

PRIVACY NOTICE – APPLICATIONS AND ENQUIRIES REGARDING EMPLOYMENT OR TRAINING

Version 1.1 - April 2021

Sparkasse Bank Malta public limited company (the “**Bank**”, “**we**” or “**us**”) has prepared this Notice in order to provide information about the processing of personal data related to individuals who apply for or enquire about training or employment with the Bank, in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679; “GDPR”) and the Maltese Data Protection Act (Chapter 586 of the Laws of Malta).

If the recruitment process is successful, you will be provided with the General Data Protection Notice to Employees, which contains information for employees of the Bank, including prospective employees and trainees, and which will supersede this Notice.

Other privacy notices apply to information related to visitors of our website, cookies, customers and persons related to them, and particular types of processing operations, for example, regarding the use of the Spar Key App and the Online Services. Such notices are available on our website.

When reference is made 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.

Types of personal data

Data subjects whose data the Bank may process include individuals enquiring about or applying for employment or training with the Bank, candidates invited for an interview and certain individuals related to them, such as family members and other persons whose details may be provided, if required.

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

The Bank will collect various types of personal data directly from the data subject, including the following:

Type of information	Examples
Identification data	Name and surname, date of birth, place of birth, nationality, country of citizenship, identity card and/or passport information, tax identification number, national insurance number, passport photo.
Contact information	Residential address, personal telephone and mobile number, personal e-mail address.
CV/Resume	Information contained in the CV/Resume provided to the Bank.
Professional life information	Information on the employment history, contact details of and reference letters from previous employers, education and training.

Information on conduct	Police conduct certificate.
Personal life information	Emergency contact details, next of kin, marital or parental status.

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

Source	Type of information
Recruitment agency	Identification and contact details, CV or resume and other information provided by a recruitment agency.
Former or current employers	Professional references, if any.
Publicly accessible sources, such as: <ul style="list-style-type: none"> - Google and other search engines, - Online and paper media, - World-Check, - Social media platforms such as LinkedIn, - Websites of authorities or government agencies. 	Newspaper articles, information on investigations, criminal or civil proceedings, convictions, penalties, regulatory sanctions.

If a candidate, applicant or other person provides the Bank with information regarding another individual, the candidate, applicant 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.

Mandatory information

If we are not provided with certain personal data which we indicate to be mandatory, then we may not be able to process your application or enquiry. For example, if we require information about experience and knowledge required for the role you have applied for and you fail to provide us with such information, we will not be able to take your application further.

Why the Bank processes personal data

The Bank processes your personal data for the following purposes:

- (i) Handling your enquiry or application;
- (ii) Entering into an agreement for employment or training (as mentioned above, prospective employees will be provided with further information in the General Data Protection Notice to Employees);
- (iii) To comply with legal or regulatory obligations, for example regulatory requirements regarding the assessment of suitability or competence and obligations related to prevention of money laundering or terrorism financing and under applicable employment law;
- (iv) 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, operations and financial interests, reputation and risk exposures of the Bank, ensuring and monitoring the safety and security of the Bank's premises.

Certain information will be processed only with your consent, for example, where you give us permission to contact your previous or current employer(s) for a reference.

Special categories of data and data relating to criminal convictions

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 information on criminal convictions and offences or related security measures.

Purpose	Legal basis
Initial due diligence checks: due diligence checks via WorldCheck, Google searches and other publicly accessible sources and the collection of a police conduct certificate upon employment	Processing of personal data relating to criminal convictions and offences or related security measures authorised by law, in particular prevention of money laundering and terrorism financing legislation and directions, orders or other measures taken by a court or law enforcement body.

Sharing of personal data

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

Type of recipient	Examples
Recruitment agencies, consultants, auditors, lawyers and other professional advisors	Recruitment agencies that you have engaged and internal and external auditors, consultants, local and foreign legal counsel, IT consultants and other professional advisors appointed by the Bank.
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 a prospective employee
Previous and current employers	Employers contacted for professional references or information about a prospective employee
Institutions providing education or vocational training	Institutions that require information on training applied for with the Bank

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 where information in relation to a prospective employee is disclosed to professional advisors, previous or current employers or other third parties mentioned as recipients of data above, based outside the EEA.

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

Data storage

The Bank keeps your personal data on its servers and other equipment, and in physical files, located within the EU. These Bank's servers may be accessed through encrypted connections over the internet. In order to ensure the security of information we keep, we have adopted security measures and use providers which ensure an adequate level of security.

If the enquiry or application does not result in an offer by the Bank to enter into an agreement for employment or training with the Bank or such offer is not accepted, we will keep your data for a maximum period of one (1) year, during which we may contact you again should a future role arise that matches your profile. We also keep your data to show, in the event of a legal claim, that we have not discriminated against candidates and that we have conducted the recruitment exercise in a fair and transparent manner. After this period, we will securely destroy your personal information in accordance with applicable law and regulations.

If the enquiry or application results in an offer by the Bank to enter into an agreement for employment or training with the Bank and you accept the offer, we will keep your information as explained in the General Data Protection Notice to Employees, a copy of which will be provided to you.

Data Subjects Rights

As a data subject you have the following rights.

I. Right of **access**

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.

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.

II. Right to **rectification**

Data subjects have the right to request the Bank to rectify inaccurate personal data concerning him or her without undue delay. Considering 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.

III. 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;

(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.

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.

IV. 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.

V. Rights in relation to **automated decision-making**, including profiling.

The data subject has certain rights related to automated decision making, including profiling. The Bank does not conduct profiling or automated decision making in relation to the data subjects addressed in this Notice.

VI. 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.

VII. 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.

VIII. 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 and at no cost. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

IX. 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: idpc.org.mt.

For a list and contact details of national supervisory authorities within the EEA (Data Protection Authorities or DPAs), please visit https://edpb.europa.eu/about-edpb/board/members_en

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 made available below. The Bank facilitates the exercise of data subjects' rights by making available a request form on its Website or upon request. We will do our best to comply with your request within a month from confirmation of your identity; such period may be extended to two months, in the event of repetitive or excessive requests. We will notify you if such case occurs, explaining the reason for the delay. We may also charge you a reasonable fee in the case of repetitive requests.

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

If you have any questions about this Notice or if you wish to exercise your rights, you may submit a request by e-mail to: dataprotection@sparkasse-bank-malta.com or by mail to: Attn: Compliance Department; Sparkasse Bank Malta Plc.; 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 Plc.; 101 Townsquare, Ix-Xatt ta' Qui-si-Sana; Sliema SLM3112; Malta

Sparkasse Bank Malta public limited company is a public limited liability company registered under the laws of Malta, with registration number C27152 and with registered office and head office at 101 Townsquare, Ix-Xatt Ta' Qui-Si-Sana, Sliema SLM 3112, Malta.

Sparkasse Bank Malta public limited company is licensed by the Malta Financial Services Authority to carry out the business of banking as a credit institution in terms of the Banking Act (Chapter 371 of the Laws of Malta), and to provide certain investment services in terms of the Investment Services Act (Chapter 370 of the Laws of Malta). The MFSA maintains a register of licence holders on its website:

www.mfsa.com.mt.