processing of their personal data based on legitimate or public interest, as well as to processing for the purpose of direct marketing, including objection to related profiling pursuant to Article 21 of GDPR. If the data subject granted their consent to the processing of personal data to the Bank, they have the right to revoke it, while this revocation has no impact on the legitimacy of processing based on the consent prior to its revocation.

Obligation to Provide Personal Data

The provision of personal data by the data subject as a mobile application user is voluntary since the actual use of the mobile application is voluntary. However, without the provision of certain personal data or without the conclusion of a contract with the Bank, it is not possible to use all the functionalities of the mobile applications. It is so due to the reason that the Bank is obliged to verify the identity of the user before entering the protected environment of banking mobile applications. If the client refuses to provide their personal data required based on special legal regulations, the Bank will refuse to perform the banking transaction. If the client refuses to provide their personal data to the Bank, which represent a contractual requirement, no contract may be concluded with them. If the client refuses to provide their personal data to the Bank, which is necessary for the processing and is based on a consent, no such processing may take place.

Data that the Applications Have Access to

According to the rules of Google, mobile applications also obtain some of the so-called *"personal and sensitive information".* According to Google, such information include, inter alia: any personal data; financial and payment data; authentication information; or sensor data related to the camera.

If the mobile application requires **access to the camera** of the mobile device, it does so in order to enable making of a payment by scanning for example of the QR code, money order or bar code or in order to verify your identity, e.g. when opening an account without being present at the branch. At the same time, this way we make sure that we communicate with a living (real) person. If you enable this access for us, it does not give us the right to access the photographs saved in the device and you do not need to worry about them.

If the mobile application requires the use of **Face recognition (for example FaceID)** functionality on Apple or Android devices, the Bank does not have access to the actual photograph or to any biometric data. They remain processed only through your mobile device and the companies Apple Inc. or Google. By the virtue of Face recognition, the Bank practically asks your mobile device whether it is actually really you. You can completely disable the use of Face recognition in the settings of your device or enable/disable this functionality only for certain applications. You can find more information on Face recognition, as well as on the setting of the said feature here:

- https://support.apple.com/sk-sk/HT208108
- https://support.apple.com/sk-sk/HT208109
- https://source.android.com/security/biometric

If the mobile application processes the **GPS location of the device**, it does so either in order to identify anomalies indicating fraudulent behaviour or any other malicious activities, to enable a functionality that is directly connected to the location of the device (e.g. offer of currency calculator with pre-set currency based on the location) or due to the increase of service security in general (e.g. when signing the payments). The application user may at any time enable or disable the recording of GPS location of their device.

When using the application mToken, also the **condition of the telephone** is being monitored. The aim is to protect the client and the Bank from any fraudulent or malicious activities. As part of the condition of the telephone, it is recorded and analysed whether other applications have inadequately strong authorisation or whether such incidents are related to them, which could indicate the presence of a fraud or malicious code (e.g. Root/Jailbreak – iOS, Android; Fingerprint – iOS, Android; SMS hijacking – Android; Overlay detection – Android; Emulator detection – Android, Human checks – Android; Debugger detection – Android).

Apart from that, mobile applications process the login data of the user, identification or authentication credentials, data related to the use of applications and mainly entering commands or instructions in relation to payment functionalities and all generally processed personal data in the banking environment (e.g. account balances, movements, payments, etc.).

Mobile applications save two files of cookies to your device; one with the term of use for 1 year and the second one with the term of use for 24 hours. These files are saved in the device through the SDK (software development kit) of the mobile application or JAVA script (so-called snippet) of the web application (internet banking). If the client blocks the saving of cookies on their devices, it does not automatically mean the rejection of service provision but the missing identifier means an increased level of risk, which may result in requesting additional authentication. Only the Bank has access to these files; however, in the environment of the Bank, other (verified) suppliers may work with the information obtained through these files such as the company ThreatMark s.r.o. These files serve exclusively for the purpose of performing security measures for fraud prevention.

We would like to assure you that none of the above mentioned files serve for your monitoring, sale to third parties or marketing. All the processed data is retained exclusively for the necessary time, in a secure manner and only in the necessary scope. In the final end, this information is processed by us in order to protect your from frauds and malicious codes.

Source of Personal Data
Mobile applications obtain the data from you and/or through communication with your device.

Period of Data Retention
In general, the above mentioned data is obtained only during the period when the mobile application is installed and used and only provided that the user enabled the obtaining of sensitive information through the settings of the device. Cookies related to mobile applications have the use term set for 1 year and 24 hours. However, the Bank retains some of the information gained through mobile applications or cookies for a period of 12 years, and that for the purpose of providing banking products and services and performing security measures to prevent frauds.

Personal Data Recipients
Authorised employees of the IS Security Management Department and verified suppliers of the Bank in the field of security (mainly the company ThreatMark s.r.o.) have access to the data processed.

Cross-border Transfer of Personal Data
In relation to mobile applications, the Bank does not perform any cross-border transfers of personal data to third countries (i.e. outside the EU, Norway, Iceland and Lichtenstein).

Rights of the Person Concerned in the Personal Data Processing
The client as a data subject has the right mainly to require from the Bank as controller the following:
- access to personal data according to Article 15 of GDPR;
- correcting incorrect and supplementing incomplete personal data according to Article 16 of GDPR;
- deletion of personal data processed by the Bank according to Article 17 of GDPR;
- restriction of processing of personal data according to Article 18 of GDPR;
- transmission / portability of data provided to the Bank according to Article 20 of GDPR in a structured, machine-readable format, which are automated and are processed under contract or consent.

The person concerned has the right:
- to object to the processing of personal data processed by the Bank on the legal basis of the protection of legitimate interests, including profiling and direct marketing according to Article 21 of GDPR;
- request not to apply automated individual decision-making to them under the terms and conditions stipulated in Article 22 of GDPR;
- to revoke consent to the processing of personal data,
- file a complaint to the supervisory authority, which is the Office for Personal Data Protection of the Slovak Republic, and/or an application initiating proceedings pursuant to Section 100 of the Act No. 18/2018 Coll. on personal data protection.

Automated Decision-making and Profiling
For the purpose of properly targeted offer of banking products and services, as well as for the purpose of providing appropriate banking products and services to the client, so that the real needs of the clients, as well as their solvency and the possibilities for providing such a product (mainly loan products) are taken into consideration, for the purpose of evaluating the risk-rate of banking transactions, the Bank uses, in the process of product approval, as well as in the process of selecting clients for the targeted offer of products and services, some of the forms of automated decision-making and profiling.

The client is entitled not to apply a decision made exclusively based on automated individual decision-making (i.e. algorithm-based decision of a computer program without any human intervention) to them and demand appropriate measures to be taken by the Bank (e.g. human intervention by the Bank, possibility to express their opinion or legal challenge to the decision in question). The above mentioned does not apply if the decision is permitted by EU law

or the law of the Slovak Republic, and which, at the same time, also determines measures guaranteeing the protection of rights and freedoms and legitimate interests of the data subject.

Code of Conduct

In compliance with Article 40 of GDPR, the Bank plans to make available (after approval by the Office for Personal Data Protection of the Slovak Republic) the Code of Conduct prepared by the Slovak Banking Association for the banking sector, whose wording following its approval will be available on the website of the Bank, on the website of the Slovak Banking Association (www.sbaonline.sk), as well as on the website of the Office for Personal Data Protection of the Slovak Republic (www.uoou.sk).

Validity and Effect

This document is effective from 13 September 2019 and each of its version is effective by its publishing on the website of the Bank, in the app store or in the mobile application. The Bank reserves the right to unilaterally amend this information and the Bank shall inform the data subjects of substantial changes in an appropriate manner, e.g. by a notice in the mobile application. If the changes are not of substantial nature, the Bank shall publish the new version of information at the same place where the original version is.