SKYBOUND

PRIVACY POLICY & COOKIE DISCLOSURE STATEMENT

SKYBOUND WEALTH EUROPE LTD

Version: V1

Last Review: 2025

TABLE OF CONTENTS

PRIVACY POLICY & COOKIE DISCLOSURE STATEMENT

1. DEFINITIONS

Company	Refers to Skybound Wealth Europe Ltd.
Consent	The data subject gives clear, informed permission, signifying agreement to process their personal data for specified purposes. Consent must be freely given, specific, and able to be withdrawn at any time\ without affecting the lawfulness of previous processing.
Controller	Skybound Wealth Europe Ltd determines the purposes and means of processing personal data.
Cookies	Small data files are stored on a user's device and collect information on interactions with the website.
Data Breach	A security incident that results in the unauthorised access, disclosure, alteration, or destruction of personal data.
Data Subject	The individual to whom the personal data relates. This includes clients, prospective clients, employees, or any identifiable person whose data is collected and processed by the Company.
Encryption	A method of protecting personal data by converting it into an unreadable format unless decrypted using a specific key.
Policy	The Privacy Policy and Cookie Disclosure Statement of Skybound Wealth Europe Ltd.
Personal data	Any information that can identify an individual directly or indirectly. This includes names, contact information, identification numbers, financial details, and online identifiers like IP addresses. Personal Data may also cover sensitive categories, like health or demographic data, when required and collected with explicit consent. All data is handled in line with relevant data protection laws, including GDPR, to ensure privacy and security.
Processing	Any action performed on personal data, such as collecting, recording, organising, storing, retrieving, altering, using, sharing, or deleting. Processing can be manual or automated, including handling personal data to fulfil the Policy's goals.
Processor	An individual or organisation processing personal data on behalf of the controller.
Regulatory Authority	Cyprus Securities and Exchange Commission (CySEC) or other relevant authorities overseeing data protection and compliance.
Retention Period	The length of time personal data is stored by the Company to fulfil the purposes outlined in this Policy or to comply with legal obligations.
Special Categories of Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, or data concerning sexual orientation.
Third Parties	External entities not directly related to Skybound Wealth Europe Ltd but engaged in processing activities.

2. POLICY STATEMENT

Skybound Wealth Europe Ltd (the "Company", "we", "SWE" or "us") a Cyprus Investment Firm (CIF), authorised and supervised by the Cyprus Securities and Exchange Comission (CySEC) under license No. 308/16. We provide financial advice and investment services to help individuals, companies, and professional advisers meet their financial objectives. We value the privacy of our clients, business partners, and website users. We are commited to safeguarding the confidentiality of any personal information provided—whether in writen form, verbally, or via the Internet.

This document sets out the procedures for collecting, processing, and storing personal data, including general information such as contact details and financial data, and, where applicable, sensitive categories of personal data. It details the types of consent required for various data processing and communication activities and provides guidelines for data retention. Additionally, it specifies individual rights under data protection laws. It explains how personal information is handled in compliance with the law Providing for the Protection of Natural Persons concerning the Processing of Personal Data and for the Free Movement of Such Data of 2018 (Law 125(I)/2018) (as amended). This law implements Regulation (EU) 2016/679 of the European Parliament and Council (GDPR) concerning protecting natural persons concerning personal data processing and free data movement, repealing Directive 95/46/EC and relevant regulations.

If you have questions about this Privacy Policy and Cookie Disclosure Statement, please get in touch with us at:

Skybound Wealth Europe Ltd, 35 Stasikratous Street, Office 302, 1065, Nicosia, Cyprus. Email: dpo@skyboundwealth.eu

3. APPLICABILITY

This Policy applies to all personal information held by the Company. It governs its processing activities regarding the personal information of its clients and prospective clients. It does not extend to the business operations or data processing activities of external organisations or third parties for which those entities are independently responsible.

The Policy establishes the minimum standards for managing personal data and ensuring compliance with applicable privacy laws, regulations, and directives, including the EU GDPR and CySEC requirements. This Policy provides a consistent, transparent, and compliant approach to data protection and privacy within the framework of our CySEC-regulated activities.

4. POLICY

4.1. WHAT TYPE OF INFORMATION WE COLLECT

We collect various types of personal data depending on the services we provide to you. This includes but is not limited to:

- **Identity Data:** This may include a person’s first name, maiden name, last name, username or similar identifier, marital status, title, date of birth, and gender.
- **Contact Data:** billing address, delivery address, email address and telephone numbers.
- **Financial Data:** Bank account, financial records, and other transaction details.
- **Transaction Data:** Records of payments to/from you and your interactions with Skybound.
- **Technical Data:** includes internet protocol (IP) address, your login data, 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 this website.
- **Profile Data:** This can include your username and password to access our client portal, as well as your interests, preferences, feedback, and survey responses.
- **Usage Data:** Information on navigating and using our website, products, and services.
- **Marketing and Communications Data:** Your preferences regarding marketing communications and contact preferences.

We may also collect, use, and share Aggregated Data—such as statistical or demographic data—for various purposes. While Aggregated Data may be derived from your personal data, it is not considered personal data under the law, as it does not directly or indirectly reveal your identity. For instance, we may aggregate your Usage Data to understand the percentage of users accessing a particular website feature. However, if we combine or connect Aggregated Data with personal data in a way that could directly or indirectly identify you, we treat the combined data as personal data, which will then be processed per this Privacy Policy.

It is unlikely that we will need to collect any Special Categories of personal data from you. These categories include race or ethnicity, religious or philosophical beliefs, sexual orientation, political opinions, trade union membership, health information, and genetic or biometric data. We also generally do not collect information related to criminal convictions and offences. However, in limited cases, if it becomes necessary to collect such data as part of an ongoing business relationship with you, we will rely on a lawful basis—such as obtaining your explicit consent—to ensure the lawful processing of this data.

4.2. HOW WE COLLECT INFORMATION

We collect your personal data through various interactions with you, including when you:

- Enquire about our products and services via our website, contact form, or by calling our office.
- Meet with a Skybound Wealth Europe financial adviser, who may record information during client onboarding, such as in Fact-Find forms, Risk Profile Questionnaires, or Client Agreements.
- Register to receive newsleters, atend events or webinars, or engage with our marketing materials.
- Participate in calls or meetings conducted through platforms such as Teams or Zoom, which may be recorded for training, compliance, and quality assurance purposes.
- Enter into a formal business relationship with us.

Additionally, we may collect personal data from documents you provide directly to us, such as during onboarding and to fulfil anti-money laundering (AML) requirements. This may include identification documents, proof of address, and evidence of income, which we retain to meet our regulatory obligations.

If you choose not to provide certain necessary personal data, we may be unable to perform the services you request or complete our contract with you, potentially resulting in the cancellation of certain products or services.

4.3. PROTECTING YOUR INFORMATION

At Skybound Wealth Europe Ltd, safeguarding personal information is a top priority. We implement comprehensive physical, electronic, and procedural measures to secure your data's integrity, confidentiality, and availability. Our security practices meet regulatory standards and are regularly updated to respond to evolving requirements and technological advancements.

4.3.1. Security Measures and Access Controls

- **Physical Controls:** We protect data in our offices by employing physical security measures, including secure disposal of confidential waste and equipment, personal card access, locked storage cabinets, and a "clear desk" policy to ensure information is properly secured when not in use.
- **Logical Controls:** Technical security measures such as access authentication, antivirus so□ware, firewalls, malware detection, and secure backup procedures are applied across all systems where personal information is stored or processed. Personal information is contained behind secured networks and is accessible only by authorised personnel with special access rights who must maintain confidentiality. Additionally, sensitive and payment-related information is encrypted for added protection.

4.3.2. Employee Training and Awareness

We prioritise staff education on data protection, fraud prevention, and information security. All employees undergo annual training on these topics, and information security awareness is included in our new employee induction program. Employees are also trained to recognise and report any suspicious activity that may indicate financial crime or internal fraud, fulfilling our regulatory and legal obligations.

4.3.3. Data Breach Response

In the event of a data breach that poses a high risk to the rights and freedoms of our clients, business partners, or employees, we will notify affected individuals without undue delay. This proactive approach is designed to mitigate risks and ensure transparency.

4.3.4. Note on Internet Security

While we employ advanced technical and organisational safeguards to protect your information, it is important to recognise that data transfer over the Internet is not completely secure. We encourage clients to exercise caution and contact us directly with security concerns.

4.4. LEGAL BASIS FOR PROCESSING YOUR DATA

We process your personal data based on the following legal grounds:

- **Contractual Obligation:** We process your identity, contact, financial, and transaction data to establish and fulfil our contractual obligations with you, including providing our financial services, administering your account, and complying with terms set out in client agreements. This processing is essential to deliver the products and services you have requested.
- **Legitimate Interest:** We process certain data to support our legitimate business interests, which include improving website functionality, personalising user experiences, and conducting service quality assessments. Our legitimate interest also extends to analysing usage data to beter understand client needs and enhance service offerings, provided these actions do not infringe on your privacy rights.
- **Legal Obligation:** As a regulated entity, we must process personal data to comply with various regulatory obligations, such as anti-money laundering (AML), counter-terrorism financing (CTF), tax reporting, and fraud prevention. This may also include data sharing with regulatory bodies or authorities when mandated by law.
- **Consent:** In cases where the bases above do not cover processing, we may request your consent. This includes instances where we may seek to process special categories of personal data (e.g., health or biometric data) or to use your data for certain marketing activities. You may withdraw your consent anytime, impacting our ability to provide specific services.

If further legal grounds are relevant to specific data processing activities, we will communicate them and provide transparency on how your data is used.

4.5. HOW WE USE YOUR PERSONAL INFORMATION

We use your personal information for the following purposes:

- Provision of Services and Account Management
  - Fulfil your requests for information, products, and services.
  - Complete transactions and manage your Skybound account and interactions.
  - Provide effective services per our regulatory obligations.
  - Meet our legal obligations and comply with regulatory requirements.

- Service Improvement
  - Enhance website functionality to deliver a personalised and effective user experience.
  - Perform internal business administration and operations, including troubleshooting, data analysis, research, and testing.
  - Notify you about service changes and keep our website secure and safe.
- Direct Marketing
  - Provide information about related services and products similar to those you have shown interest in or requested.
  - Send newsleters and other marketing communications. If you prefer not to receive marketing messages, please get in touch with us.

For existing clients, we rely on our legitimate interests as the lawful basis for direct marketing, ensuring that such communications align with your preferences and are delivered via the methods we typically use to communicate with you (e.g., email). We assess and balance our legitimate interests with your privacy rights, and we do not use your data for activities where your rights would override our interests.

If you would like more information about how we balance legitimate interests against potential impacts on your privacy, please contact us.

4.5.1. Change of Purpose

We will only use your personal data for the purposes for which it was originally collected unless we reasonably determine that it needs to be used for another purpose compatible with the original intent. Should we need to use your data for an unrelated purpose, we will notify you and explain the legal basis. If you would like more information on the potential use of your data for a new purpose, please contact us.

4.5.2. Automated Decision-Making

We generally do not use automated decision-making processes that significantly affect you. However, there are limited instances where automated processes are applied, such as our investment risk profiling tool and specific regulatory requirements for anti-money laundering (AML) compliance.

- **Investment Risk Profiling:** Automated systems may help us generate suitable investment options tailored to your risk profile and financial circumstances. These options are intended as recommendations, and any final decisions will be made in collaboration with your financial adviser.
- **AML Compliance:** We use automated systems as part of our AML regulatory obligations. However, this is solely for compliance and does not impact your services.

Decisions on how your data is processed are typically based on your instructions, our contractual agreements with you, and our legal and regulatory obligations. In all cases, automated processes are used with professional oversight and critical decisions are made with human involvement, ensuring they are not solely “automated” in nature.

Please note that certain third parties may use automated decision-making tools or software. While we are not responsible for other entities’ privacy practices, we will take reasonable steps to inform you of any automated third-party decisions that could affect you. We encourage you to review the privacy practices of any third parties you engage with.

4.6. HOW LONG WE HOLD YOUR DATA

We retain your personal data only for as long as is necessary to fulfil the purposes for which it was collected, as outlined in this Privacy Policy, or as required to meet our legal, regulatory, or business obligations.

Retention periods are determined based on the data’s type, nature, sensitivity, and potential risk of harm from unauthorised use or disclosure. We also consider applicable legal requirements and whether the purposes for processing can be achieved by other means.

Generally, we retain personal data for a minimum of five years after the end of our client relationship in compliance with legal and regulatory obligations. However, data may be held longer where necessary to:

- Comply with additional legal or regulatory requirements.
- Fulfill obligations related to tax, social security, pension management, or other legitimate business needs.
- Protect your vital interests or those of another natural person.

Once the relevant retention period has expired, we ensure that your data is securely deleted or anonymised under GDPR and regulatory standards. You can contact us anytime for specific details about our data retention practices.

4.7. YOUR DATA PROTECTION RIGHTS

Under data protection law, you have the following rights regarding the personal data we hold about you:

- **Right to Access:** You can request access to your personal data and obtain a copy of the information we hold about you free of charge. If your request is manifestly unfounded or excessive, particularly repetitive, we may charge a reasonable fee or refuse to act.
- **Right to Rectification:** If you believe that any personal data we hold about you is inaccurate or incomplete, you have the right to request that we correct or complete that information. We will take reasonable steps to verify and make corrections as necessary.

- **Right to Erasure (Right to be Forgoten):** You may request the deletion of your personal data when it is no longer necessary for the purpose for which it was collected or if you have withdrawn your consent (where consent was required). However, please note that there are certain exceptions where we are legally obligated to retain your data, such as for regulatory compliance or to defend legal claims.
- **Right to Restriction of Processing:** In certain situations, you have the right to request that we restrict the processing of your personal data, for example, if you contest the accuracy of the data or if the processing is unlawful but you oppose erasure.
- **Right to Data Portability:** Where technically feasible, you can request that we provide your personal data in a structured, commonly used, and machine-readable format and/or transfer this data to another entity directly. This right applies where processing is based on your consent or the performance of a contract and is carried out by automated means.
- **Right to Object:** You have the right to object to processing your personal data, and we rely on legitimate interests as the legal basis for processing. You can also object to using your data for direct marketing purposes at any time.
- **Right to Withdraw Consent:** If we rely on your consent to process your personal data, you can withdraw that consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.
- **Right to Lodge a Complaint:** If you believe we have not complied with data protection laws, you have the right to lodge a complaint with the relevant data protection authority, which in our case is the Office of the Commissioner for Personal Data Protection in Cyprus, or the appropriate supervisory authority within the EU.

To exercise your rights, please contact us using the details in this notice. We will respond to your request as quickly as possible and within the timeframes required by law.

4.8. INFORMATION SHARING WITH THIRD PARTIES

Skybound Wealth Europe Ltd does not share your personal data with third parties for marketing purposes. You do not need to request that we refrain from sharing your information for such purposes.

We may, however, share the information we collect about you with certain third parties as permited or required by law to support the delivery of our services. This includes:

- **Product and Service Providers:** To provide and manage financial products or services, we may share your data with third-party providers such as fund managers, insurers, insurance brokers, and credit brokers. These providers use your information solely to fulfil contractual obligations related to your accounts and investments.
- **Operational Service Providers:** We engage with third-party service providers who support various business functions, including customer service, account administration, marketing (on our behalf), online support, and research. We disclose only the necessary information required for these providers to deliver their services, and we maintain contracts requiring them to keep your information secure and to prohibit any use for their own marketing purposes.
- **Other Skybound Entities:** When necessary, we may share information within the Skybound Wealth Management Group to ensure that our services and recommendations align with your complete financial picture, allowing us to provide consistent and coordinated advice.
- **Fraud Prevention and Security:** We may disclose information to protect against potential or actual fraud, unauthorised transactions, claims, or other liabilities.
- **Regulatory Compliance:** To comply with legal obligations, we may share your data with government agencies, regulatory authorities, law enforcement officials, and internal or external auditors.

We work closely with product and service providers to bring you a broad range of wealth management solutions. When you inquire about or invest in one of these offerings, the relevant third-party provider may use your information to fulfil their contractual duties. These providers may also share necessary data with us, which we handle in line with this Privacy Policy.

In the event of a sale, restructuring, or reorganisation of our business or assets, we may transfer your personal information as part of that process. In such cases, we will maintain your privacy rights and inform you if this affects your data.

All third-party providers and entities with whom we share your information are contractually required to maintain the confidentiality and security of your data per applicable law.

4.9. TRANSFERRING PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

There may be instances where we need to transfer personal data provided to us to countries outside the European Economic Area (EEA), which includes EU member countries as well as Iceland, Liechtenstein, and Norway. Such transfers, known as "third-country transfers," may be necessary when engaging providers or partners outside the EEA.

If a transfer outside the EEA is required, Skybound Wealth Europe will implement measures to ensure that individuals' data privacy rights are maintained in line with our obligations under GDPR and other applicable regulations. Specifically:

- **Adequate Safeguards:** When transferring data to a third country that the European Commission has not deemed to provide an adequate level of data protection, we will ensure appropriate safeguards are in place. These may include Standard Contractual Clauses (SCCs) or equivalent mechanisms that provide enforceable rights for individuals.
- **Explicit Consent:** In cases where adequate safeguards cannot be guaranteed, we seek explicit consent from the data subject before the transfer. We will provide full information regarding the reason for the transfer, the associated risks, and the individual's right to withdraw consent at any time.

For data transfers to the United States, we will only engage providers certified under an EU-approved mechanism, such as the EU-US Data Privacy Framework, which ensures similar protections to those required by GDPR.

Our compliance team regularly reviews and monitors these arrangements to ensure they continue to meet regulatory standards. For additional information on international transfers, refer to the European Commission's resources on third-country data protection safeguards.

4.10. COOKIES AND WEBSITE USAGE

As part of our commitment to enhancing user experience and optimising website performance, Skybound Wealth Europe Ltd uses cookies on our website. Cookies are small text files stored on users' devices that collect information about site interactions, including pages visited, session duration, and navigation behaviour. This data allows us to analyse usage paterns, identify areas for improvement, and tailor site functionality to meet user needs.

For operational transparency, the following cookie guidelines apply:

- Strictly Necessary Cookies: Essential for core website functionality and session management.
- Performance and Analytics Cookies: These compile statistical reports, track visitor interactions, and inform site improvements.
- Cookie Users can manage cookie settngs directly through their browser preferences, and further instructions on cookie management are available at www.allaboutcookies.org. However, disabling certain cookies may limit website functionality.

Non-essential cookies will expire within their specified timeframe and, in all instances, no later than 12 months aer use for the purpose they were initially set. For further guidance, refer to our Privacy Policy and Cookie Disclosure Statement or contact the compliance team directly.

4.11. TIME LIMIT TO RESPOND TO DATA REQUESTS

Skybound Wealth Europe aims to respond to all legitimate data-related requests, such as data access or correction requests, within one month. We may extend this response period by up to two additional months for complex requests or multiple concurrent requests. Should an extension be necessary, the requestor will be notified within the initial one-month timeframe, including an explanation for the delay.

4.12. SUPERVISORY AUTHORITY AND HANDLING COMPLAINTS

Skybound Wealth Europe Ltd takes privacy concerns seriously. If an individual is dissatisfied with how their data is processed, they may file a complaint with the Office of the Commissioner for Personal Data Protection:

Address: Kypranoros 15, Nicosia 1061, Cyprus

Postal Address: P.O. Box 23378, 1682 Nicosia, Cyprus

Telephone: +357 22818456

Fax: +357 22304565

Email: commissioner@dataprotection.gov.cy

Website: htp://www.dataprotection.gov.cy

However, Skybound Wealth Europe Ltd encourages individuals to contact us directly first. We are commited to resolving any privacy concerns quickly and to the satisfaction of the individuals involved, as the protection and integrity of their data are of utmost importance.

5. ROLES AND RESPONSIBILITIES

5.1. BOARD OF DIRECTORS

The Board of Directors ensures that the Company maintains a robust data protection and compliance framework. This includes oversight of privacy practices and delegating specific responsibilities to relevant commitees or individuals while retaining ultimate accountability for adherence to this Policy.

5.2. REGIONAL HEAD OF COMPLIANCE: EUROPE

The Regional Head of Compliance: Europe owns, maintains, and periodically reviews this Policy to ensure it aligns with applicable laws, regulations, and best practices. The Regional Head is also tasked with:

- Ensuring effective implementation of this Policy across all business units.
- Providing guidance and oversight to employees and managers on data protection maters.
- Leading investigations into data breaches and ensuring appropriate remediation and reporting.

5.3. DATA PROTECTION OFFICER (DPO)

The DPO is critical in ensuring compliance with GDPR and other applicable data protection regulations.

Key responsibilities include:

- Monitoring compliance with this Policy and data protection laws.
- Providing advice on data protection impact assessments (DPIAs).
- Acting as the primary contact point for supervisory authorities and individuals regarding privacy concerns or complaints.
- Delivering training and awareness initiatives to promote a data protection culture within the Company.

5.4. MANAGERS AND LINE SUPERVISORS

Managers are responsible for:

- Ensuring their teams understand and comply with this Policy.
- Supporting employees in implementing data protection measures relevant to their roles.
- Reporting potential or actual data breaches promptly to the Compliance Team or DPO.
- Ensuring employees complete required training on privacy and data protection.

5.5. EMPLOYEES AND ASSOCIATED PERSONS

All employees and associated persons must:

- Familiarise themselves with this Policy and adhere to its requirements.
- Safeguard personal data they handle as part of their roles.
- Report any suspected or actual data breaches, security incidents, or non-compliance issues to the DPO or Compliance Team.
- Participate in training sessions to stay updated on data protection obligations.
- Ensure the accuracy and integrity of personal data processed in their areas of responsibility.

5.6. THIRD-PARTY SERVICE PROVIDERS

Third-party service providers processing personal data on behalf of Skybound Wealth Europe must:

- Comply with the terms of this Policy and any applicable data protection agreements.
- Implement appropriate technical and organisational measures to protect personal data.
- Notify the Company promptly of any data breaches or incidents impacting personal data.

6. DISCIPLINARY ACTION

Skybound Wealth Europe Ltd is commited to ensuring compliance with this Privacy Policy and applicable data protection regulations, including GDPR. Any breach of this Policy, whether intentional or due to negligence, is considered a serious mater that may result in disciplinary action.

Adherence to this Policy is mandatory for all employees. Failure to comply with the requirements outlined in this Policy may lead to disciplinary action. The Company expects all employees to act with integrity and align with the firm's values and regulatory obligations. Employees are encouraged to seek guidance from their manager or the compliance team if uncertain about any aspect of this Policy.

7. POLICY REVIEW

The Privacy Policy is reviewed every two years to ensure its effectiveness, relevance, and alignment with applicable laws, regulations, and best practices. The Regional Head of Compliance: Europe leads the formal review in collaboration with the Group Head of Compliance, assessing the Policy's effectiveness in handling complaints and its adherence to the evolving regulatory environment across European jurisdictions. The Regional Head of Compliance: Europe is responsible for maintaining the Policy and ensuring it remains effective and compliant with local regulatory requirements. The Board must approve any interim changes upon the recommendation of the Regional Head of Compliance: Europe.

We may also update this Privacy Policy periodically to reflect changes in our information practices, regulatory requirements, or technological advancements. Updates will be posted on our website, and we encourage you to review the Privacy Policy regularly to stay informed about how we protect your information and rights. If material changes significantly impact your privacy, we will provide additional notice, where possible, before the changes take effect. By continuing to use our website after an updated Privacy Policy is posted, you acknowledge and agree to the changes. If you disagree with any updates, you should discontinue using the website.

8. OWNERSHIP

The Board of Directors owns this Policy. The Regional Head of Compliance: Europe will coordinate the drafting and review of the Policy as mandated by the Board.

9. APPROVAL

The Regional Head of Compliance: Europe recommends the Policy and the Board of Directors approve it.

10. REVISION HISTORY

Version #	Revision Purpose	Effective Date	Next Review Date	Summary of Critical Revisions
V.1	New Policy	March 2025	March 2027	N/A. New Policy