Privacy Notice

Last Updated: May 2025

Introduction

This document represents our privacy notice, both to customers and users of our website (the "**Notice**").

The Access Bank Malta Limited (C107833) of Level 4, The Piazzetta Business Plaza, Triq Għar il-Lembi, Sliema, SLM 1605, Malta ("**we**", "**us**", "**our**" or the "**Bank**") respects your privacy and is wholly committed to protecting your personal data.

We are a credit institution licensed and regulated in Malta by the Malta Financial Services Authority ("**MFSA**"). We are providing this Notice as the controller of your personal data. We process all personal data in an appropriate and lawful manner, in accordance with the Data Protection Act, Chapter 586 of the laws of Malta, and the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), as may be updated or otherwise amended from time to time.

This Notice explains how we will process your personal data when you:

- approach us and enter into a banking relationship with us;
- request and/or receive our banking products and services (our "Services"); and
- visit and use our dedicated website www.theaccessbankmaltaltd.mt (the "**Website**" or the "**Site**"), regardless of where you visit and use it from.

This Notice covers any personal or commercial products or services you have with us such as savings, current, term deposits and other bank accounts, loans and overdrafts as well as any future updates to products and services offered by the Bank including any new product/ service.

It also covers any data that you may provide for and in relation to our newsletters, industry updates, events and other marketing and promotional communications.

Where you are a corporate customer (i.e. not a natural person), we will also request and collect personal data about your directors, representatives, officers, authorised signatories, shareholders and ultimate beneficial owners typically for anti-money laundering, due diligence and other vetting requirements (which we refer to in this Notice as an "**individual connected to a business**"). This Notice also explains how we process personal data about such individuals and should therefore be circulated accordingly.

You must ensure that they are made aware of this Notice and the individual rights and information it sets out prior to us receiving their information (whether obtained directly, obtained from you or from other sources). If you, or anyone else on your behalf, has provided, or provides, information on an individual connected to your business to us (or any entity associated with us), you or they must first ensure that you or they have that individual's authorisation to do so and will be required to confirm the same to us.

In this Notice, "you" is therefore generally also used to refer to individuals connected to your business.

It is important to note that your entry into a banking relationship with us gives rise to the existence of a contractual relationship, the General Terms.

Capitalised terms not defined herein shall have the same meaning as in the General Terms unless otherwise specified.

Please also use the **Glossary** to understand the meaning of some of the terms used in this Notice.

1. Important information and who we are

Purpose of this Notice

This Notice aims to ensure that you are fully informed on how the Bank will collect and process your personal data in the scenarios set out in the Introduction (and also applies to any data that you may provide for marketing and promotional communications). It informs you about the types of personal data which we will collect about you and describes how we will handle it (regardless of the way you interact with us, directly or indirectly, whether by email or otherwise). It also provides information on how to exercise your rights as a data subject.

Some of our banking products and services may be subject to supplemental privacy or processing notices, which may be found in specific agreements which you may enter with the Bank or which the Bank may notify you from time to time.

It is therefore important that you read this Notice carefully, together with any other privacy notice or fair processing notice that we may issue on specific occasions when we are collecting or processing personal data about you, so that you are fully aware of how and why we are using your data.

This Notice supplements our other notices and is not intended to override them.

Controller

The Bank, as previously defined, is the controller and responsible for your personal data.

We have appointed a data protection officer ("DPO") who is responsible for overseeing questions in relation to this Notice. If you have any questions about this Notice, including any requests to exercise your legal rights as a data subject, please contact the DPO using the details set out below.

You can address any comments, queries or complaints to the DPO, using the details indicated below, with the words 'Data Protection Matter' in the subject line.

Contact Details

Our full details are:

Full name of legal entity:	The Access Bank Malta Limited
Name or title of DPO:	Ms Graziella Gatt
Email address:	dpo@theaccessbankmaltaltd.mt
Postal address:	Level 4, The Piazzetta Business Plaza, Triq Għar il-Lembi, Sliema, SLM 1605, Malta
Telephone number:	+356 23167900

Your duty to inform us of changes

It is imperative that the personal data we hold about you is accurate and current at all times. Otherwise, this will impair our ability to provide you with our Services or the quality of your banking relationship with us (amongst other potential and salient issues).

Please keep us informed if your personal data changes during your relationship with us.

Third-party links

The Website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy notice or policies.

We strongly encourage you to read the privacy notice of every website you visit, particularly when leaving our Website.

2. The data we collect about you

Personal data, or personal information, means any information relating to an identifiable individual. It does not include data where the identity has been removed (**anonymous data**).

In the course of any banking relationship, the Bank will need to collect, use, and sometimes, disclose different types of personal data for various purposes associated with the scope of the banking products and services (the "Services") that we provide, as requested and directed by you or your organisation, either for yourself (the customer) or your organisation (where you are an individual connected to a business). Given the broad spectrum of our potential Services, we cannot realistically provide an exhaustive list of all the types of personal data which we may need to process about our customers and/or the individuals connected to their business.

However, to ensure transparency, we have made an attempt to group and categorise below the different kinds of personal data about our customers or mere users of the Site. For the reasons explained above, these data categories are strictly indicative and not exhaustive.

Currently, the Bank deals with companies and other legal persons (that is, "corporate customers" and not natural persons per se). Nonetheless, please note that we have legal and regulatory obligations to collect, process, store and at times even to disclose personal information about the individuals who own, control or are otherwise responsible for or involved in the management and administration of its corporate customers (that is, "individuals connected to a business"). Furthermore, we also require personal information about such individuals in order to enable us to provide and perform the requested Services.

These data categories are set out below:

- **Identity Data** includes first name, middle name, maiden name, last name, title, identity document number, gender, nationality, citizenship, marital status, employment status, organisation, occupation and (in the context of the Site) username or similar identifier.

- **Contact Data** includes mailing address, email address, mobile number and telephone number.

  In the context of our legal entity customers, we may collect **Identity and Contact Data** about the following individuals:

  - directors;
  - legal and judicial representatives;
  - company secretary and other officers (for example, MLROs, DPOs and risk officers);
  - shareholders and ultimate beneficial owners (**UBOs**); and/or
  - authorised signatories.
  - founders and board of administrators in the case of Foundation;
  - settlors, beneficiaries, protectors and trustees in the case of a Trust.

- **Banking Data** includes bank account and internet banking details with the Bank.

- **Banking Mandate Data** includes details about the customer's principal bankers and bank account number(s) with those particular banks.

- **Transaction Data** includes the following information about our customers: (i) bank statements, (ii) a history of transactions with the Bank and (iii) the relative details of each individual transaction.

- **Compliance Data** may include the following due diligence information and documentation relating to our customers and/or the individuals connected to their business: (i) copy of identity document, (ii) copy of a recently issued utility bill or other documentation to verify the residential address, (iii) professional references, (iii) tax domicile status and tax identification, (iv) source of wealth and funds, (v) 'KYC' (database) and criminal records checks, (vi) data about your education, profession or work and (vii) any other documentation which may be mandated from time to time by applicable anti-money laundering or sanctions laws or the Financial Intelligence Analysis Unit ("**FIAU**") and/or any other competent authority or related legislation.

- **Additional Compliance Data** includes, for particular cases, copies of bank statements held by the customer with other credit institutions and, in the case of respective individuals connected to the business (such as UBOs, shareholders), copies of payslips or salary slips.

- **Financial Data** includes financial history, your credit rating or history and information such as account, profile and balance provided for banking purposes.

- **Specific Documents** may include asset contracts, public deeds, public wills, testamentary instruments and/or inheritance agreements (as relevant to the particular circumstances), which in and of themselves may contain and disclose particular personal information about you.

- **Court Data** includes information relating to freezing orders, garnishee orders, monitoring orders, precautionary warrants, executive warrants, witness summons, interdiction or incapacitation orders and any other order that may be issued by a Court of law or any other competent authority, and/or requests for information from regulatory or law enforcement authorities such as the MFSA, the FIAU or the Police, and which are served on the Bank in relation to the customer and/or the account/s held by the customer with the Bank.

- **Telephone recordings:** We may record any transactions or instructions received over the telephone, in particular instructions received from customers.

- **Usage Data** includes information about how our banking products and services are used (including frequency).

- **Technical Data** includes internet protocol (IP) address, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access the website, your internet banking page and our mobile application, and information about other online identifiers (including cookie and information data generated via your browser) including user login and registration data e.g. login credentials for internet and mobile banking applications (where applicable)

- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences. This may include information whether you have subscribed or unsubscribed from any of our mailing lists, attended any of our events or accepted any of our invitations.

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregate may be derived from your personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to ascertain the existence of any trends with regards to our banking or payment services. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

If we decline to enter into a relationship with an applicant due to the existence of a criminal record or other litigation, or due to an unsatisfactory due diligence process, we will keep an annotation of this decision in eventuality that the same applicant seeks to re-apply.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of the contract we have with you (pursuant to your entry into a banking relationship with us), **and you fail to provide that data when requested**, we may not be able to perform the contract that we have or which we are trying to enter into with you (namely, providing the banking products and/or services which you may request and which we offer as a credit institution duly authorised and regulated by the Malta Financial Services Authority). In certain cases, particularly where it relates to Compliance Data, we may even need to exercise our prerogative to terminate the contract in accordance with the General Terms or otherwise decline to enter into a banking relationship with you, but we will notify you if this is the case at the time.

Special categories of personal data

We may also need to occasionally process certain special categories of personal data about you as part of our statutory due diligence and sanction screening requirements. This may comprise personal data revealing your political opinions or affiliations, and also personal data relating to criminal convictions and offences or related security measures (e.g. Court Data).

Below are the circumstances and purposes for which this may take place:

- Initial and on-going customer due diligence checks, which would include determination of whether or not the customer and certain persons related to the customer are "politically exposed persons" in terms of applicable AML legislation; and
- Initial and on-going customer due diligence and screening checks: due diligence checks via WorldCheck, Google Searches, databases of regulatory or supervisory authorities, and other publicly accessible sources;
- fulfil any mandated external regulated reporting, such as to the FIAU; and
- abide by Court orders.

As a lawful basis, the processing of this data is necessary for reasons of substantial public interest on the basis of an EU or national law (namely, AML related) or otherwise relates to data which has been manifestly made public by the data subject or is necessary to comply with Court orders/decisions.

There may be other occasions where we may need to process special categories of personal data about you, namely where:

- the processing is necessary for the detection or prevention of crime (including the prevention of fraud) to the extent permitted by applicable law or regulation; or
- the processing is necessary for the establishment, exercise or defence of legal rights.

In other cases, for example where required as part of the Service provision, we will rely on your authorisation to process the special category of personal data.

The officers and employees that form part of the Bank are bound by duties of confidentiality and may also be subject to professional secrecy obligations.

3. How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Account Opening.** You will need to give us the Identity, Contact and Compliance Data of your UBOs, shareholders, directors, representatives and/or authorised signatories (i.e. relevant individuals connect to your business) when opening a bank account with us, regardless of the type, nature or purposes of the account. This information will be required from you for each account opening. You provide this information to us, and we collect and process the same, when you fill in and submit our account opening form and other related forms. Any Banking Data (e.g. bank account details) issued to you on the basis of your account opening is also retained and stored by us.

- **Service Use**. Through your use of our banking products and services, we generate and compile your Banking, Financial and Transaction Data, including in the form of records. These sets of data are either issued or made available to you upon request, and are retained by us for the purposes set out below. Moreover, to act upon certain service requests (e.g. deposits of a certain size), you will need to provide us with the Additional Compliance Data that we require.

- **Direct Interactions**: You may give us your Identity, Contact, Compliance, Banking, Financial and Transaction Data by filling in our other forms (i.e. separate to our account opening form) or by corresponding with us by post, phone, e-mail or otherwise. This includes personal data you provide when you, as may be applicable:

- enter into a banking relationship with us;
- subscribe to our internet banking services;
- request further assistance with us;
- contact us with complaints or queries;
- report issues;
- submit the Compliance Data or Additional Compliance Data that we request;
- request marketing to be sent to you;
- express an interest in and/or attend any of our events;
- participate in a survey;
- subscribe to our newsletters and updates; or
- provide us with feedback.

- **Service of Court orders and similar orders, or requests for information from public authorities and regulators**. The Bank could be served with Court orders or judicial acts that may be issued or filed against you the accounts which you hold with us or individuals connected to your business (i.e. **Court Data**). The Bank may also be served with requests for information or orders from regulatory or law enforcement authorities. In such a case, copies of the relative Court order or judicial act will be processed and retained by us.

- **Automated technologies or interactions.** As you interact with our website, internet banking portal and mobile application, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies.

- **Third parties or publicly available sources.** We may receive personal data about you (namely, Identity, Contact, Court, Compliance and Additional Due Diligence) from various third parties, such as your professional referees, and from publicly available source such as public court documents, the Malta Registry of Companies, the Registry of Companies of other jurisdictions, and from electronic data searches, online search tools (which may be subscription or license based), anti-fraud databases and other third party databases, sanctions lists and general searches carried out via online search engines (e.g. Google).

If you attend an event or meeting at our offices, we may hold images of you captured by our CCTV cameras.

4. How we use your personal data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where you wish to enter into a banking relationship with us;
- Where we are providing you with the banking products or services that you have requested;
- Where it is necessary to give effect to the contract entered into by your acceptance of our Terms and Conditions (this is referred to below as **performance of a contract**).
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

We do not generally rely on consent as a basis for processing your personal data, other than in relation to sending third party direct marketing communications. You have the right to withdraw consent to such marketing at any time by contacting us, as indicated below.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data pursuant to more than one lawful ground or basis, depending on the specific purpose for which we are using your data.

Accordingly, please contact us at dpo@theaccessbankmaltaltd.mt if you need details about the specific legal basis we are relying on to process your personal data where more than one basis has been set out in the table below.

Purpose/Activity	**Type of data**	**Lawful basis for processing**
Onboarding Requirements (a) 'New customer onboarding' ▪ to decide on your banking application, for onboarding requirements and to comply with our internal policies and procedures; and ▪ to assess and take an informed decision on whether we will enter into a banking relationship with you. (b) To determine whether we can provide you with the requested Services and, as applicable, perform them on an ongoing basis; (c) To enter into a formal banking relationship with you and your organisation.	(a) Identity; (b) Contact; (c) Banking Mandate; (d) Transaction; (e) Compliance; (f) Additional Compliance; (g) Financial; (h) Specific Documents; (i) Court.	(a) Performance of a contract with you. (b) Necessary to comply with a legal obligation. (c) Necessary for our legitimate interests (to determine whether we can or want to enter into a service relationship with you, to determine whether we can provide the Services that you have requested, to carry out internal conflict clearance searches and verify your ability to meet financial commitments that may result from the Service provision).
AML, Anti-bribery and "KYC" processes (a) To fulfil our regulatory and legal obligations relating to the prevention of money laundering, anti-bribery, fraud prevention, counter-terrorist financing, politically-exposed-persons checks, sanctions checks and any other "know your customer" ("KYC") checks. This includes: verifying your identity; and screening against lists maintained by a third party which assists with this process (such as sanctions lists). (b) To fulfil our other due diligence and KYC internal compliance policies and requirements; (c) To fulfil any external mandatory reporting obligations that we may, from time to time, have to the local and overseas public and regulatory authorities and/or law enforcement	(a) Identity; (b) Contact; (b) Banking Mandate; (c) Transaction; (d) Compliance; (e) Additional Compliance; (f) Financial (g) Specific Documents; (h) Court. *provided that we are exempted from professional	(a) Necessary to comply with a legal obligation. (b) Necessary for our legitimate interests (to establish and verify the identity of our corporate customers and individuals connected to their business, even where the requested assistance does not amount to a 'relevant activity', for internal risk assessment and internal management). It also helps us to determine the extent of the Bank's compliance with law, regulations and internal policies and procedures, and to protect the Bank's reputation.

agencies (including the MFSA or the FIAU) or tax authorities (including in terms of FATCA).	secrecy obligations in case of disclosure and reporting.	
Service Provision (a) To provide you or your organisation with our banking products and services (as instructed by you), which may include: ▪ account openings; ▪ deposits; ▪ payment and transfer instructions; ▪ fund withdrawals and releases; ▪ production of bank statements; ▪ our other services. (b) To improve the provision of those Services to you or your organisation.	(a) Identity; (b) Contact; (c) Compliance; (d) Banking; (e) Transaction; (f) Financial; (g) Telephone Recording; (h) Specific Documents.	(a) Performance of a contract with you. (b) Necessary to comply with professional obligations and ethical duties. (c) Legitimate business interests (quality control, business reputation, to keep track of the Services provided and their status or outcome, to be able to revisit them should issues arise).
(a) For billing and invoice purposes; (b) To collect and recover money which is owed to us (debt recovery); (c) Internal record keeping (including files).	(a) Identity; (b) Contact; (c) Compliance; (d) Banking; (e) Transaction; (f) Financial; (g) Telephone Recording.	(a) Performance of a contract with you. (b) Necessary to comply with a legal obligation (accounting and other record-keeping requirements). (c) Necessary for our legitimate interests (to recover debts due to us, to keep track of the Services provided to the customer and their status or outcome, to be able to revisit such matters if new issues arise).
Relationship management. To manage our professional relationship with you (as a customer or where the customer is your organisation), which may include the following: (a) notify you about changes to our terms of business or privacy notices; (b) deal with your enquiries, requests, complaints or reported issues; (c) contact you in the course of providing the requested Services; (d) ask you to participate in a survey;	(a) Identity; (b) Contact; (c) Banking; (d) Financial (e) Usage; (f) Profile; (g) Marketing and Communications; and (h) Telephone Recording.	(a) Performance of a contract with you. (b) Necessary for our legitimate interests (for customer relationship handling and management, to study business growth and possible trends regarding our service areas, to enable a review and assessment of our service provision, to develop and grow our business).

(e) request feedback from you; (f) advise you of industry and legislative updates; (g) inform you about our events and seminars (including webinars); (h) provide you with information about our Services, and (i) provide you with any other information or materials that you have requested to receive from us.		
Business and financial management (a) To run our business in an efficient and proper manner, (b) To enable third parties to provide us with services necessary for the provision of our Services; (c) To respond to customer due diligence requests; and (d) To investigate and respond to customer complaints.	(a) Identity; (b) Contact; (c) Banking; (d) Financial; (e) Compliance; (f) Usage; (g) Profile; (h) Marketing and Communications; and (i) Telephone Recording.	(a) Performance of a contract with you. (b) Necessary for our legitimate interests (**for administering, managing and operating the affairs of our business properly**, including managing our financial position, business capability, planning, communications, corporate governance, audit, insurance, sales, to prevent fraud and to maintain the confidentiality of communications, and in the context of a business reorganisation or group restructuring exercise). (c) Necessary to comply with a legal obligation
(a) To detect, investigate and prevent and/or report - breaches of internal and regulatory policies; and/or - fraudulent activity and/or any other criminal activity. (b) To assist and cooperate in any criminal or regulatory investigations against you, as may be required of us. (c) **Risk Management**: to effectively operate our audit, compliance controls and other risk management functions.	(a) Identity; (b) Contact; (c) Banking Mandate; (d) Transaction; (e) Compliance; (f) Additional Compliance; (g) Financial (h) Specific Documents;	(a) Necessary to comply with a legal obligation. (b) Necessary for our legitimate interests (regulator relations, business reputation).

	(i) Court. *provided that we are exempted from professional secrecy obligations in case of disclosure and reporting.	
(a) To administer and protect our firm, business and the Website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data). (b) To manage the performance and security of our equipment, IT systems and electronic platforms, including administering access rights; (c) To operate IT security audits.	(a) Identity; (b) Contact; (c) Technical; and (d) Usage.	(a) Necessary for our legitimate interests (for running and administering our firm and business (including IT support), systems administration, network security, to prevent fraud and to maintain the confidentiality of communications, and in the context of a business reorganisation or group restructuring exercise). (b) Necessary to comply with a legal obligation.
Marketing and Business Growth (a) To carry out market research campaigns; (b) To market our Services to you by email or other means if you have subscribed to one of our mailing lists (**where you are not a customer**); (c) To deliver relevant Website content and advertisements to you, and measure or understand the effectiveness of the advertising we serve to you.	(a) Identity; (b) Contact; (c) Technical; (d) Usage; (e) Profile; and (f) Marketing and Communications.	(a) Necessary for our legitimate interests (to develop our lines of Services and grow our business, to define our customers and their industries or sectors, to keep our Services and the Site updated and relevant, and to inform our marketing strategy). (b) On the basis of your consent, in the absence of a customer relationship.
To permit us to pursue available remedies or limit any damages that we may sustain.	All data categories.	(a) Performance of a contract with you. (b) Necessary for our legitimate interests.

As part of our legitimate (business) interests, we may need to share, disclose or transfer your personal data to any potential acquirer of the Bank or the Bank's business or part thereof, or to an actual or potential assignee or transferee of the Bank's rights against you.

Telephone Recordings

We monitor our calls for security as well as the following purposes:

- for instructions that you provide to effect transfers on your behalf;
- to follow up on your complaints and for occasional call grading and training;
- in case of any cash discrepancies found when conducting reconciliations;
- for potential fraud;
- for calls relating to your account and instructions; and
- for calls pertaining to complaints/feedback and service quality purposes.

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around advertising and marketing. Through your Identity, Contact, Banking, Technical and Usage Data, we can form a view on what we think you or your organisation may want or need. This how we decide which of our products or services may be of most relevance or interest for you and/or your organisation (we call this **marketing**).

You may receive marketing communications from us (which may consist of mailshots, publications and/or information about our products and/or events), where:

- you have entered into a banking relationship with us (be it as a customer or as an individual connected to a business), regardless of whether there is a formal agreement; and
- provided you have not opted out of receiving marketing from us (see **Your right to object** below).

Where the above does not apply to you, we will only send you our marketing communications where you have expressly consented to receive them from us.

Third-Party Marketing

We will get your express opt-in consent before we share your personal data with any third parties for marketing purposes.

Opting out

You can ask us to stop sending you advertising and marketing communications at any time by:
- following the opt-out links on any marketing message sent to you;
- contacting us at any time at dpo@theaccessbankmaltaltd.mt

Where you opt out of receiving such communications, this will not apply to personal data processed or provided to us as a result of your entry into a banking relationship with us and our service provision.

Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of the Website may become inaccessible or not function properly. This Notice should be read in conjunction with our **Cookie Policy** found on our website www.theaccessbankmaltaltd.mt

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us at dpo@theaccessbankmaltaltd.mt.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without the need to obtain your consent, in compliance with the above rules, where this is required or permitted by law.

5. Disclosures of your personal data

We may transfer your personal data to The Access Bank (UK) Limited or any affiliated or associated entities, for the following purposes:

- to facilitate and administer your business relationship with us or the service provision;

- as part of our regular reporting activities on company performances;
- to consolidate our reporting and accounting procedures;
- to ensure business efficiency (all above being part of our legitimate interests), and/or
- where necessary to achieve or further any of the purposes in section 4 above.

We may have to share, disclose or allow access to your personal data with the parties or authorities identified below for the purposes set out in the table in section 4 above.

- External Third Parties as set out in the Glossary.
- Regulators and other Authorities as set out in the Glossary.
- Correspondent Banks.
- To any relevant party in connection with our anti-money laundering, anti-bribery, anti-fraud or 'KYC' requirements or policies (including third party service providers which carry out sanctions checks on our behalf)
- Our professional advisers (including our auditors, accountants, financial advisers, and legal counsel);
- To regulators, government bodies and tax authorities (local and overseas) when required by applicable laws and/or regulations);
- To any relevant party, claimant, law enforcement agency or court, to the extent necessary for the establishment, exercise or defence of legal claims in accordance with applicable law and regulation;
- To any relevant party for the purposes of prevention, investigation, detection or prosecution of criminal offences in accordance with applicable law;
- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets, including to any potential acquirer of the Bank or the Bank's business or part thereof. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.
- Any actual or potential assignee or transferee of the Bank's rights against you (the Customer).

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

We may also disclose your data if we are under a duty to disclose or share your personal data to comply with any legal obligation, judgment or under an order from a court, tribunal or authority. This includes exchanging information with the Police or regulatory bodies in Malta or if applicable, overseas, and other organisations and may undertake credit or fraud searches with relevant agencies for the purposes of fraud detection and prevention.

We may also transfer your personal data to applicable governmental and regulatory authorities, agencies and other public bodies in order to comply with our legal obligations. In particular, we may transfer your personal data to the Malta Financial Services Authority, the Malta Business Registry, the Financial Intelligence Analysis Unit as well as applicable tax authorities. We may also transfer your personal data when we are required to do so by any judicial body, court order or order issued by a police authority.

We may also disclose your data to enforce our contractual terms with you or your entity, or to protect our rights, property or safety, that of our partners or other applicants or investors. This includes exchanging information with other companies and organisations for the purposes of fraud protection.

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 (or any other authorities) in order to comply with legal requirements applicable in the United States (or in any other country) for the prevention of crime and in accordance with the EU-US Terrorist Finance Tracking Program (TFTP) agreement.

6. International transfers

The Bank forms part of a group. We may from time-to-time need to share your personal data with our parent company, The Access Bank (UK) Limited based in the United Kingdom, in order to: (i) provide you with your requested banking products or services, (ii) fulfil our contractual obligations to you or exercise our contractual obligations against you, (iii) comply with our legal or regulatory obligations,(iv) assert, file or exercise a legal claim.

or (iv) where necessary to achieve or further any of the purposes listed in Section 4 above. The European Commission has, by means of an adequacy decision, recognised the UK as providing an **adequate level of data protection** within its national law. Notwithstanding this, we still ensure that the extent of this access is minimised and appropriately limited to those officials within our parent company who require such access to your data.

In addition, to process your payments and bank transfers, we will need to share certain personal data with our correspondent banks. This may involve transferring your data outside of the EEA, specifically when the requested payment or transfer is to be made to a non-EEA account. On other occasions, we may be requested, whether by you directly or by another financial institution with your knowledge, to provide banking reference that pertains to you.

Where we do need to transfer your personal data to outside the EEA (whether for these stated purposes or any other purpose listed in Section 4 above), we will ensure a similar degree of protection is afforded to that personal data by ensuring at least one of the following safeguards applies or is otherwise implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries.
- In the absence of an adequacy decision, we will use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see European Commission: Model contracts for the transfer of personal data to third countries.
- Where we use providers based in the U.S., we may transfer data to them if they are part of the EU-US Data Privacy Framework which requires them to provide similar protection to personal data shared between the Europe and the US. For further details, see European Commission: EU-US Data Privacy Framework.

Failing the above, we will only transfer your data if it is necessary:

- for the performance of your banking relationship with us;
- for the performance of a contract concluded in your interests between us and another person;
- for important reasons of public interest;
- in order to comply with a legal or regulatory obligation to which we are subject; or
- for the filing, exercise or defence of legal claims.

If we have to transfer your data to outside the EEA and cannot rely on any of the mechanisms set out above, we shall request your explicit consent to do so.

Please contact us at dpo@theaccessbankmaltaltd.mt if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

7. Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

We have also put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so, and within the timeframe prescribed at law.

8. Data retention

How long will you use my personal data for?

Please note that we (the Bank) considers its relationship with customers to be an ongoing and continuous customer relationship, until such time that it is terminated in accordance with the General Terms.

To determine the appropriate retention period, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm to it from unauthorised use or disclosure, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

With respect to customers, we will only retain your personal data for as long as necessary to fulfil the purposes for which we collected it, i.e. the provision of the Services and the ongoing performance of our professional relationship with you

thereafter:

- for the purpose of satisfying any legal, accounting, tax or reporting obligations to which we may be subject (which include AML record keeping obligations on the individuals connected to your business); and/or

- to the extent that we may also need to retain your personal data to be able to assert, exercise or defend possible future legal claims against or otherwise involving you.

Note that we may need to retain your personal data, or some of it, for longer period(s), such as in relation to threatened or commenced claims, disputes or litigation, ongoing or pending investigations, requests made by competent authorities or to abide by court orders or as dictated by the nature of the services or the business relationship.

In some circumstances you can ask us to delete your data. See Request erasure below for further information.

In other circumstances, we may also anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

Kindly contact us at dpo@theaccessbankmaltaltd.mt for further details about the retention periods that we apply. In that respect, we observe and apply the 'Retention Periods' set out in the Banking Sector Guidelines (entitled 'Data Protection Guidelines for Banks'), which were developed by the Malta Bankers' Association after a consultation process with the IDPC who ascertained that these Guidelines comply with the GDPR.

Data Minimisation

Whenever and to the extent possible, we may anonymise the data which we hold about you when it is no longer necessary to identify you from the data which we hold about you. In some circumstances, we may even pseudonymise your personal data (so that it can no longer be associated with you, without the use of additional information) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

9. Your Legal Rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data.

- *Request access to your personal data*.
- *Request for information about your personal data*.
- *Request correction (rectification) of your personal data*.
- *Request erasure of your personal data*.
- *Object to processing of your personal data*.
- *Request restriction of processing your personal data*.
- *Request transfer of your personal data*.
- *Right to withdraw consent*.

If you wish to exercise any of the rights set out above, please contact us at dpo@theaccessbankmaltaltd.mt.

These rights are explained below.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within a period of one (1) month from the date of receiving your request. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Your legal rights

You have the right to:

(i) Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

You may send an email to dpo@theaccessbankmaltaltd.mt requesting information as the personal data which we process. You shall receive one copy free of charge via email of the personal data which is undergoing processing.

(ii) Right to information when collecting and processing personal data about you from publicly accessible or third-party sources. When this takes places, we will inform you, within a reasonable and practicable timeframe, about the third party or publicly accessible source from which we have collected your personal data.

(iii) Request correction or rectification of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected and/or updated, though we may need to verify the accuracy of the new data you provide to us.

(iv) Request erasure of your personal data. This enables you to ask us to delete or remove personal data where:

- there is no good reason for us continuing to process it;
- you have successfully exercised your right to object to processing (see below);
- we may have processed your information unlawfully; or
- we are required to erase your personal data to comply with local law.

Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request. In particular, notwithstanding a request for erasure, we may continue to retain your personal data where necessary to:

- comply with a legal obligation to which we are subject; or
- establish, exercise or defence of legal claims.

(v) Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes (as under **Marketing** in section 4).

In some cases, we may demonstrate that we have compelling legitimate grounds to process your information that override your rights and freedoms.

(vi) Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- if you want us to establish the data's accuracy;
- where we no longer have a lawful basis for processing your data, but you do not want us to erase it;
- where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
- you have objected to our use of your personal data but we need to verify whether we have overriding legitimate grounds to use it.

(vii) Request the transfer (data portability) of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

(viii) Withdraw your consent at any time where we are relying on consent to process your personal data (which will generally not be the case). This will not however affect the lawfulness of any processing which we carried out before you withdrew your consent. Any processing activities that are not based on your consent will remain unaffected.

Kindly note that none of these data subject rights are absolute, and must generally be weighed against our own legal obligations and legitimate interests. If a decision is taken to override your data subject request, you will be informed of this by our data protection team along with the reasons for our decision.

10. Complaints

You have the right to lodge a complaint at any time to a competent supervisory authority on data protection matters, such as in particular the supervisory authority in the place of your habitual residence or your place of work. In the case of Malta, this is the Office of the Information and Data Protection Commissioner (the "IDPC") https://idpc.org.mt/en/Pages/Home.aspx

We would, however, appreciate the opportunity to deal with your concerns before you approach the supervisory authority, so please contact us in the first instance.

11. Conclusion

We reserve the right to make changes to this Notice in the future, which will be duly notified to you.

Please note that if our business, or any part of it, is sold or transferred at any time, the information we hold may form part of the assets transferred, although it will still only be used in accordance with this Notice.

We reserve the right, at our discretion, to change, modify, add, or remove portions from this Notice at any time. Please read this Notice carefully and re-visit this page from time to time to review for changes.

If you have any questions regarding this Notice, or if you would like to send us your comments, please contact us using the Contact Details indicated in this Notice.

12. Glossary

Set out below are key definitions of certain terms which appear in this Notice:

- "**data subjects**" means living, natural persons about whom we process personal data;
- "**data controller**" or "**controller**" means any entity or individual who determines the purposes for which, and the manner in which, any personal data is processed;
- "**data processor**" or "**processor**" means any entity or individual that processes data on our behalf and on our instructions (we being the data controller);
- "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- **"legitimate interest"** means our interest to conduct and manage our business appropriately and responsibly, to protect the reputation of our business, and to provide the best possible services. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests;
- "**personal data**" means data relating to a living individual (i.e., natural person) who can be identified from the data we possess about him or her. This includes, but is not limited to, your name and surname, address, date of birth, nationality, civil status, identity card number or passport number, photographic image, bank account details, online identifiers and contact details. The term "personal information", where and when used in this Notice, shall have the same meaning as personal data;
- "**processing**" means any activity or set of operations that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties; and
- "**special categories of personal data**" includes information about a person's racial or ethnic origin, political opinions, religious, philosophical or similar beliefs, trade union membership, physical or mental health or condition or sexual life or his or her biometric data.

External Third Parties

- Service providers who provide IT and system administration, maintenance and support services and other service providers (or sub-contractors) which may be engaged by the Bank to provide certain services to the customer on behalf of the Bank or to provide services which are necessary for the Bank's operations.
- Professional advisors including external legal counsel, internal and external auditors and consultants, brokers and insurers who provide legal, insurance (including professional indemnity), auditing and accounting services as may be engaged by the Bank from time to time.
- Credit reference agencies and debt recovery agencies who assist us with establishing the creditworthiness and credit risk of prospective customers and with the recovery of debts owed to us.

Regulator and other Authorities

- The Financial Intelligence Analysis Unit, Malta Financial Services Authority, Commissioner for Revenue, the Central Bank of Malta, the Police Authorities, The Sanctions Monitoring Board and other authorities (including overseas authorities) each of whom may require reporting in respect of processing activities and the activities of our customers in certain circumstances or who may request information from us or to whom we are required to disclose information in terms of applicable law, in terms of applicable law and in certain circumstances.