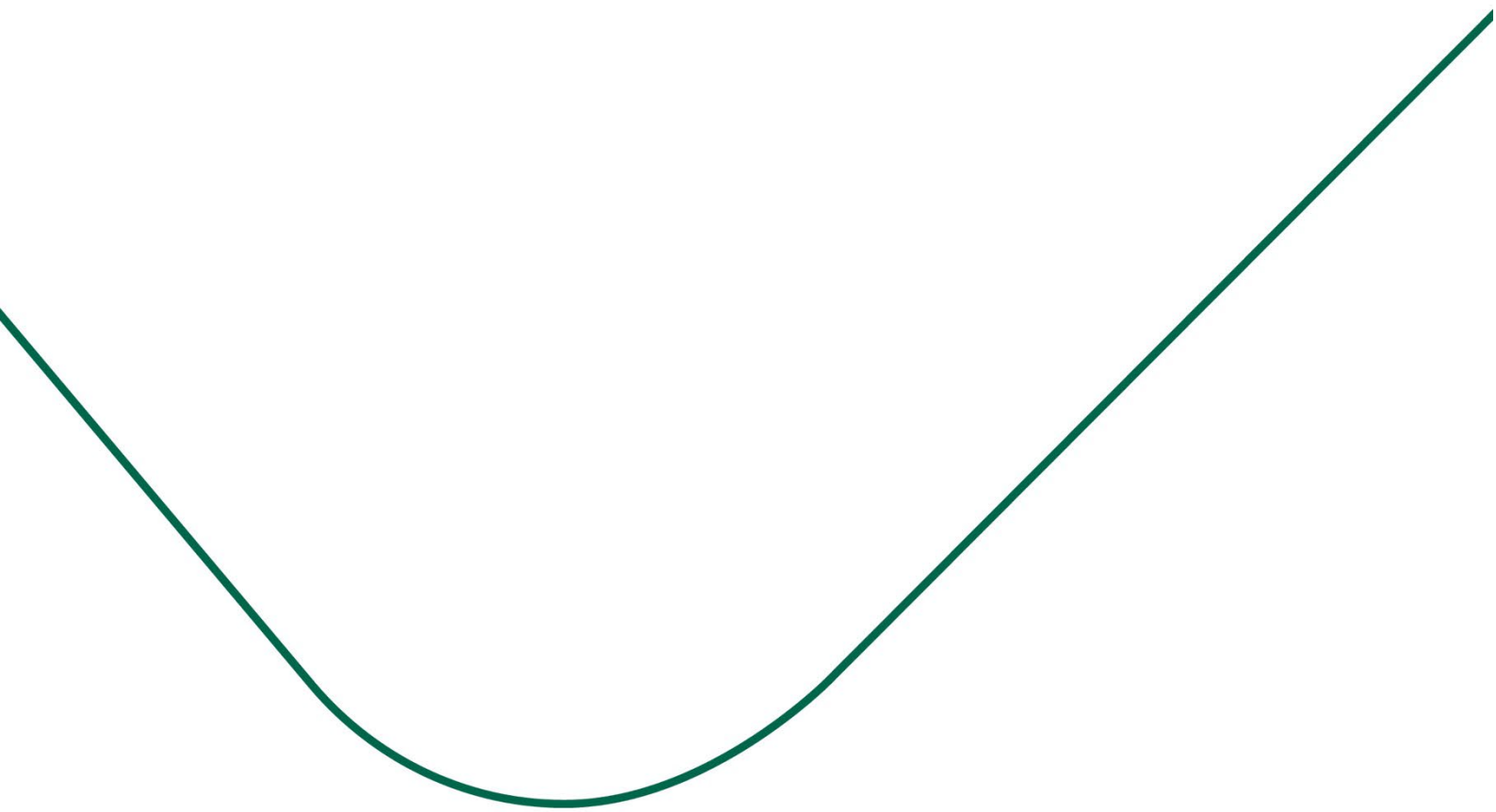
Data Privacy Policy

April 2025



APS bank

values you can bank on

Contents

Policy Overview

APS Bank plc is committed to protecting and respecting Your privacy.

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.

As part of this ongoing commitment and in line with our obligations under the EU General Data Protection Regulation 'GDPR', We have put in place a Data Privacy Policy that We keep regularly updated as well as internal procedures that are also regularly evaluated and updated as needed.

The APS Data Privacy Policy applies to personal information held by APS Bank plc and its subsidiary as data controllers. This Policy is meant to help You understand what information We collect, why We collect it, and how You can update, manage, and delete Your information. We believe that We have a duty to help You better understand Your various rights at law.

If there are any substantial changes in the way We process data or changes that will affect You directly, We will notify You of these changes by updating this Policy as referred to in Section 16.

About Us

APS Bank plc is regulated by the Malta Financial Services Authority as a Credit Institution under the Banking Act 1994 and to carry out Investment Services activities under the Investment Services Act 1994. The Bank is also registered as a Tied Insurance Intermediary under the Insurance Distribution Act 2018.

APS Bank plc also provides products and services through its subsidiary, ReAPS Asset Management Limited, which is ultimately owned by APS Bank plc. ReAPS Asset Management Limited is licensed by the MFSA as an Investment Manager and UCITS Manager under the Investment Services Act.

How is this Policy applicable to You?

We collect Your personal data from You when You make use of our products and services through our branches and digital channels, such as myAPS, our website and through our Contact Centre.

We may also collect Your personal data from other sources. This is explained in more detail in Section 4 "What personal information is collected about You?".

The term 'personal data', refers to:

- all personally identifiable data about You
- information that can be used to identify You personally

This Data Privacy Policy explains what personal information We collect, how this is used, and Your rights over Your personal data. All data collected is in line with the relevant rules and regulations.

Emanating from the Data Privacy Policy, there are two other policies that provide further background on the processing of Your personal data. Both policies are available on the Bank's Website and these are the:

- Cookies Policy to ensure the proper functionality of the Bank's website ensuring a better user experience; and
- CCTV Policy, providing an overview of how the CCTV footage system is used and managed throughout the Bank's property.

Initials: _____

Personal data collected about You by Us

Information is collected when You:

- Call Us or visit one of our branches
- Provide Us with the data Yourself
- Visit our website and mobile channels
- Complete any forms
- Correspond with Us
- Participate to any of our surveys
- Open an account or use any of our services
- Register to attend discussions/focus groups/workshops

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.

The following types of information is collected:

Personal Details: name, gender, date of birth, place of birth, country of birth, nationality, citizenship, marital status, identification document details;

Contact details: address, email address, landline and mobile number;

Occupation & Income: employment details, salary information and employer's details, source of funds and wealth;

Domicile and residency: Your country of residence, tax residency information and tax identification number;

Other details: further information may be collected to conduct due diligence checks, anti-money laundering checks and sanctions.

Copies of Your identification document (for example ID Card, Driving Licence or Passport) and any other information that may be provided to prove that You are eligible to use our services;

Details of the bank account, including the account number and IBAN;

Details of the APS debit and credit card including the card number, expiry date and CVC (the last three digits at the back of the card);

Your myAPS username (this is the username used when using myAPS);

Record of discussions held when interacting through any of the Bank's e-channels (such as by phone, face to face, email, myAPS secure messaging system);

Your image in photo or video format as captured through CCTV;

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 and other credit facilities;

Information that is passed on to third party companies for processing of products/services including contracts and claims: special categories of data concerning health, medical questionnaires and marital status. This information is required for insurance and loan products.

Business Customers: We collect, and process personal data of the individuals authorised to set up the account and give Us instructions about the account. We may also collect and process personal data about other authorised personnel of the Business Customer that receives APS Business Banking Services.

Data protection laws do not apply to information about legal entities (for example, limited liability companies). However, they do apply to people.

Information collected from use of our website and internet banking (including myAPS) When You use our website or myAPS, We collect the following information:

Online identifiers (including Internet Protocol (IP) address, cookie and information data generated via Your browser), Your login information, the browser type and version, the time zone setting, device language, the operating system and platform, the device You use (if the device uses a virtual private network (VPN)) and a unique device identifier.

Information about Your visit, including the links You have clicked, through and from the website or myAPS application, page response time, services You viewed or searched for, download errors, length of visits to certain pages, page interaction information and methods used to browse away from the page;

Information on transactions and Your use of APS products (for example, payments into and out of Your account), including the date, time, amount, currencies, exchange rate, beneficiary details, details of the merchant or ATMs associated with the transaction, IP address of sender and receiver, sender's and receiver's name and registration information, messages sent or received, details of device used to arrange the payment and the payment method used.

Although myAPS supports using biometric features to log-in to the application, We do not store or process such information. We rely 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 or any issues/queries please contact your Operating System (OS).

Information from other and publicly available sources

Personal data is collected from third parties, public data sources, such as the Central Credit Register maintained by the Central Bank of Malta, Credit Reference Agencies and other databases provided by third party providers (such as Credit Info and the Malta Association of Credit Management). Information about other people such as joint account holder, spouse or family. This includes Your credit record, information about late payments, information to help Us check Your identity.

Legal documentation (including but not limited to court decrees, court judgement and power of attorney) concerning special or general authorizations, which may include health, marital and family status.

Information on court proceedings or convictions against You and similar information on any other person where such information may affect our relationship with You.

Information about detection of any suspicious and unusual activity and information about parties connected to You on these activities.

This information is used for enhanced due diligence obligations, security searches and KYC purposes and other applicable laws, and to assist with fraud monitoring.

Digital Onboarding

We have collaborated with Onfido SAS, a company incorporated and registered in France, to provide for document check and verification as per applicable due diligence requirements.

In case, You make use of this service and at the time You are a resident of the United States, You hereby acknowledge that Onfido SAS may lawfully obtain your personal data (including biometric identifiers and/or biometric information) for the purpose of providing the services in accordance with applicable biometric information laws, including the Illinois Biometric Information Privacy Act (BIPA), in particular the requirements pertaining to providing notice and obtaining consent (where required) as outlined in Onfido's Facial Scan Policy (https://onfido.com/facial-scan-policy-and-release/), Onfido's Developer Guides (https://developers.onfido.com/guide/onfido-privacy-notices-and-consent) and Onfido's Terms of Service (at https://onfido.com/terms-of-service/).

Initials: _____

Information from social media

The Bank may use publicly available information about You from selected social media websites or applications to carry out enhanced due diligence checks. Publicly available information from social media websites or apps may also be provided to Us when We conduct general searches on You (for example, to comply with our anti-money laundering or sanctions screening obligations).

Information collected throughout the recruitment process

Personal data included in a CV, application form, covering letter or interview notes, such as qualification, skills, experience and employment history. Information about Your entitlement to work in Malta (where applicable), references, and any other information, voluntarily disclosed by You, for which the Bank needs to make reasonable assessments during the recruitment process.

Our legal basis for using Your personal data

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 Article 6 – Lawfulness of Processing.

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

Contractual

When We need to process Your personal information to enter into or administer a contractual agreement We have with You, for example the:

- maintenance of Your banking relationship with Us. To provide You with the appropriate products and services, to administer, access and manage Your profile and accounts, communicate with You by providing You with necessary notices and keeping You up to date with any news on Your banking relationship with us, process Your transactions and instructions, and communicate our policies and terms from time to time.

Legal Obligations

When We need to process Your personal information and documentation held by the Bank to comply with our legal obligations including:

- 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;
- for audit and investigative purposes;
- testifying in court and the establishment and when required to file judicial documentation; and
- exercise or defence of legal claims.

Public interest

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 Your identity and suitability of the product;
- Your 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 authorised third parties in Malta and overseas, governmental, regulatory or tax authorities, fraud prevention or law enforcement agencies, credit reference or to any other person that the Bank considers necessary for these purposes.

Consent

When We have Your consent to process Your personal information for a specific purpose.

Legitimate interest

When We need to pursue our legitimate interest such as:

- in the defence 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;
- send You newsletters and information about financial matters in general that We think might be of interest to You;
- to undertake risk management;
- to conduct due diligence to determine Your eligibility and suitability to our products and services; and
- for customer profiling and data analytical purposes to better understand products and service preferences and categories of customers' behaviours.

Vital Interest

Processing is necessary in order to protect vital interest or another person's where subject is incapable of giving consent

How do We use Your personal data?

The following is a description of how We use Your personal data and the corresponding legal grounds We rely on for doing so.

Purpose of Processing	**Categories of Personal Data**	**Lawful Basis for Processing**
Booking an appointment with Us to start Your banking relationship.	Registration details	Contractual
Setting up Your personal profile on our systems to record You as a customer.	Registration Details, Personal Information, and Communication Data	Contractual Legitimate Interest (to ensure We have accurate and up to date details)

Checking Your identity: We will use Your personal data to check Your identity or the identity of joint account holders (as part of our KYC obligations). During digital on-boarding, we will aslo gather 'biometric data' to verify your identity as part of our KYC checks, to authenticate as you as an authorised user, or to detect and prevent fraud. . This data is collected in photo form, and facial scan data extracted from your photo.	Personal Information Identification and Verification Data	Contractual Compliance with Legal Obligations Substantial Public Interest Consent
Providing our Services/Managing our relationship with You: Whenever You apply for or use one of our products or service, We will use Your personal information to: • evaluate Your application • meet our contractual and legal obligations relating to any products or services You use (for example, making payments into and out of Your account, withdrawing cash or making payments with Your APS debit/ credit card) • recover debt and exercise other rights We have under any agreement with You • offer investment provision and tied insurance intermediary services in line with Our licenses • provide You with customer support services. We may record and monitor any communications between You and us, including phone calls, to maintain appropriate records, check Your instructions, analyse, assess and improve our services, and for training and quality control purposes. • Authenticate You as a registered and authorised user of our products and services when necessary and tell You about changes to our services. • Help keep our website and myAPS app safe and secure	Personal Information Identification and Verification Data	Consent Contractual Compliance with Legal Obligations Legitimate Interest

AML/CFT and due diligence purposes	Identification and Verification Data	Compliance with Legal Obligations
Background, Sanction, Fraud and Credit Checks	Personal Risk Information Personal Information made publicly available on apps/ websites used for enhanced due diligence checks, security searches and KYC.	Conditional Consent Legitimate Interest Substantial Public Interest Compliance with Legal Obligations
Providing You with marketing material, You may have requested from Us or that We may be authorised at law to provide to You	Marketing Data	Consent (when needed) Legitimate Interest (when consent is not needed)
Research and anonymous statistical datasets used for evaluating customer experience and quality checks, identifying how We can improve our products and services, prioritising our product features and improving product designs through analysis in terms of preferences and needs, and to comply with requests from competent authorities	Market Research and Statistical Data	Legitimate interest (to conduct research and analysis, including to produce statistical research and reports) • Legal obligations

If there is the need to start processing Your data for any purposes which is entirely unrelated to the above, We will inform You of such processing in advance and You may exercise Your applicable rights (as explained in "Your rights as a data subject").

Please be aware that without certain Personal Data/Information relating to You, We may not be in a position to provide some or all of the services You expect from Us.

Do We make automated decisions about You?

Depending on the Bank's products or services You use, We may make automated decisions about You. This means that We may use technology that can evaluate Your personal circumstances and other factors to predict risks or outcomes. This is sometimes known as profiling. We do this for the efficient running of our services and to ensure decisions are fair, consistent, unbiased and based on the right information. Where We make an automated decision about You, You have the right to ask that it is manually reviewed by an individual.

For example, We may make automated decisions about You that relate to:

Account Opening:

- KYC, anti-money laundering and sanctions checks
- identity and address checks

Determining credit eligibility:

- assessing whether You are eligible to apply for a credit product

Approving credit applications:

- credit and affordability checks to see whether We can accept Your credit application
- setting credit limits

Monitoring credit agreements:

- assessing how You're repaying any credit product You hold with us
- amending Your credit limit
- terminating Your credit agreement

Detecting fraud:

- monitoring Your account to detect fraud and financial crime

Determining Appropriateness/Suitability of a Financial Investment:

- conducting 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, based on Your financial background, knowledge and experience, investment objectives and risk tolerance and score the result based on data inputted.

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).

Facilitating credit checks on You

We may access and record information about You from publicly and externally available sources such as, but not limited to information from public data sources, 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) to run credit checks if You apply (or tell Us You want to apply) for a credit product.

We will also share Your personal data with the abovementioned providers of credit information to:

- confirm details You have provided when You apply for products or services;
- make an assessment about whether to accept Your credit application; and
- determine an appropriate credit limit for You.

When You enter into a credit agreement with us, We may continue sharing information with the Central Credit Register, such as information about Your repayments and whether You repay in full or on time.

We may carry out additional credit checks on You from time to time to ensure Your financial wellbeing hasn't changed over time.

Using Your personal data for marketing purposes

Our marketing communications include marketing materials and communications about our products and services. We may analyse Your personal data to send You marketing messages

that are relevant and interesting to You. We will assume You want to be contacted by Us with information about our products and services if prior consent has been obtained.

Where We have the necessary permission to do so. We may also send direct marketing materials related to products and services of selected collaborators, which currently include:

- APS Funds SICAV plc
- IVALIFE Insurance Limited
- Mapfre MSV Life plc
- Other private companies We might collaborate with from various industry sectors

We do not share Your personal data with these third parties for marketing purposes unless We have Your consent.

If You do not want to receive any direct marketing communication, You can request to opt-out by sending a secure message on myAPS App/Internet Banking, or by contacting our Contact Centre by calling on 2122 6644 or visit one of our branches in person.

In case of direct marketing sent by e-mail (where We are legally authorised to do so) You will be given an easy way of opting out by unsubscribing from any such communications.

You may still receive communications including generic information or certain important information on our products and services. We do not share Your personal data with third parties for direct marketing purposes unless there is consent to do so.

We remind You that We are obliged to acquire consent from You before sending marketing material and to provide You with relevant information interesting to You.

Your rights as a data subject

You as a data subject have rights in respect of personal data, We hold on You.

These rights include:

- **Right to know how We use Your personal data** – We provide You with the Data Privacy Policy to explain the purposes, amongst others behind processing of Your personal data/ information.
- **Right of Access/Request** - Accessing Your personal data that We hold about You and the information related to its processing. Upon Your request We shall provide You with a copy of Your personal data undergoing processing.
- **Right to Rectification** - Requesting the correction/amendment of Your personal data or information related to You if it is incomplete or inaccurate.
- **Right to Object and restrict** – You may object or restrict the processing of personal data, such as marketing and profiling, if our lawful basis for using Your personal data is of 'legitimate interest'.

  However, if there is an overriding reason why We need to use Your personal data, We will not accept Your request. If You object to Us using personal data which We need to provide our services, We may need to terminate the relationship as We won't be able to provide the service.
- **Right to Withdraw Consent** – You have the right to request the withdrawal of consent for a specific processing activity at anytime.
- **Right to Erasure** – You may request the erasure of Your personal data if:
  - We have no lawful basis to continue using it

- You have withdrawn that consent, and We have no other lawful basis to maintain Your personal data
- You have successfully exercised Your right to object
- Your personal data was used unlawfully
- We are required by law to delete Your personal data

In some instances, We may not be able to comply with Your erasure request if the processing of Your personal data is required for:

- compliance with a legal obligation to which We are subject to: or
- the establishment, exercise or defence of legal claims.

- **Right to Data portability** - Receiving in a structured, widely used format, the personal information related to You which You have provided to Us and transfer them to another data controller where technically possible.
- **Right to lodge a complaint** – You also have the right to lodge complaints with the appropriate Data Protection Supervisory Authority. The competent authority in Malta is the Office of the Information and Data Protection Commissioner (IDPC), Floor 2, Airways House, Triq il-Kbira, Tas- Sliema, SLM 1549, Malta, +356 2328 7100, idpc.info@idpc.org.mt.

  We kindly ask You to first attempt to resolve any issues You may have with Us first, even though as stated above, You have the right to contact the competent authority at any time.

As a security measure, before being in a position to help You exercise Your rights We will need to verify Your identity to ensure that We do not disclose to or share Your information with any unauthorised individuals.

We try to accede to all legitimate requests within one month from receiving them, however there might be instances where We might take longer than a month, for example in case of particularly complex or multiple requests. In such cases, We will inform You accordingly and keep You updated with progress.

How do You exercise Your rights as a data subject

You can exercise any of Your rights through the following channels:

- By visiting one of our branches;
- By sending a secure message through myAPS/Internet Banking, under 'GDPR';
- By contacting our Customer Service Centre on (+356) 2122 6644; 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 We ll as including Your original signature.

We may accept requests via electronic mail addressed to dataprotectionofficer@apsbank.com.mt 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. We may ask You to revert to the above-mentioned channels if We are not able to verify You.

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 myAPS app/Internet Banking is the fastest way to reach us, without requiring additional identity verification.

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 Information and Data Protection Commissioner's Office, particularly when You consider that the exercise of Your rights has not been achieved satisfactorily.

Sharing Your personal data with third parties

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

Individuals or companies that You transfer money to	Where You make a payment from Your APS account, We will provide the recipient with Your details alongside Your payment such as Your name and IBAN/Bank Account number, given that We are required by law to include certain information with payments.
Individuals or companies that transfer money to You	When You receive a payment to Your APS account, We will provide the payer with Your details (for example, Your name and IBAN/Bank Account number). This is necessary to confirm that the payment has been made to the correct account.
Suppliers / Vendors / Collaborators	To help Us provide and improve our services to You or to help Us improve our website or myAPS. Such as: • IT service providers/vendors • Website and security service providers • Payment services partners and payment schemes • Identity verification and KYC service providers • Card manufacturing, personalisation and delivery • Analytics providers and search information providers • Marketing and Printing companies • Customer service/survey providers • Collaborators for insurance products/services We may work with other collaborators to offer You co-branded services or promotional offers. If this is the case, We will make sure You understand how We and our partners process Your personal data for these purposes.
Subsidiaries and APS Funds SICAV plc sub-funds and associated companies/ collaborators	Who may assist in the provision of products and services, including but not limited to ReAPS Asset Management Ltd, in its role as Sub-Investment Manager to the sub-funds of APS Funds SICAV plc, Fund Administrators, other Banks as Custodians of APS Funds SICAV plc, and any other service providers who assist Us in the provision of products and services. These may include other third-party investment providers where We act as Distributors 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).

Initials: _____

Joint account holders	If You have a joint account with us, We will share account and transaction information between joint account holders. For example, Your co-account holder will see any transactions You make from Your joint account.
Other third parties	To correspond with and/or seek assistance from: • Fund Managers • Execution Venues/Brokers • Your employer and/or any association You are a member of, if You are benefitting from certain schemes such as an employee loan facility scheme • Lawyers, architects, surveyors and other third parties as necessary • Merchant acquirers, where You have given Us Your consent to do so
For legal reasons	We also share Your personal data with other financial institutions, financial services companies, insurance providers, government authorities, law enforcement authorities, tax authorities, companies and fraud prevention agencies to check Your identity, investigate or protect against suspected fraud, keep to tax laws, anti-money laundering laws, or any other laws and confirm that You're eligible to use our products and services; 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; 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; 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.
Where You ask Us to share Your personal data	Where You direct Us to share Your personal data with a third party, We may do so. For example, You may authorise third parties to act on Your behalf (such as a lawyer, accountant or family member or guardian under a power of attorney). We may need to ask for proof that a third party has been validly authorised to act on Your behalf.

When sharing Your personal information We will always ensure that We adhere to applicable laws and regulations.

Transfers of personal data outside the European

As a general rule, the data We process about You will be stored and processed within the European Union (EU)/European Economic Area (EEA) or any other non-EEA country deemed by the European Commission to offer an adequate level of protection ("white-listed" countries).

The USA is also deemed to provide an adequate level of protection where the US recipient of the data is Privacy-Shield certified.

In some cases, it may be necessary for Us to transfer Your personal data to a non-EEA country not considered by the European Commission to offer an adequate level of protection (for example to one or more of our data processors located there).

If We transfer Your personal data to another country that doesn't offer a standard of data protection equivalent to the EEA, We will make sure that Your personal data is sufficiently protected. For example, where required, We have/will ensure that the recipient is bound by the EU Standard Contractual Clauses, or Binding Corporate Rules or one of the other alternative measures designed to protect Your personal data provided for in the Data Protection Laws, as though it were an intra-EEA transfer. You are entitled to obtain a copy of these measures by making contact with us.

Protecting Your personal data

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 policies, procedures and the law.

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 defence 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 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).

How long will We keep Your personal data for?

We will keep Your personal data:

- for as long as necessary to achieve the original purpose We collected it for
- in line with relevant laws

Our normal practice is to determine whether there is/are any specific EU and/or Maltese law(s) 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 five (5) years in those cases where Our contractual relationship with You terminates or two (2) years in those cases where no such contractual relationship exists). 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/Information in question.

Keeping You updated about how We use Your personal data

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 shall be informed by us 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 Your interest to regularly check for any updates to this Privacy Policy (which are usually deemed to be effective on the date they are published on our website), in the event that our attempts to notify You of such updates do not reach You.

Use of Cookies

We use cookies to ensure the functionality of our site and to make Your website experience better. A cookie is an element of data (usually a very small file) that a website can send to Your browser, which may then store it on Your computer or mobile device. These cookies allow the Bank to correctly operate the site, provide a secure online environment, and/or to provide You with web pages or content that are tailored to You.

For further information in this regard, You are strongly encouraged to read through our Cookies Policy, available on our website.

Contacting Us or the Data Protection Authority

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.

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, and if in Malta the Information and Data Protection Commissioner's Office, Floor 2, Airways House, Triq Il-Kbira, Tas-Sliema SLM 1549, Malta, (+356) 2328 7100, idpc.info@idpc.org.mt,

Signature: _____ Date: DD/MM/YYYY

Approved and issued by APS Bank plc, APS Centre, Tower Street, B'Kara BKR 4012. APS Bank plc is regulated by the Malta Financial Services Authority as a Credit Institution under the Banking Act 1994 and to carry out Investment Services activities under the Investment Services Act 1994. The Bank is also registered as a Tied Insurance intermediary under the Insurance Distribution Act 2018. The Bank is a participant in the Depositor Compensation Scheme established under the laws of Malta.