SPARKASSE
Bank Malta plc

101, Townsquare, Ix-Xatt ta' Qui-si Sana, Sliema SLM 3112

Tel: (+356) 2133 5705 – info@sparkasse-bank-malta.com – www.sparkasse-bank-malta.com

SPAR KEY – PRIVACY NOTICE

Version: July 2019

Personal information collected by or through the Spar Key App (the "**App**") and the Online Services to which the App gives access will be processed in accordance with the provisions of the Data Protection Act (Chapter 586 of the Laws of Malta) and General Data Protection Regulation (Regulation (EU) 2016/679; "**GDPR**"). Information on the purpose(s) and legal basis for processing of personal data, to whom the information may be disclosed, and the rights of data subjects is given in the General Data Protection Notice to Customers and below.

While general information regarding data protection under the GDPR is given in the General Data Protection Notice to Customers, additional information specifically related the App and the exchange of information between the App and the Online Services is given in this Spar Key Privacy Notice; it also contains information which the Bank is required to give pursuant to the Processing of Personal Data (Electronic Communications Sector) Regulations (S.L. 586.01) (the "**ePrivacy Regulations**").

Words and expressions used in this Spar Key Privacy Notice have the meaning given to them in the Glossary to the General Terms and Conditions for Banking Services (available from our Website), unless stated otherwise. The term "**personal data**" means any information in relation to an identified or identifiable individual (natural person), who is referred to as the "**data subject**". The term "**processing**" includes various types of operations such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data. The "**controller**" of personal data in terms of the GDPR is essentially the person or entity who determines the purpose (why) and means (how) of the processing of personal data.

Types of information processed via the App

Apart from the information provided by the Customer or User when applying for the Online Services and the use of the App, the Bank will access, collect, transmit, analyse, store and otherwise process the types of information summarised below via the App.

The App temporarily stores certain cryptographic information in the form of a virtual smart card generated via the underlying technology. The App technology features a device binding mechanism to link the device to the relevant user profile on the Bank's Online Services.

The use of the App requires the use of security credentials created by you on your device, namely a PIN and, where enabled, a fingerprint (optional), but the Bank will not be able to view or have access to these data.

The Bank collects, transmit and makes use of the following types of data via the App:

Type of data	**Description**
IP address	the public IP address of the device on which the App is installed;
Geo-location	the latitude and longitude of the device on which the App is installed;*

Device information	vendor, type of device, serial number, type of operation system (OS) and processor type;
Security information	device configuration data related to security features, including whether the device was 'jailbroken', 'rooted' or runs in debug mode;
Identification details	user identification number assigned by the Bank (entered as a "Username" in the App);
App information	version of the App installed on the device;
Authentication information	messages related to actions to be authorized sent by the Bank and received through the App (e.g. authentication code), and messages granting or refusing authorization sent to the Bank through the App (e.g. digital signature);
Log-in details	timestamps of log-in and log-out of the App;

(*) The source of location information on the device will depend on how you configure your device and permission settings, and the Bank will not have control over the source of location data.

For security purposes, in particular transaction monitoring, the Bank may use the following types of information, which are not necessarily collected through the App itself, but may be provided by the Customer or User through other means or generated through the Bank's systems: (i) information on compromised or stolen authentication elements; (ii) amounts of payment transactions; (iii) information to identify known fraud scenarios in the provision of payment services; (iv) signs of malware infection in any sessions of the authentication procedure; (v) logs of the use of the device or the App and the abnormal use of the device or the App.

Why information is processed through the App

The purposes for processing of information collected via the App, or exchanged between the device on which the App is installed and the Bank's infrastructure for the Online Services, are explained below. The legal basis for processing the information will be one or more of the following:

(i) to enter into or perform a contract, including the Bank's standard terms and conditions for the provision of banking and, or investment services and the use of the Online Services;

(ii) compliance with a legal or regulatory obligation to which the Bank is subject, in particular under regulatory requirements for the provision of payment services, investment services and other regulated activities carried out by the Bank, and laws requiring the Bank to adopt security measures related to the Online Services;

(iii) legitimate interests pursued by the Bank or by a third party: the Bank's legitimate interests will generally be the protection and management of the business and financial interests, reputation and risk exposures of the Bank, and third party's legitimate interests will be mainly those of other payment services users, payment service providers, counterparties to transactions in financial instruments and their financial services providers, correspondent banks and other intermediaries involved in financial transactions.

Insofar as the App stores information or gives access to information stored in the device on which it is installed, the processing of such information will be limited to the technical storage or access for the sole purpose of carrying out or facilitating the transmission of communications between the device on which the App is installed and the Bank's systems, or as may be strictly necessary in order for the Bank to provide an the Online Services requested by the Customer or the User on the Customer's behalf.

Processing of information by or through the App, whether or not in combination with the Online Services, will generally not require consent. The Bank is not in a position to provide the Online Services to Customers and Users without accessing, collecting, analysing, storing, using and otherwise processing information via the App.

Information is processed via the App for the following purposes:

Installation and activation of the App

You will need the identification number provided by the Bank and an activation code (these may be combined in a QR code, for mobile devices), in order to activate the App.

You will need to create a PIN code to open and use the App; if your device and your permission settings allow it, you may also use fingerprint recognition.

Authentication

The Bank is required by law to apply strong customer authentication where the Customer, as payer, accesses its payment accounts through the Online Services, initiates a payment transaction through the Online Services or carries out any action through the Online Services which may imply a risk of payment fraud or other abuses. Where the Online Services are used to access portfolio accounts or to give instructions for transactions in financial instruments, the Bank is also required by law to have systems and procedures that are adequate to safeguard the security, integrity and confidentiality of information.

The Bank therefore requires the use of an authentication procedure to access and give certain instructions through the Online Services; this procedure involves the use of the App. The App comprises authentication software and the Customer or User is required to install and activate the App as an application on a mobile or desk top device that belongs, or is assigned to, the Customer or User.

Information is exchanged between the device on which the App is installed and the Bank's systems for authentication purposes, and also to facilitate other security measures which the Bank is required to take, such as transaction monitoring (explained below).

Transaction monitoring

The Bank is required to carry out transaction monitoring so that it is able to detect unauthorised or fraudulent payment transactions related to the authentication procedure mentioned above. Transaction monitoring is based on the analysis of payment transactions, taking into account elements which are typical of the Customer or the User in the circumstances of a normal use of the personalised security credentials. This will involve the collection and processing of information regarding your authentication

elements, payment transactions, information about the device on which the App is installed and a log of the use of the App and the device on which it is installed. This form of "profiling" entails automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to the Customer or User, in particular to analyse aspects concerning his or her transactions, location and use of the App. If anything unusual is detected that the Bank considers relevant for security purposes, the Bank will be alerted, analyse the circumstances and decide on any measures to be taken. Measures the Bank may take if the Bank suspects unauthorised or fraudulent behaviour, include, for example, contacting the Customer or User to confirm the instructions given, suspending or blocking the instruction or account(s) of the Customer, or temporarily or permanently blocking authentication. The Bank may also be required to report to the relevant competent authorities.

Alerts

The Bank may use information collected via the App and the Online Services in order to trigger and send any alerts to Customers.

Maintenance and support

The App will give access to information about your device and the App in order to allow the Bank to ensure that the App functions properly and that the user is informed when the App requires updating or replacing.

Testing, training and improvement of services or products

The Bank may use information about the use of the App and devices on which it is installed, to improve the Online Services, to test upgrades and new versions of the App, and to train staff.

Disclosure to regulatory authorities

The Bank may be required to disclose or report information to the Malta Financial Services Authority, the Central Bank of Malta or other competent authorities, in Malta or other jurisdictions.

Sharing of information

The Bank may be required to disclose or report information to the Malta Financial Services Authority, the Central Bank of Malta or other competent authorities, in Malta or other jurisdictions.

Certain service providers of the Bank (e.g. auditors) may require access to information collected via the App or the Online Services.

International transfer of personal data

The App is made available through the "stores" provided by Apple and Google, which may have servers based outside the EEA.

The exchange of information between the Customer's or User's device on which the App is installed and the Bank's systems, which operate on servers in Malta, may involve the international transfer of personal data if the device is located outside Malta.

Duration of processing and storage of information

The App itself does not retain data in storage; except for the virtual smart card which is used only for the duration of each session.

Information on access to and use of the Online Services, including the use of the App and device on which it is installed, will be stored on the Bank's servers in accordance with the retention policy explained in the General Data Protection Notice to Customers, unless otherwise required by law or a competent authority.

Automated decision-making

While transaction monitoring may entail a form of "profiling", as explained above, decision making will not be based solely on automated processing, and will require human intervention.

Data subjects' rights

As a data subject you have the following rights under the GDPR:

(i) to access your personal data;
(ii) to rectify inaccurate personal data about you;
(iii) to have the Bank erase your personal data;
(iv) to ask the Bank to restrict use of your personal data;
(v) the right to 'data portability';
(vi) to object to the Bank processing your personal data;
(vii) to lodge a complaint with the relevant supervisory authority.

The nature of these rights and the conditions under which they can be exercised are explained in the General Data Protection Notice to Customers.

As no consent to process personal data is being relied on in relation to the App, the right to withdraw consent does not apply.

Installing and using the App involves storing of information, and obtaining access to limited information stored in the device on which the App is installed (as outlined earlier). The Bank does not require your consent for this as it requires the information in order to transmit communications between your device and the Bank's system, and for the Bank to provide the Online Services (and the services and products to which the Online Services give access) to the Customer or the User acting on the Customer's behalf.

Updates to this Notice

This Notice may be amended from time to time, for example, if there are changes in the processing activities of the Bank, due to legal and regulatory developments or guidance issued by a competent authority or to clarify information given.

A copy of the latest version of this Notice will be available from our Website and will be provided upon request (our contact details are given below). If changes to this Notice have a significant impact on the nature of processing or data subjects concerned, we will give advance notice.

Contact information

Individuals who have any questions about this Notice or would like more information about their rights or wish to exercise them, may submit a request by e-mail to: dataprotection@sparkasse-bank-malta.com; or by mail to: Attn: Compliance Department; Sparkasse Bank Malta p.l.c.; 101 Townsquare, Ix-Xatt ta' Qui-si-Sana; Sliema SLM3112; Malta

The contact details of the Bank's Data Protection Officer (DPO) are:

E-mail: dpo@sparkasse-bank-malta.com

Mail: The Data Protection Officer; Sparkasse Bank Malta p.l.c; 101 Townsquare, Ix-Xatt ta' Qui-si-Sana; Sliema SLM3112; Malta