GENERAL DATA PROTECTION NOTICE TO CUSTOMERS

Sparkasse Bank Malta public limited company (the "**Bank**", "**we**" or "**us**") has prepared this Notice in order to provide information to existing and prospective Customers, Signatories, Users of the Online Services and the Spar Key App and other individuals (natural persons) related to them whose information may be collected in relation to banking, investment and other services and products offered or provided by the Bank, in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679; "**GDPR**").

The information given in this Notice applies to the processing of information in relation to private Customers (individuals) and corporate Customers (legal entities) of the Bank, as well as individuals related to them, in general. A specific privacy notice applies to the Spar Key App (the "**App**") and the Online Services to which the App gives access (the Spar Key Privacy Notice, available from our Website). Other notices and information may be given separately for particular products or services or for specific purposes, e.g. the use of our Website or CCTV monitoring at the Bank's offices.

Capitalised words and expressions used in this 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. When we refer to "**personal data**", this 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 Bank is a "**controller**" of personal data in terms of the GDPR which means that it determines the purpose (why) and means (how) of the processing of personal data.

1. Types of personal data processed by the Bank

Data subjects whose data the Bank may process include existing, future and former Customers, if they are individuals themselves, and individuals who are connected to existing, future and former private and corporate Customers such as Signatories, Users of the App and the Online Services or representatives of the Customer and, in the case of corporate Customers, directors, officers, employees, individual shareholders and ultimate beneficial owners.

The Bank collects and processes different types of personal data depending on the type of service or product applied for or provided: general banking and investment services, e.g. the opening and maintenance of cash accounts (including payments made to and from accounts), the opening and maintenance of portfolio accounts (including transactions in securities), spot foreign exchange, credit cards and pre-paid cards, fixed term deposits, precious metals, loans, overdrafts and other types of credit facilities, the Bank's online services, as well as specialised services available to certain types of corporate Customers such as depositary and custody services, fiduciary accounts, foreign exchange derivative transactions and collateral management.

The Bank processes personal data collected directly from the individuals concerned, and indirectly from other sources.

The Bank will collect various types of personal data directly from prospective and existing Customers and individuals connected to them, including the following:

Type of information	**Examples**
Identification data	Name and surname, date of birth, place of birth, nationality, country of citizenship, identity card or passport information, tax identification number.
Contact information	Residential address, personal and/or work telephone number, personal and/work mobile number, e-mail address.
Financial information	Source of funds and source of wealth, use of credit and pre-paid cards obtained through the Bank and, in cases where the Bank is required to assess the suitability of transactions in financial instruments, information on financial transactions, financial situation and investment objectives.
Tax status	Country of tax residence, CRS form and US taxpayer declaration for FATCA purposes, beneficial ownership in the case of nominee / custody services.
Professional life information	For investment services, information on employment or professional status, information on education and qualifications, experience in the field of financial services.
Transaction data	Data relating to transactions carried out on the account, such as the IBAN, name of beneficiary, name of remitter, payment amount, payment details.
Transaction information	Instructions and communications regarding payment transactions, trades in financial instruments and corporate actions.
Account data	Data on all aspects of the account, other than transaction data; e.g. withholding tax instructions, opening of account details, contact details and residence status.
Account information	Application forms for the accounts and products and services applied for, signature card, letter of indemnity, FATCA Compliance Declaration, CRS Form.
Personal life information	Information to determine if the Customer is a "politically exposed person" in terms of anti-money laundering legislation and verification as to whether the Customer holds a public profile, and for investment services, information on the marital status.
Correspondence	E-mails and mail for the opening and operation of accounts, provision of services and products, requests for information, enquiries and complaints.
Connection data	Log-in to the Online Services, User ID and Password, use of the Online Services.
Market abuse information	For investment services, information to determine insider status.

Recordings of telephone conversations	Telephone number, verification of the identity of the caller / responder and transaction related data.

The Bank may also collect information about data subjects indirectly from other sources, including the following:

Source	**Type of information**
The Bank's own systems and records	Information on the use of accounts, services, transactions or products generated by the Bank or kept in the Bank's records through the Online Services, systems, applications and programmes, or manually created.
The Customer, joint account holders or persons related to the Customer providing information on other persons	Information provided about individuals related or authorised to represent, sign, use the Online Services or who may have access to information about the Customer, or who are a joint account holder together with the Customer. In the case of corporate Customers, this includes information on shareholders, ultimate beneficiary owners, directors and authorised employees.
Holders of a Power of Attorney or other form of mandate, Signatories, Users, referrers of business and other representatives	Information on the (other) representatives of the Customer as well as transaction information and communications about the Customer on whose behalf the representative acts.
Service providers of the Customer	Information on the use of credit and pre-paid cards obtained through the Bank from the card issuer, instructions and communications from investment advisors or managers, information for transfer in or transfer out of assets.
Remitting, receiving and correspondent banks and other financial institutions and intermediaries involved in payment transactions	Information on the payer and other details regarding payments remitted to or received into an account.
Banks and other persons providing references in respect of a (prospective) Customer	Bank references, bank statements, professional references.
Pledgees and other persons in whose favour a security interest is created over the Customer's accounts or assets held with the Bank	Notices of events of default, enforcement actions, including transaction information and communications on behalf of the Customer.
Regulatory and supervisory authorities, administrative bodies, courts and law enforcement bodies	Information on regulatory status, regulatory sanctions, investigations, requests for information or other procedures in respect of the Customer, court and administrative orders.

Publicly accessible sources, such as: - Google and other search engines, - Online and paper media, - World-Check - Supervisory and regulatory authorities' websites - Company registers - Sanctions and embargo lists	Newspaper articles, information on investigations, criminal, civil or administrative proceedings, convictions, penalties, regulatory status, involved persons, business websites of the Customer or related persons.
UBO Registers maintained in Malta by the Registrar of Companies (or in another country, if publicly accessible)	Information on ultimate beneficial owners of Customers.
Referrers of business	Details of a prospective, existing or former Customer, types of accounts, services and products required.

If a Customer or other person provides the Bank with information regarding another individual, the Customer or person providing the information should make sure that the individual concerned is aware of it and is provided with a copy of, or made aware of the contents of, this Notice.

For information about the types of data processed in connection with the App and the Online Services, please refer to the Spar Key Privacy Notice.

Mandatory information

If we are not provided with certain personal data which we indicate to be mandatory, then we may not be able to provide the relevant service or product, enter into a contract and, or perform all our obligations under the applicable terms and conditions or agreement (contractual requirements) or at law (statutory requirements). In those cases, we may decide not to provide the service or product requested, restrict access, impose limits, suspend or terminate the service or product or terminate the relationship.

Specifically regarding tax, if the Bank does not have the necessary information, this may lead to tax being withheld or higher taxes and charges being levied.

2. Why the Bank processes personal data

The table below indicates why we process personal data (listed under "**Purpose**") and the legal basis for doing so (listed under "**Legal basis**"), which will in most cases be one or more of the following:

(i) to enter into or perform a contract, including the Bank's standard terms and conditions and other specific agreements which may be entered into for the provision of services or products by the Bank, including the use of the App and the Online Services (marked below as "**Contract**");

(ii) compliance with a legal or regulatory obligation to which the Bank is subject (marked below as "**Law**");

(iii) legitimate interests pursued by the Bank or by a third party (marked below as "**Legitimate Interests**"): in this case, 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, or other legitimate interests which may be indicated below;

(iv) consent to the processing of personal data for one or more specific purposes (marked below as "**Consent**").

Purpose	Legal basis
On-boarding of a prospective Customer	Contract; Law; Legitimate Interests.
Opening and maintenance of accounts, including execution of payment orders and execution, transmission of orders in relation to financial instruments	Contract; Law; Legitimate Interests.
Provision of investment advice, including suitability or appropriateness assessment	Contract; Law.
Tailoring and providing (other) services and products (e.g. depositary / custody services, loans, overdrafts and other types of credit facilities, FX spot or derivative transactions)	Contract; Law; Legitimate Interests.
Communications regarding services and products or to provide information for legal, regulatory or contractual purposes	Contract; Law; Legitimate Interests.
On-going monitoring and due diligence, particularly for the prevention and detection of fraud, money laundering and terrorism funding and other crimes, including monitoring of sanctions and embargos, and transaction monitoring to detect unauthorised or fraudulent transactions or other abuses	Contract; Law; Legitimate Interests (also: public interest).
Blocking, suspension or closure of accounts, restriction of access, transaction limits, termination of services or products	Contract; Law; Legitimate Interests.
Handling of requests for information, queries, complaints and dispute resolution, and taking remedial action	Contract; Law; Legitimate Interests (also: preventing incidents that could lead to complaints from other Customers or other persons).
Security checks, including identification, verification of identity and authentication of access, instructions or requests	Contract; Law; Legitimate Interests (also: preventing and detecting unauthorised access to the Bank's systems and other security breaches in the interests of the Bank, Customers and other persons who may be affected by such breach).
Business analysis, research and statistics for the evaluation, development and improvement of the Bank's business model and strategy and, or the Bank's systems, products and services	Legitimate Interests.
Measurement and management of credit risk exposures related to overdrawn balances and loans, overdrafts and other types of credit facilities	Contract; Law; Legitimate Interests.

Logging of defaults and notification of defaults to the Customer and, or third parties	Contract; Law; Legitimate Interests (also: legitimate interests of secured third parties, such as pledgees, and investors).
Reporting to tax authorities, regulators, supervisory authorities and other competent bodies	Contract; Law.
Compliance with legal and regulatory obligations under applicable law, including cooperation with tax authorities, regulators, supervisory authorities and other competent bodies and law enforcement bodies and compliance with administrative and court orders and requests from or other actions taken by law enforcement bodies	Law.
Recording of telephone conversations	Contract; Law; Legitimate Interests.
Training (e.g. trainees and new staff members)	Legitimate Interests.
Maintenance, development, improvement and testing of systems, applications, software and hardware, analysis of services and products	Law; Legitimate Interests.
Business continuity, including back-ups	Law; Legitimate Interests.
Archiving	Law; Legitimate Interests.
Debt recovery, handling and enforcement of legal claims, administrative or court proceedings	Contract; Law; Legitimate Interests.
Marketing communications about services or products offered by the Bank	Consent.

Special categories of data

Some of the information processed by the Bank belongs to special categories of personal data which enjoy stronger protection than other types of data under the GDPR. The Bank may process certain sensitive data, such as personal data revealing political opinions and data concerning health, and also personal data relating to criminal convictions and offences or related security measures.

Purpose	**Legal basis**
Initial and on-going customer due diligence checks: determination of whether or not the Customer and certain persons related to the Customer are "politically exposed persons" in terms of prevention of money laundering and terrorism financing legislation	Processing of sensitive data is necessary for reasons of substantial public interest on the basis of EU or national law, or relates to data that are manifestly made public by the data subject.
Initial and on-going due diligence checks: due diligence checks via Worldcheck, Google searches,	Processing of personal data relating to criminal convictions and offences or related security measures authorised by law, in particular

databases of regulatory or supervisory authorities, and other publicly accessible sources	prevention of money laundering and terrorism financing legislation and directions, orders or other measures taken by a regulatory or supervisory authority, court or law enforcement body.
Provision and tailoring of products and services (including investment advice and, or other investment services) to vulnerable customers or customers requiring personalised communication or assistance based on medical or health grounds (e.g. hard of hearing or poor eyesight)	Processing of sensitive data is based on explicit consent or necessary for reasons of substantial public interest on the basis of EU or national law.

Direct marketing

The Bank requires consent for processing of personal data in relation to direct marketing. Generally, consent is requested upon account opening and the necessary information provided in order to be able to give, decline or withdraw consent. Direct marketing gives the Bank the opportunity to make Customers aware of any new products and services which might be of interest to them. The information collected through marketing activities enables to Bank to improve its services and provide Customers with suitable products and services. As a rule, the Bank we will not send any unsolicited communications by means of an automatic calling machine, fax or electronic mail (including via the Online Services) for third parties or other direct marketing purposes unless prior consent in writing is given.

Cookies for the use of Online Services

We use cookies for our Online Services; a cookie is a small text file stored on the browser of the person who accesses the Online Services. Cookies are used when the Customer, Signatory or User logs in, to allow the Bank to ensure that the session is authenticated. The cookies used in this way are not stored after the Customer, Signatory or User logs out. For information about the use of cookies, please refer to the Cookie Notice available from our Website.

For information about processing of personal data in connection with the App and the Online Services, please refer to the Spar Key Privacy Notice.

Processing of personal data for the provision of payment services

In terms of PSD2 and Directive No 1 of the Central Bank of Malta on the provision and use of payment services, payment systems and payment service providers are permitted to process personal data when necessary to safeguard the prevention, investigation and detection of payment fraud. Furthermore, payment service providers may only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.

By signing the Account Opening Form, and thereafter when you continue to use our payment services, you (the Customer) give your consent as a payment service user to the processing of personal data necessary for the provision of payment services under the Agreement, and consent to and accept the contractual provisions in relation thereto as set out in the Account Opening Form, the General Terms and Conditions for Banking Services, the Additional Terms and Conditions for Online Services and other relevant parts of the Agreement. Your consent may be withdrawn by giving us notice in writing by mail or e-mail, and such notice will be treated as a termination notice.

If you (the Customer) do not give your consent or you withdraw consent, we will not be or no longer be able to accept instructions, orders, execute transactions or receive funds for your Account and generally, we will not be able to provide any payment services in relation to any Account, or any other services and products. Therefore, if you do not give your consent or you withdraw consent, your Account will not be opened or will be closed and the relationship terminated.

Information accompanying transfers of funds

As a payment service provider, we are required to process personal data on the basis of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds (the "**Transfer of Funds Regulation**"), for the purpose of the prevention of money laundering and terrorist financing. The Transfer of Funds Regulation applies, in principle, to transfers of funds, in any currency, which are sent or received by a payment service provider or an intermediary payment service provider established in the EEA. This means that it concerns all funds remitted to and transferred from an Account that you hold with us.

The Transfer of Funds Regulation imposes legal obligations on payment service providers that generally require the following:

- As a rule, the payment service provider of the payer (e.g. the Bank, if you transfer funds from your Account) must ensure that transfers of funds are accompanied by the following information: (a) the name of the payer; (b) the payer's payment account number; (c) the payer's address, official personal document number, customer identification number or date and place of birth; (d) the name of the payee; and (e) the payee's payment account number. Before transferring funds, the payment service provider of the payer is also required to verify the accuracy of the information on the payer (referred to in (a), (b) and (c)), on the basis of documents, data or information obtained from a reliable and independent source.
- The payment service provider of the payee (e.g. the Bank, if you receive funds in your Account) is required to check whether the necessary information regarding the payer and payee is missing. The payment service provider of the payee also has to verify the accuracy of the information on the payee on the basis of documents, data or information obtained from a reliable and independent source, before crediting the payee's payment account or making the funds available to the payee.
- Where the payment service provider of the payee becomes aware, when receiving transfers of funds, that the necessary information is missing or incomplete, it has to reject the transfer or ask for the required information on the payer and the payee before or after crediting the payee's payment account or making the funds available to the payee, on a risk-sensitive basis.
- Intermediary payment service providers are required to ensure that all the information received on the payer and the payee that accompanies a transfer of funds is retained with the transfer. They also needs to check whether the necessary information on the payer or the payee is missing. Where the intermediary payment service provider becomes aware, when receiving transfers of funds, that the necessary information is missing, it will reject the transfer or ask for the required information on the payer and the payee before or after the transmission of the transfer of funds, on a risk-sensitive basis.

SWIFT

Personal data in relation to transactions effected via SWIFT (Society for Worldwide Interbank Financial Telecommunication) may be required to be disclosed to the United States authorities in order to comply with legal requirements applicable in the United States for the prevention of crime and in accordance with the EU-US Terrorist Finance Tracking Program (TFTP) agreement.

3. Sharing of personal data

The Bank will keep information related to Customers confidential, but may share personal data with third parties in certain circumstances, in particular the following:

Type of recipient	**Examples**
Suppliers, delegates, agents, and other service providers of the Bank (and their sub-contractors)	Consultants, external auditors, professional advisors and providers of services outsourced by the Bank, mainly in relation to IT (e.g. hardware and software providers and maintenance); internal audit; transaction reporting services carried out on behalf of the Bank in compliance with regulatory requirements; administrative service providers used for reconciliation tasks.
Advisors, investment managers, delegates and other service providers of the Customer	Power of Attorney holders, representatives, agents, professional advisors and wealth managers acting on behalf of a Customer.
Payment service providers and other entities involved in processing of payments or payment transactions	Other banks remitting or receiving payments, correspondent banks, members of payment schemes and messaging systems such as SWIFT.
Financial institutions involved in the provision of the services or products	Brokers and other financial intermediaries, transfer agents, central securities depositories (CSDs, including Clearstream and Euroclear), sub-custodians, settlement agents, proxy service providers and other providers of services in relation to tax reclaims, withholding tax or corporate actions.
Issuers and their representatives	Issuers of shares traded on a regulated exchange, who may be entitled to information about their shareholders.
Other financial institutions or third parties the Bank is requested to deal with	Institutions from or to which the Customer's portfolio is transferred, pledgees, security trustees or agents, professional advisors representing the Customer.
Regulatory and supervisory authorities and other government agencies or bodies	Local competent authorities such as the Malta Financial Services Authority (MFSA), the Financial Intelligence Analysis Unit (FIAU), the Office of the Information and Data Protection Commissioner (IDPC) and foreign competent authorities regulating or supervising regulated activities, prevention of money laundering and funding of terrorism or data protection.
Local and foreign tax authorities	Inland Revenue Department ("IRD") and foreign tax authorities.
Courts, administrative bodies and law enforcement bodies	Provision of information upon a request, e.g. in the course of an investigation or ongoing legal proceedings pursuant to court orders or requests for information by the MFSA, FIAU or police
Recipients of bank references issued by the Bank	Competent authorities, banks and other service providers to whom a bank reference issued by the Bank is addressed

Card issuers or distributors	Issuers or distributors of pre-paid and credit cards provided to Customers through the Bank.
Restructuring, sale or acquisition or transfer of business	Potential buyers of all or part of the Bank's business or their representative carrying out due diligence on the Bank (e.g. in the unlikely event that the Bank's recovery plan may be triggered).
WorldCheck and other due diligence service providers	Provision of information to the service provider in order to carry out WorldChecks and other due diligence checks on the background of prospective and existing Customers and corresponding parties.
Central credit register and credit reference agencies / fraud prevention agencies	Central credit register maintained by the Central Bank of Malta.

Given the international nature of the Bank's business and operations, the recipients of data referred to above may be located outside Malta or the jurisdiction where the Customer is located or where the Bank operates from.

4. International transfer of personal data

In certain cases, personal data may be transferred to a third country (that is, a country which is not an EEA State) or an international organisation. This may be the case, for example:

(i) where the Bank is requested by remitting, receiving or correspondent banks or intermediaries to provide information regarding incoming or outgoing payments, if certain information is missing or additional information is required for the prevention and detection of fraud, money laundering, terrorism financing and other crimes, monitoring of sanctions and embargos, or to meet other legal or regulatory requirements;

(ii) where the Bank is requested by issuers of securities or their agents, central securities depositaries (CSDs) or financial intermediaries to provide information on the Customer for whom the Bank holds financial instruments as nominee or custodian, for tax reasons, disclosure of information on shareholdings or compliance with (other) legal or regulatory requirements.

Personal data may also be transferred to third countries by third parties and authorities, for example, where the Bank provides information related to FATCA or CRS[1] to local tax authorities, which the local authorities may then pass on to their counterparts abroad.

The Bank may transfer data to a third country or international organisation, where the European Commission has decided that the third country or the international organisation in question ensures an adequate level of protection[2], or in the absence of such decision, adequate safeguards are provided for (for example, by means of standard data protection clauses adopted or approved by the European Commission). In the absence of an adequacy decision by the European Commission or appropriate safeguards, the transfer may only take place in specific situations, for example, where the data subject explicitly consents to the proposed transfer or the transfer is necessary for the performance of a contract

[1] Information on CRS and FATCA is available from our website: https://www.sparkasse-bank-malta.com/en/library
[2] An overview of the European Commission's adequacy decisions is available from: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

between the data subject and the Bank. Information on the safeguards in place (if required), will be available upon request (see our contact details in section 9 below).

5. Data storage

The period for which the Bank stores personal data will depend on the type of information held, the purpose and legal basis for processing and the legal or regulatory requirements that may apply to the retention of information and record keeping.

The Bank determines the time for which data are stored (retention periods) primarily on the basis of the legal and regulatory obligations to which it is subject, and will in principle follow industry standards published by the Malta Bankers' Association.[3] As a rule, the Bank will store data in a form which permits identification in accordance with local industry standards, as follows:

(i) electronic data in the Bank's systems related to cash accounts: ten (10) years from the transaction for transaction data (debit and credit transactions passing through the account over the years), and ten (10) years from the closure of an account for account data (data on all aspects of the account, other than transaction data; e.g. withholding tax instructions, opening of account details, contact detail and residence status);

(ii) paper records and scanned documents related to cash accounts: six (6) years from the transaction for transaction information (e.g. cheques), and six (6) years from the closure of the account for account information (e.g. account opening and other application forms);

(iii) in the case of investment services related to portfolio accounts: six (6) years from the end of the investment relationship for customer profile forms, suitability and appropriateness assessments and reviews, etc., and six (6) years from the transaction, for documents related to transactions in financial instruments; and

(iv) telephone recordings: ten (10) years from the date of recording if they are the only proof of a debit authority or of a contract, or in the case of investment services, if they relate to transactions in financial instruments, or up to thirty (30) days in other cases.

Data may be held for a longer period if the Bank is requested to do so by a competent authority, court or law enforcement agency or to pursue or defend legal claims.

6. Automated decision-making

The Bank has certain systems in place that may result in decisions being taken based on automated processing, including profiling, that could significantly affect the data subject concerned.

Automated decisions and profiling may occur when the Bank carries out checks for the prevention and detection of fraud, money laundering, terrorism financing and the application of sanctions and embargos and as part of security measures such as transaction monitoring purposes. The Bank uses specialised software to block or flag transactions prohibited because of international sanctions or embargoes and also to monitor transactions for particular attributes or patterns against the Customer's profile, in order to block or flag potentially suspicious transactions.

[3] In particular, Annex I to the Data Protection Guidelines for Banks, issued by the Malta Bankers' Association in consultation with the Office of the Information and Data Protection Commissioner: https://idpc.org.mt/en/Press/Pages/Banking-Sector-Data-Protection-Guidelines-.aspx

If automated decision-making is necessary for the performance of a contract or based on consent, the data subject has the right to obtain human intervention, to express his or her point of view and to contest the decision.

7. Data subjects' rights

An individual has certain rights regarding his or her personal data, subject to applicable law. Data subjects' rights under the GDPR include:

(i) the right to request access to data;

(ii) the right to request rectification;

(iii) the right to request erasure ("right to be forgotten");

(iv) the right to request restriction of processing;

(v) the right to data portability;

(vi) the right to object to processing;

(vii) the right to withdraw consent; and

(viii) the right to lodge a complaint with a supervisory authority.

Information on these rights is given below.

Any request regarding the exercise of data subjects' rights must be made by the data subject or a person duly authorised by him or her, in writing, by mail or e-mail, using the contact details set out in section 9 below. The Bank facilitates the exercise of data subjects' rights by making available a request form on its Website or upon request.

Right of access by the data subject

Individuals have the right to request the Bank to confirm whether or not personal data concerning him or her are being processed. If it is confirmed that the Bank processes his or her personal data, the data subject has the right to request access to the personal data and the following information:

(i) the purposes of processing;

(ii) the categories of personal data concerned;

(iii) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(iv) where possible, the envisaged period for which the personal data will be stored, or if not possible, the criteria used to determine that period;

(v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(vi) the right to lodge a complaint with a supervisory authority;

(vii) where the personal data are not collected from the data subject, any available information as to their source;

(viii) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where personal data are transferred to a third country or to an international organisation, the data subject also has the right to be informed of the appropriate safeguards relating to the transfer.

Right to rectification

Data subjects have the right to request the Bank to rectify inaccurate personal data concerning him or her without undue delay. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure ("right to be forgotten")

Data subjects have the right to request the Bank to erase personal data concerning him or her without undue delay. However, the Bank is only required to erase personal data upon request, on one of the following grounds:

(i) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(ii) the data subject withdraws consent on which the processing is based (see below), and where there is no other legal ground for the processing;

(iii) the data subject objects to the processing (see below) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes;

(iv) the personal data have been unlawfully processed;

(v) the personal data have to be erased for compliance with a legal obligation in EU or national law to which the Bank is subject;

(vi) the personal data have been collected in relation to the offer of information society services to a child.

The right to erasure does not apply, and the Bank is not required to erase personal data, to the extent that processing is necessary for exercising the right of freedom of expression and information, compliance with a legal obligation which requires processing by EU or national law to which the Bank is subject or the establishment, exercise or defence of legal claims.

Right to restriction of processing

Data subjects have the right to request the Bank to restrict processing where one of the following applies:

(i) the accuracy of the personal data is contested by the data subject, for a period enabling the Bank to verify the accuracy of the personal data;

(ii) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(iii) the Bank no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(iv) the data subject has objected to processing (see below) pending the verification whether the legitimate grounds of the Bank override those of the data subject.

Where processing has been restricted, the personal data will (with the exception of storage) be processed only: (a) with the data subject's consent, (b) for the establishment, exercise or defence of legal claims, (c)

for the protection of the rights of another natural or legal person, or (d) for reasons of important public interest of the EU or of a Member State.

Right to data portability

Data subjects have the right to receive the personal data concerning him or her, which he or she has provided to the Bank, in a structured, commonly used and machine-readable format and the right to transmit those data to another controller without hindrance from the Bank, if the following conditions are met:

(i) the processing is based on consent or on a contract; and

(ii) the processing is carried out by automated means.

In exercising his or her right to data portability, the data subject has the right to have the personal data transmitted directly from the Bank to another controller, where technically feasible.

Right to object

A data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on legitimate interests pursued by the Bank or a third party, including profiling based on such ground. The Bank is required to no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to processing of personal data concerning him or her for such marketing.

Right to withdraw consent

In cases where personal data are processed based on consent, the data subject has the right to withdraw his or her consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, every data subject has the right to lodge a complaint with a supervisory authority in terms of the GDPR, in particular in the EEA State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the GDPR.

The supervisory authority for the GDPR in Malta is the Office of the Information and Data Protection Commissioner; its contact details are available from, and complaints can be submitted via the IDPC website.

For a list and contact details of national supervisory authorities within the EEA (Data Protection Authorities or DPAs), please visit the European Commission's website.

8. 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 in section 9 below). If changes to this Notice have a significant impact on the nature of processing or data subjects concerned, we will give advance notice.

9. 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

Version: July 2019