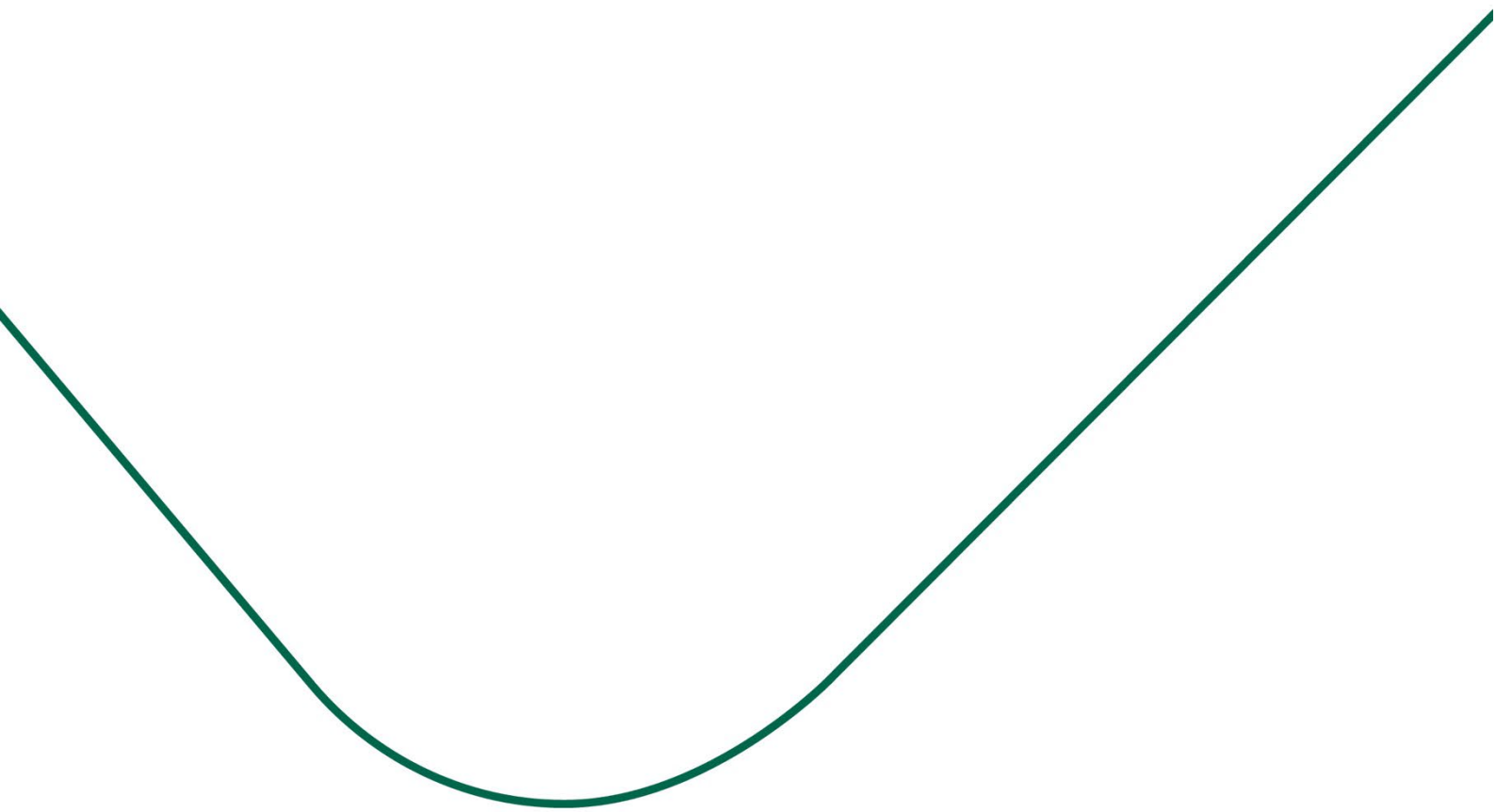
Data Privacy Policy

January 2023



APS bank

values you can bank on

Overview

APS Bank plc (the controller) is a public limited company having company registration number C2192 and its registered office at APS Centre, Tower Street, Birkirkara, BKR 4012.

Our main contact details are, telephone number: +356 2122 6644 and email address: info@apsbank.com.mt.

We are part of a structure which includes ReAPS Asset Management Limited which is a subsidiary and ultimately owned by APS Bank plc.

You may hold investments in a sub-fund of the UCITS Scheme APS Funds SICAV plc having company registration number SV 78 and its registered office at APS Centre, Tower Street, Birkirkara, BKR 4012 ("APS Funds SICAV"). This Scheme is organised as a multi-fund investment company with variable share capital and consists of multiple funds and sub funds (the "Fund"). For those who hold investments in these Funds, APS Funds SICAV will also be a data controller and the APS Funds SICAV Privacy Policy will also apply.

APS Bank plc has also been appointed to act as the Main Distributor of the Fund alongside other third party investment Firm Distributors. You may also hold investments traded by APS Bank plc directly in your name or held under the Bank's nominee. APS Bank plc is authorised to act as a distributor to other third party investments providers as well as a Tied Insurance Intermediary to insurance companies.

This privacy policy applies to personal information held by APS Bank plc and explains how personal information is collected, used and disclosed by APS Bank and its subsidiaries (collectively, 'APS Bank', 'Bank', 'we', 'our' or 'us').

APS Bank is committed to respecting the privacy of your personal information.

This policy describes how we process information in support of the provision of our products and services as well as other lawful purposes in accordance with applicable data protection legislation including the General Data Protection Regulation (Regulation 2016/679) (the "GDPR" or "Data Protection Laws").

This privacy policy 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, investments and debit cards, mortgages, insurance intermediation, pensions as well as any future updates to products and services offered by the Bank including and any new product/ service.

(I) Definition of personal data

Personal data means any information that identifies you as an individual or that relates to an identifiable individual.

Whenever it is not possible or feasible for us to make use of aggregated and/or anonymised data (in a manner that does not identify you) we are nevertheless committed to protecting your privacy and the security of your personal data.

We collect personal data in various ways depending on how you engage with us: digitally via our websites including www.apsbank.com.mt, maltasustainabilityforum.com (collectively "Website/s") and any other future websites or when you choose to provide us with data or in some cases, automatically or from third parties (with permission to share it with us) as well as non-digitally for example when you fill in a physical form to benefit from one or more of our products or services.

(II) Information we collect

The information we collect depends on the products/services that you are interested in.

Such information may include current and historical information about you including:

- Identification related data e.g. name, contact information, gender, date and place of birth, country identification documents (photo ID, passport, national ID card);
- Data about your education, profession or work;
- Details of your family members and other relationships, including your marital status;
- Financial information e.g. history and information collected, your credit rating or history and information such as account, profile and balance provided for banking and investment purposes such as summary of assets, protection and retirement planning & loans & other credit facilities;
- Due Diligence information (including country of origin, residence, citizenship, source of funds and wealth);
- Other regulatory requirements e.g. country of taxation or foreign tax payer reference and anti-money laundering requirements;
- Market research e.g. information obtained from surveys and focus groups;
- Special categories of data concerning health, medical questionnaires and marital status required for insurance and loan products (where applicable) which is passed on to third party companies for processing of products/services including contracts as well as claims;
- Legal documentation (including but not limited to court decrees, court judgements and powers of attorney) concerning special or general authorizations, which may include health, marital and family status;
- Press cuttings and other information relating to court proceedings or convictions against You and similar information on any other person where such information may affect Our relationship with You;
- Online identifiers (including IP addresses, 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);
- CCTV and our systems capturing image, video and audio footage (for more information see *'CCTV and Telephone Recordings'* section below and notifications);
- Any other information provided during our interaction whether face-to-face, online, by phone, email or otherwise.

The collection of your personal information such as your Identification and Due Diligence

related data can occur during our customer acceptance, appropriateness and due diligence process, at account opening stage or in response to additional information on a particular product/service such as investments in line with relevant laws and regulations. If you do not provide us with the personal information required we may not be able to process or assess your application to provide you with our products and services.

Personal information is in most instances collected directly from you. You are responsible for making sure the information you give us is accurate and up to date and inform us of any changes as soon as possible.

External Sources: We may also collect information about you from publicly and externally available sources such as, but not limited to information from public data sources, the Electoral Register, the Central Credit Register maintained by the Central Bank of Malta and other databases provided by third party providers such as Credit Info (mt.creditinfo.com/contact-us) and The Malta Association of Credit Management (www.macm.org.mt/contact).

We may use this information to keep your data up to date on our databases and to verify information we collect. We may also use this information for profiling and marketing purposes, please see our *'Direct Marketing, Profiling and Market Research'* section. Moreover, this information may be used to comply with our internal policies and our legal obligations including amongst others, the prevention and detection of financial crime, money laundering and funding of terrorism and to ensure compliance with court decrees/judgements and powers of attorney.

We may also use any information and documentation held by the Bank, concerning you, in court when testifying, after being exempted from professional secrecy or in certain limited cases by all the involved parties and also when required to file judicial documentation.

(III) The purpose of handling your personal information

We will only process the personal information collected from you or from external sources when we have a lawful basis to process your personal information, in line with the GDPR.

We will process your personal information for the following purposes and lawful reasons:

- When we need to process your personal information to enter into or administer a contractual agreement we have with you, for example, to provide you with the appropriate products and services, to administer, access and manage your accounts, communicate with you by providing you with necessary notices, process your transactions and instructions, provide you with online internet and mobile banking applications and communicate our policies and terms;

- To calculate fees based on domestic and international use of the card on the account;

- When we need to process your personal information and documentation held by the Bank to comply with our legal obligations including:

    - testifying in court and the establishment and also when required to file judicial documentation;
    - exercise or defense of legal claims;
    - to monitor the use of your accounts and services;
    - to prevent unauthorised access and/or unauthorised administration of your funds;
    - carry out customer due diligence and screening in line with our legal responsibilities including amongst others the prevention or detection of financial crime;
    - the filing of regulatory returns to the relevant competent authorities; and
    - for audit and investigative purposes.

- When processing of your personal information is necessary for the performance of a task carried out in the public interest such as the prevention and detection of financial crime, fraud, money laundering and terrorist activity and the provision of financial and other services to persons who may be subject to sanctions. This includes but is not limited to:

    - the verification of customer's identity and suitability for the product;
    - customer's ability to meet financial commitments;
    - to recover debt and in order to comply with the Bank's obligations under any applicable laws and regulations, including for tax compliance purposes.

This may require the disclosure of information to third parties in Malta and overseas, governmental, regulatory or tax authorities, fraud prevention or law enforcement agencies, credit reference and debit recovery agencies or to any other person that the Bank considers necessary for these purposes.

- When we have your consent to process your personal information for a specific purpose –we will ask for your consent to send you direct marketing material if you are not an existing customer of APS Bank.

- When we need to pursue our legitimate interest such as:

    - in the defense and protection of our legal rights and interests;
    - to manage our relationship with you and for product and business development to improve our product range and customer offerings through better understanding your needs;
    - to provide you with information and marketing on our products and services we think may be relevant for you (unless you tell us otherwise, to request to opt-out of direct marketing kindly see *'Request to Opt-Out/Object'* and *'Contact Us'* sections below); and send you newsletters and information about financial matters in general that we think might be of interest to you;
    - placing marketing phone calls;
    - to undertake risk management;
    - to conduct due diligence to determine your eligibility and suitability to our products and services;
    - for customer profiling and data analytical purposes to better understand products and service preferences and categories of customers' behaviours (unless you tell us otherwise, to request to object to personal data profiling (where applicable), please see *'Request to Opt-Out/Object'* and *'Contact Us'* subsections below).

- Processing is necessary in order to protect vital interest.

- Processing special categories of data such as health and marital status when this is necessary and in accordance with Data Protection Laws, including but not limited to:

    - Processing necessary for obligations and exercising specific rights of you or APS in the field of social security and social protection law or necessary for the management of health services;
    - Processing necessary to protect your vital interest or another person where subject is incapable of giving consent;
    - Processing necessary for legal claims;
    - Substantial public interest and public health;
    - Alternatively, where appropriate we may seek your explicit consent.

Initials: _____

We use various measures to keep your information safe and secure and require our staff and our designated third parties to protect information. We respect the essence of the right to data protection and provide appropriate safeguards for data subjects' fundamental rights and interest.

Direct Marketing, Profiling and Market Research

Personal data is processed in the context of marketing, product and customer profiling and data analysis and market research. This processing forms the basis for marketing, product and business development to offer you similar products and services, improve our product range and customer offerings.

Research, Product and Business Development

We will be using your personal information (based on the information you provide to us and through your interactions through the Bank's services/products) for research purposes, such as evaluating customer experience and quality checks and identifying how we can improve our services and products, prioritising our product features and improving product designs through analysis in terms of preferences and customers' need, including price sensitivity amongst other parameters.

For this purpose we may contact you physically or digitally for example via email, telephone or in person to participate in online surveys and focus groups.

Direct Marketing

We may also use your personal data to send you direct marketing material and notifications by post, email, telephone, text messages, and via the Bank's internet and mobile banking facilities as well as online channels.

Marketing communications includes communications and materials on savings, current, term deposits and other bank accounts, loans and overdrafts, investment opportunities, debit cards, mortgages, insurance intermediation, pensions as well as any future offerings.

Our *Research, Product and Business Development* also helps us evaluate creative campaigns to ensure that communication is relevant, customised and tailored to what may be of interest to you and customers.

We may also send you communications including newsletters and emails about general financial matters and other non-financial services.

Third Party Marketing

Where we have the necessary permission to do so we may also send Direct Marketing materials related to products and services of our selected third parties.

Our third parties currently include:

- APS Funds SICAV*;
- IVALIFE Insurance Limited (https://www.iva.life/);
- MAPFRE MSV Life p.l.c. (www.msvlife.com/life-insurance/personal);
- Communication, telecom, information technology companies, aviation, travel & tourism services, retailers, utilities companies, insurance, financial and payment services and real estate agencies amongst others.

We do not share your personal data with third parties for direct marketing purposes unless there is consent to do so.

Initials: _____

(* in some situations may be deemed to be a separate third party entity).

Marketing Profiling:

Customer Profiling and Data Analysis

The Bank uses data to analyse product performances, trends and to carry out customer segmentation and targeted marketing based on data that is generated by the customer through the Bank's services/products and typical profiles, for example, we utilise anonymised personal data, and use analytics to indicate parameters such as age, gender, marital status, residency, loan amount, income by salary bracket and investments in particular securities.

We may analyse this information to send you tailored marketing communications.

Cardholders

Personal information about you as a cardholder and your account is put onto the Bank's database and processed, analysed and assessed by the Bank to provide you with relevant services and product offers, Direct Marketing as well as for profiling purposes, unless you tell us otherwise.

Please note that if you are a Visa card holder with APS Bank, in the event that the Bank re-issues a new VISA card for you, for example due to expiry or damage to the card, your new card details will be securely exchanged with acquirers for credential-on-file merchants through the Visa Account Updater (VAU) application. In the case of loss, fraud or theft, the Bank will notify the merchant of this event only and the merchant will contact you directly requesting your new card details. All of the above applies only in those instances where you have given your card details to the said merchants for recurring transactions and/or subscriptions.

We share your card information in the manner explained above on the basis of our legitimate interests, as understood by Article 6(1)(f) of the GDPR, which include abiding by the requirements of VISA. VAU provides you with a seamless card update process.

If you don't want to have your cards automatically updated in this manner, you can opt out of this service (or opt back in) by sending a secure message through myAPS or by visiting any one of our branches. However, opting out means that you will need to communicate any Visa card changes directly with those merchants with whom you have recurring transactions and/or subscriptions.

Investment Customer Personal Data Profiling

In case of investment clients, where applicable, our investment advisers as Distributor (for APS Funds SICAV and other third party fund providers) may review your Financial Information and assets from time to time to determine interest to investment products, where profiling is on a personal basis we will get your permission to do so.

Home Loan Insurance Customer Profiling

In case of home loan clients, where applicable, our insurance representatives will offer home and life insurance products from third parties (please see *'Third Party Marketing'* section), where profiling is on a personal basis we will get your permission to do so.

Online & Social Media Advertising

We make use of social media platforms, such as Facebook, Instagram and Google Search, so as to promote our products by for example, through paid for advertising, banners, displays, posts. We do not send your personal data to social media, please also see our *'Cookies and other tracking technologies'* section.

Initials: _____

Request to Opt-Out/Object

If you wish to object to personal data market profiling (where applicable), do not want to receive any direct marketing communication or participate in market research, as well as indicating your preference on the relevant application forms, you can request to opt out by contacting us on marketing@apsbank.com.mt or via post (APS Bank plc, F.A.O. MARKETING Department, APS Centre, Tower Street, Birkirkara, BKR 4012 Malta).

Non-Marketing Profiling:

Application Customer Profiling

As part of the Bank's ongoing AML obligations and the Bank's customer acceptance policy, regular customer profiling activities are undertaken by:

- *Collecting identification documents to verify customer's identity;*
- *Assessing data provided by the customers that is verified against official documentation, third party provider databases and open-source information using standard internet search engines;*
- *Undertaking risk scoring using standard methodologies in line with the Prevention of Money Laundering & Funding of Terrorism Regulations.*

Based on this information, the Bank takes an impartial and informed decision on whether the customer falls within its risk appetite based on our internal policies and legal responsibilities.

We may also request information from External Sources, and use any of this information for identification and verification purposes, debt tracing and the prevention of and detection of financial crime, money laundering and funding of terrorism and management of the customer accounts.

Investments Appropriateness Test and Suitability Testing

As a Distributor to APS Funds SICAV and other third party investments providers, we may need to conduct an Appropriateness Test or a Suitability Test in order to be able to assess the relative appropriateness or suitability of the product with your needs. As a result we will input a set of data relating to your financial background, investment knowledge and experience and score the result based on data inputted. This is not an automated decision making process.

CCTV and Telephone Recordings

CCTV and our systems capturing image, video and audio footage

All the Bank premises, property and surrounding areas are covered by CCTV (closed-circuit television) Surveillance Systems. The use of CCTV imagery and access control is mainly to ensure the safety of staff members, customers and other third parties who visit the Bank and its facilities, security of such persons and property, whilst detect, investigate, prevent crime and specific security incidents.

Cameras are strategically located in sensitive areas throughout the premises of the Bank, both in public and non-public areas.

The exact location of the cameras is confidential and restricted information due to security reasons. However, where there is a CCTV camera, signage is usually prominently placed at strategic points to notify staff members, visitors and members of the public that a CCTV System is in operation in that area.

Telephone Recordings

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

- Call centre: for providing you with a service including instructions that you provide to effect transfers on your behalf, to follow up on your complaints and for occasional call grading and training;
- Trading Desk/Asset Liability Management/Investment Management Unit/Wealth Account Services related calls at any stage of an investment transaction per regulation/law;
- Operations Department (cards, credit and cash services units): you might be contacted by these departments in case of any cash discrepancies found when processing deposits from bulk deposit machines, instructions on card limits, potential fraud and guidance on unutilised balances on loan accounts;
- Retail banking/branches: for calls relating to your account and instructions;
- Voice of the Customer: for calls pertaining to complaints/feedback for complaints handling and service quality purposes.

(IV) Disclosing your personal information to Third Parties

We may share your personal information with others where lawful to do so in the following instances:

- During the provision of products and services and to fulfill our contractual obligations we may share your personal information with other companies to provide you with the products or services you require such as for insurance products/services, to transfer funds to/from your beneficiaries/originators, joint account holders, attorneys appointed through a power of attorney, fund managers, custodians and administrators, curators or executors, trustees, intermediaries, correspondent/agent banks, payment service providers, clearing houses, clearing or settlement systems;
- With our subsidiaries and the APS Funds SICAV plc sub funds who may assist in the provision of your products and services;
- With our associated companies such as the Investment Manager in our role as sub-Investment Manager, including but not limited to Distributors and Administrators, service providers who assist us in the provision of your products and services – for example as Distributor to other third party investment providers as well as in our capacity as a Tied Insurance Intermediary to designated insurance companies. We facilitate investment meetings, administer application forms and questionnaires, carry out work for the establishment, performance and conclusion of such contracts and may, from time to time, send marketing material (where there is permission to do so).
- With any counterparties with respect to guarantees issued on your behalf;
- With other financial institutions and other third parties who have a security over any of your assets pledged in our favour and who are acting as sureties and/or guarantors, your representative, including sending them relevant correspondence;
- With the courts of law when required to disclose your personal and financial information when, amongst others, summoned to testify filing a schedule of deposit, filing of judicial acts and any other court-related matter;
- To correspond with and/or seek assistance from lawyers, architects, surveyors and other third parties as necessary;
- With regulators, auditors, courts, Central Bank of Malta, credit rating and fraud prevention agencies and other authorities as required for us to comply with our legal obligations and for reporting, compliance, auditing and investigative purposes;

Initials: _____

- With third party marketing and printing companies for the purpose of carrying out survey, printing and communicating promotional material on our behalf;
- Other parties in connection with litigation or asserting or defending legal rights and interests including but not limited to when processing information with regards to defaulting customers with external lawyers, filing of judicial acts in court and providing information to the Central Credit Register in relation to facilities granted to you;
- With your employer/s, if you are benefitting from certain schemes such as an employee scheme facility;
- With Merchant Acquirers where you have given us your consent to do so;
- With IT service providers, vendors, including cloud, website and security service providers who are contracted by us to provide digital products and solutions and carry out technical, support and maintenance on the data on our systems.

When sharing your personal information we will always ensure that we adhere to applicable law and regulations.

(V) Transferring your personal information outside the European Economic Area ('EEA')

For the purpose of providing you with our products or services, to fulfill our legal obligations, to protect the public interest or for our legitimate interest we may be required to transfer your personal information to so called third countries i.e. countries outside the EEA. Such transfers can be made if any of the following conditions apply:

i the EU Commission has determined that there is an adequate level of protection in the country in question; or

ii other appropriate safeguards have been taken such as the use of standard contractual clauses approved by the EU Commission or the data processor has valid binding corporate rules in place; or

iii in exceptional circumstances such as to fulfill a contract with you or subject to your consent to a specific transfer.

(VI) Retaining your personal data

We will retain your personal data only for as long as is necessary (taking into consideration the purpose for which it was originally obtained). The criteria we use to determine what is 'necessary' depends on the particular personal data in question and the specific relationship we have with you (including its duration).

Our normal practice is to determine whether there is/are any specific EU and/or Maltese law(s) (for example tax, anti-money laundering or corporate laws) permitting or even obliging us to keep certain personal data for a certain period of time (in which case we will keep the personal data for the maximum period indicated by any such law).

We would also have to determine whether there are any laws and/or contractual provisions that may be invoked against us by you and/or third parties and if so, what the prescriptive periods for such actions are (this is usually two (2) or five (5) years). In the latter case, we will keep any relevant personal data that we may need to defend ourselves against any claim(s), challenge(s) or other such action(s) by you and/or third parties for such time as is necessary.

Where your personal data is no longer required by us, we will either securely delete or anonymise the personal data in question.

(VII) Your privacy rights

You as a data subject have rights in respect of personal data we hold on you. These rights include (as applicable):

- Accessing personal information APS Bank holds about you and the information related to its processing;
- Requesting the rectification of data if it is incomplete or inaccurate;
- Requesting the erasure of data unless we are required to retain such data;
- Requesting the withdrawal of your consent for a specific processing activity;
- Receiving in a structured, widely-used format, the personal information related to you which you have provided to APS Bank and transfer them to another controller where technically possible (data portability);
- Objecting or restricting the processing of personal data in instances such as marketing and profiling.

All of the above requests may be forwarded, if applicable to third party processors involved in the processing of your personal data as previously listed.

You can exercise your rights through the following channels:

- as per details provided in 'Request to Opt-Out/Object' sub-section (where applicable),
- by visiting one of our branches (please bring your ID card with you as this may be needed for verification purposes),
- sending a message through the internet banking channel (under Topic title 'GDPR Rights'),
- or by sending a letter to the attention of the Data Protection Officer, APS Bank plc, APS Centre, Tower street, Birkirkara BKR 4012, Malta, specifying your ID card number as well as including your original signature (unless the letter request is made on your behalf by your legal counsel).

We may accept requests via electronic mail but only in exceptional circumstances and only if we are satisfied that we can adequately verify your identity via such channel. Such special requests will be analysed on a case-by-case basis and may require that you send us adequate supporting documentation. For reasons of added security and also, out of convenience to you, we encourage you to use the channels specified above wherever possible. If you are an existing customer, using the internet banking channel is the fastest way to reach us without requiring additional identity verification.

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.

You may also file a claim with the Data Protection Authority, the Information and Data Protection Commissioner's Office (idpc.org.mt) or to the respective data protection regulator in your country particularly when you consider that the exercise of your rights has not been achieved satisfactorily.

(VIII) Automated decision making

If you are a prospective customer trying to apply to be onboarded with us through the MyAPS application (digitally), you may be subject to automatic decision making taken solely by automated means. According to the data you input into the MyAPS application system at onboarding stage, you may be automatically rejected or allowed to proceed with your

application by having an appointment set with a Branch to continue the application process. This automatic decision-making operates on the basis of the Bank's internal Customer Acceptance Policy. Since such processing solely by automated means is necessary for you to enter into a contract with us (if your application is acceptable to us), we will process your personal data in this manner on the basis of our contractual necessity without requiring your consent with the suitable measures to safeguard your rights and freedoms and legitimate interests (as per Article 22 of the GDPR). If your application is rejected, such that you are not given an appointment with a Branch to continue the application process, you have the right to approach a Branch to request that your application be reconsidered by means of human intervention.

If you are a prospective or an existing client trying to apply for a loan or credit facility with us, you may be subject to decision making taken solely by automated means, including profiling (at least at the first stage). The credit scoring program automatically generates a set of questions based on the number of clients/non-clients involved and the chosen product, some items will be populated from our internal systems resulting from data provided by you. According to the answers which are populated in the system, the score shall be automatically calculated (each answer tallies with a pre-determined score) and a result shall be determined according to the sum of the answers inputted. According to predetermined score levels, you can either be rejected or accepted or, if the result is neither an acceptance or rejection, your request will be manually assessed by one of the Bank's representatives for an acceptance or rejection. A number of factors may lead to the rejection of your application, including but not limited to high commitments and lack of propensity to save. The credit scoring methods used are regularly tested to ensure that they remain fair, effective and unbiased. This is done by means of regular quality assurance checks and algorithmic auditing, amongst other methods. Since such processing solely by automated means is necessary for you to enter into a contract with us (if for example, your credit score is acceptable to us), we will process your personal data in this manner on the basis of our contractual necessity without requiring your consent with the suitable measures as described above to safeguard your rights and freedoms and legitimate interests (as per Article 22 of the GDPR). At the same time, should your loan application be rejected, you have the right to contact the Bank to request that your application be reconsidered by means of human intervention by approaching the relevant Branch or by emailing csc@apsbank.com.mt.

(IX) Security Measures

The Bank takes a number of security initiatives to online security as described as follows:

The personal information which we may process (and/or transfer to any authorised third party, external/third party service providers, subcontractors as the case may be) will be held securely in accordance with our internal security policy, procedures and the law.

To meet appropriate security standards we use all our reasonable efforts to safeguard the confidentiality, integrity, as well as the availability of our IT systems as well as personal data that we may process relating to you and regularly review and enhance our technical, physical and managerial procedures so as to ensure that your personal data is protected from:

- unauthorised access;
- improper use or disclosure;
- unauthorised modification;
- unlawful destruction or accidental loss.

To this end we have implemented security policies, rules and technical and organisational measures to protect the personal data that we may have under our control. This protection shall follow a defense in depth strategy through continuous investment in technology, processes and other resources in line with industry practices. The Bank shall enshrine a risk culture in its operations and across personnel and foster a continuous training programme for all its employees complemented by customer awareness on topical matters.
All our employees and data processors are further obliged (under contract or equivalent) to

respect the confidentiality of your personal data as well as other obligations as imposed by the Data Protection Laws.

Despite all the above measures, we cannot guarantee that a data transmission or a storage system can ever be entirely secure and we are not responsible for matters outside our control.

Our authorised third party legal processors and other Third Parties (kindly see *'Disclosing your personal information to Third Parties'* section) with permitted access to your information are required to apply appropriate technical and organisational security measures that may be necessary to safeguard the personal data being processed from unauthorised or accidental disclosure, loss or destruction and from any unlawful forms of processing.

As stated above, where the said service providers are our data processors, they are also bound by a number of other obligations in line with the Data Protection Laws (particularly, Article 28 of the GDPR).

We require our customers to always be vigilant and observe standard information security precautions such as attackers or fraudsters may try to obtain Banking information by impersonating individuals from the Bank, the Police or other companies that you may trust, so:

- Never disclose your Online Banking Pin or password, CVV, security questions and answers, account numbers, personal information and other confidential account data to anyone over any channel such as phone, email, social media, even if a caller claims to be from your bank or the police;
- Never disclose your hardware and software token codes, Mobile App Secure passcode, online one time password or activation codes to anyone;
- Never transfer money from your account, either online or in a branch after being instructed to do so without checking via trusted source;
- Never allow someone to take control of your computer or other devices if you receive a call or message that you aren't expecting;
- Never assume that a mobile, phone call, email, social media messaging or sms is genuine. Prior to carrying out any operation, transfer etc. always check via a trusted source.

The following are a few security tips to protect yourself online and the security of your account information, in tandem to other security measures that you might wish to further take:

Enhance the security of your account

- Use secure email Message Hub either using the myAPS Mobile Banking, Internet Banking or Secure eMail to send email containing account information or questions;
- Change your password periodically. Choose a password that is difficult to guess;
- Be Aware of Phishing and Scams;
- Keep Your Operating System Up-to-Date;
- Keep Your Software Up-to-Date;
- Keep Your Web Browser Up-to-Date;
- Use Anti-Malware Software;
- Secure Your Wireless Connection;
- Prevent Spyware;
- Use a Firewall;
- Set different Login credentials for Banking and other sites such as social media, e-commerce;
- Take the time to regularly monitor your bank account statement;

- Do not allow anyone else to use your card, online banking logins, account data or personal information;
- If you are shopping online, be sure the website you are visiting is secure (indicated by https:// or A padlock icon,) and has a valid digital certificate before you enter your card number and login details.

It is important that you take all necessary precautions to protect your personal data, alongside this, for updated information on Security and Tips, FAQs and Security Guidelines kindly refer to www.apsbank.com.mt/protect.

Please note that we will never send you an email or message or sms or call you to ask you for or to verify your banking login details, passwords, account numbers and information, PINs or to click on a link to activate or unblock your account. If you receive an email or text message with this request, please take responsibility to delete the message and DO NOT enter the information or click on the link.

If you **believe there has been an unauthorised transaction in your account or you believe the security of your password has been compromised** or if you have responded to any suspicious communication such as giving our your account or online log-in details, **please contact us on +356 2122 6644 or email: info@apsbank.com.mt immediately.**

(X) Omni App

Personal data is processed via the App including user session.

Additionally we store the user profile number after the activation of OneSpan license during log-in.

Although myAPS supports using biometric features to log-in to the application, the Bank is not storing or processing such information. The Bank is relying on your operating system installed on the device to check the validity of the biometric feature used and upon confirmation from the operating system, access is allowed or otherwise. For further information any issues/queries please contact your Operating System (OS) or OneSpan (www.onespan.com/contact-us).

(XI) Cookies and other tracking technologies

We collect information about your usage and activity on our sites using certain technologies such as cookies and other technologies to operate our websites, provide a secure online environment, provide a enhanced online experience, track our website performance and make our website content more relevant to you. Some cookies provide us and social media with insights into any online marketing campaign that we might be running.

For further and more detailed information on how we and third parties use cookies and how you may restrict such contacts please refer to our Cookies Policy located on our website: www.apsbank.com.mt/cookie-policy.

(XII) Changes to the Privacy Policy

We reserve the right, at our complete discretion, to change, modify, add and/or remove portions of this Privacy Policy at any time. If you are an existing client with whom we have a contractual relationship, you will be notified of any changes made to this Privacy Policy.

If you are a user of our website with whom we have no contractual relationship nor a lawful way of tracing, it is in your interest to regularly check for any updates to this Privacy Policy, in the event that our attempts to notify you of such updates do not reach you.

(XIII) Contacting Us or the Data Protection Authority

Contact Us

If you have any questions or concerns regarding our privacy policy you can contact our Data Protection Officer by sending an email to dataprotectionofficer@apsbank.com.mt or a letter to the Data Protection Officer, APS Bank plc, APS Centre, Tower Street, Birkirkara, BKR 4012, Malta.

Data Protection Authority

If unsatisfied, you can also lodge a complaint or contact the Data Protection Authority in any of the countries where we provide services or products to you.

Signature: _____ Date: DD/MM/YYYY