PRIVACY POLICY

No	Date	Author	Change Description
001	November 2018	Sven Büchel	N/A
002	May 2020	Sven Büchel	update contact details
003	October 2021	Sven Büchel	Update License Number
004	October 2025	Sven Büchel	Complete new wording with enhanced MFSA/FIAU compliance

Privacy Policy

Van Sterling Capital Ltd.

MFSA Licence Number: VANS-IF-9616
Effective Date: October 1, 2025

Last updated: October 1, 2025

1. Introduction

Van Sterling Capital Ltd. ("Van Sterling", "we", "our", or "us") is committed to safeguarding the privacy and integrity of personal data entrusted to us by our clients and business partners. As a regulated investment firm licensed by the Malta Financial Services Authority (MFSA) under licence number VANS-IF-9616, we operate strictly in accordance with the requirements of the General Data Protection Regulation (EU) 2016/679 (GDPR), the Maltese Data Protection Act (Chapter 586 of the Laws of Malta), and all related financial services legislation applicable under MiFID II and MiFIR.

This Privacy Policy sets out in detail how we collect, process, store, and protect personal data in the course of providing our regulated investment services. It also explains your rights as a data subject and the measures we have taken to ensure the resilience and integrity of our information systems in line with the Digital Operational Resilience Act (DORA).

We recognise that privacy and trust are fundamental to a sustainable client relationship. For this reason, we handle all personal data with the highest standards of transparency, proportionality, and accountability.

2. Data Controller

Van Sterling Capital Ltd., incorporated under the laws of Malta with its registered office at Van Sterling Capital Ltd., Nu Bis Centre, Mosta Road, LJA 9012 Lija, Malta, acts as the Data Controller in relation to all processing activities covered by this policy.

Data Protection Officer Contact Details:

- **Email:** gdpr@vansterling.com
- **Postal Address:** Van Sterling Capital Ltd., Nu Bis Centre, Mosta Road, LJA 9012 Lija, Malta
- **Telephone:** +356 27 289615

The Data Protection Officer is responsible for monitoring compliance with this policy, handling data subject requests, and serving as the point of contact with the Office of the Information and Data Protection Commissioner (IDPC).

3. Categories of Personal Data Processed

In the course of delivering our investment services, we process several categories of personal data relating to our clients, their representatives, and in some cases beneficial owners.

3.1 Identification and Contact Information

This includes names, dates and places of birth, nationality, gender, residential and correspondence addresses, telephone numbers, email addresses, and copies of identification documents (passports, identity cards, driving licences). This information is obtained directly from clients when they apply for our services and is essential for verifying their identity and maintaining accurate records.

3.2 Financial and Professional Information

This comprises data such as occupation, employer, employment status, tax residency, tax identification numbers (TINs), national insurance or social security numbers, and detailed source of funds and source of wealth documentation. In line with anti-money laundering (AML) requirements, we collect supporting evidence including bank statements, payslips, contracts of employment, property deeds, inheritance documentation, and business ownership records where relevant. Bank account details, IBAN numbers, payment information, and transaction records are also required to facilitate investment transactions, deposits, and withdrawals.

3.3 Investment Profile and Suitability Information

Under MiFID II suitability requirements, we collect information about your knowledge and experience in the investment field, your financial situation (including details of income, regular financial commitments, assets and liabilities, and capacity to bear losses), investment objectives (including risk tolerance, investment horizon, and specific preferences), and ESG/sustainability preferences where applicable. This information is necessary to ensure that investment services and products are suitable for you.

3.4 Regulatory and Compliance Data

This includes documentation and outputs generated during our know-your-customer (KYC) and AML checks, results from sanctions lists screening, politically exposed persons (PEP) status verification, adverse media screenings, enhanced due diligence assessments, ongoing monitoring alerts, and other due diligence sources. We also retain records of customer risk assessments and classification as retail, professional, or eligible counterparty clients.

3.5 Transaction and Account Data

This refers to orders submitted by clients, records of order execution, portfolio information, full transactional history, investment performance records, valuation reports, and all related documentation. This category also encompasses communications that relate directly to transactions, including instructions received via email, recorded telephone conversations, instant messages, and meeting notes.

3.6 Recording of Communications

In accordance with MiFID II requirements (Article 16(7) of MiFID II Directive), we record telephone conversations and electronic communications that relate to transactions or the provision of investment services. These recordings are maintained regardless of whether the communications lead to the conclusion of a transaction. Recordings include telephone calls, voice messages, instant messaging, emails, and other electronic communications involving our employees when dealing or intending to deal on behalf of clients.

3.7 Technical Information

This is generated when clients access our systems and platforms, including internet protocol (IP) addresses, browser characteristics, device identifiers, operating system information, login times, access logs, session duration, and pages accessed. Such information is used primarily for system security, fraud detection, operational monitoring, and ensuring the integrity of our services.

3.8 Special Categories of Personal Data

We do not intentionally collect sensitive personal data (special categories of data under Article 9 GDPR, such as health, biometric information, racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, or data concerning sex life or sexual orientation). Where such data is exceptionally required for enhanced due diligence purposes, it will be processed lawfully with explicit safeguards and, where applicable, your explicit consent. If you provide such data to us voluntarily, we will process it only where legally permitted and with appropriate protections.

4. Legal Basis for Processing

The processing of personal data by Van Sterling is always underpinned by a lawful basis as required by Article 6 of the GDPR.

4.1 Performance of a Contract (Article 6(1)(b) GDPR)

Most commonly, processing is necessary for the performance of a contract to which you are party. This includes activities such as opening accounts, providing portfolio management services, executing client orders, processing transactions, and delivering investment advice. Without this data, we would not be able to deliver our contractual obligations.

4.2 Legal Obligation (Article 6(1)(c) GDPR)

We process personal data where necessary to comply with legal obligations imposed on us as a licensed investment firm. This includes obligations under:

- MiFID II and MiFIR requirements (transaction reporting, record-keeping, best execution reporting)
- The Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR)
- The Investment Services Act (Chapter 370 of the Laws of Malta)
- Tax reporting frameworks (Common Reporting Standard, FATCA, DAC6)
- Supervisory requirements of the MFSA, FIAU, and other competent authorities
- Court orders, regulatory investigations, and lawful requests from law enforcement

4.3 Legitimate Interests (Article 6(1)(f) GDPR)

In certain cases, we process personal data on the basis of our legitimate interests. These legitimate interests include:

- Ensuring the security and resilience of our ICT systems and preventing unauthorised access
- Preventing fraud, money laundering, terrorist financing, and other financial crime
- Maintaining accurate business records and audit trails
- Improving the efficiency and quality of our client services

- Managing our business operations and internal administrative purposes
- Exercising or defending legal claims

When processing on this basis, we always conduct a balancing test to ensure that our interests are balanced against your fundamental rights and freedoms. You have the right to object to processing based on legitimate interests.

4.4 Consent (Article 6(1)(a) GDPR)

Where processing is based on consent, such as for the sending of marketing communications, newsletters, or processing special categories of personal data, we will request explicit, informed consent from you and provide the right to withdraw that consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.

5. Purposes of Processing

Personal data is used by Van Sterling for several defined purposes that are closely linked to our regulatory obligations and service delivery.

5.1 Client Onboarding and Due Diligence

To conduct KYC checks, verify identity, assess source of funds and wealth, comply with AML and counter-terrorist financing laws, screen against sanctions lists, assess PEP status, and conduct ongoing customer due diligence.

5.2 Provision of Investment Services

To receive and transmit orders, execute trades on behalf of clients, provide investment advice, manage client portfolios, conduct suitability and appropriateness assessments, deliver discretionary portfolio management services, provide custody services, and ensure best execution in line with MiFID II requirements.

5.3 Regulatory Reporting and Compliance

To provide transaction reports to competent authorities, prepare and submit periodic statements, comply with regulatory disclosures, report suspicious transactions to the FIAU, fulfil tax reporting obligations (CRS, FATCA), and respond to regulatory enquiries and audits.

5.4 Client Communications and Service Management

To manage client communications relating to service provision, contract changes, regulatory updates, fee schedules, portfolio performance, market developments, and responses to queries. To send statements, confirmations, disclosures, and other service-related documents.

5.5 Risk Management and Security

To manage operational risk, detect and prevent fraud, monitor for suspicious transactions, maintain cybersecurity defences, conduct incident detection and response, ensure business continuity, and protect the security of our ICT systems in accordance with DORA requirements.

5.6 Legal and Accounting Obligations

To comply with statutory obligations in accounting, financial reporting, auditing, tax compliance, and to cooperate with regulators, tax authorities, law enforcement agencies, and courts when legally required.

5.7 Improvement and Development of Services

To analyse service usage, improve client experience, develop new products and services, and conduct market research, always in accordance with applicable data protection principles.

6. Data Sharing and Use of Third Parties

Van Sterling makes use of carefully selected third-party service providers in order to deliver efficient and compliant services. All such providers are bound by contractual arrangements that include data protection clauses aligned with GDPR requirements, including provisions for data processor obligations under Article 28 GDPR.

6.1 ICT Infrastructure Providers

Our ICT infrastructure is hosted by **Hetzner** and **Hosteurope**, both EU-based providers offering secure, GDPR-compliant cloud services. These partners ensure redundancy, availability, and resilience of our systems, and their performance is monitored as part of our DORA framework.

6.2 Client Relationship Management

Client relationship management is supported through **HubSpot**, hosted within the European Union, and **Teamleader**, based in Belgium. These platforms assist in managing client communications, service workflows, compliance records, and operational efficiency.

6.3 Electronic Signature Services

For digital signatures, we use **YouSign**, a provider established in France and compliant with the EU eIDAS Regulation for advanced electronic signatures, ensuring the legal validity and security of electronically signed documents.

6.4 KYC and AML Service Providers

For KYC and AML obligations, we rely on **Shufti Pro** for document verification, identity authentication, and biometric checks, and **Muinmos** for automated client onboarding, suitability assessments, and client classification in line with MiFID II rules.

6.5 Financial Institutions and Payment Processors

Where necessary, we share client data with payment institutions, banking partners, investment platforms, custodians, and other financial intermediaries within the EU to facilitate the settlement of transactions, custody of assets, and related financial flows.

6.6 Professional Advisors

We may share data with lawyers, auditors, tax advisors, compliance consultants, and other professional advisors where necessary for the provision of their services to us.

6.7 Regulators and Public Authorities

We disclose data to regulators such as the MFSA, FIAU, IDPC, tax authorities (including foreign tax authorities under international agreements), the Malta Police Force, financial intelligence units, courts, and other competent authorities when required by law or in response to lawful requests.

6.8 Group Companies

Where applicable, personal data may be shared with other entities within our corporate group for administrative purposes, subject to appropriate safeguards and data protection agreements.

6.9 No Sale of Personal Data

Van Sterling does not sell or make personal data available to unrelated third parties for independent commercial purposes. We do not engage in profiling for marketing purposes or share data with data brokers.

7. International Data Transfers

In some cases, personal data may be transferred outside the European Economic Area (EEA). When this occurs, we ensure that appropriate safeguards are in place, consistent with Chapter V of the GDPR.

7.1 Adequacy Decisions

Transfers may be made to jurisdictions that are subject to an adequacy decision by the European Commission pursuant to Article 45 GDPR, ensuring that they provide an equivalent level of data protection to that within the EEA.

7.2 Standard Contractual Clauses

Where no adequacy decision exists, we rely on Standard Contractual Clauses (SCCs) as approved by the European Commission pursuant to Article 46(2)(c) GDPR. These clauses provide appropriate safeguards for the transfer of personal data.

7.3 Transfer Impact Assessments

We conduct transfer impact assessments (TIAs) to evaluate the legal framework of the destination country, considering factors such as access by public authorities, availability of effective remedies, and the

rule of law. Where required, we implement supplementary measures such as encryption, pseudonymisation, strict access controls, and contractual commitments.

7.4 Derogations

In exceptional circumstances, transfers may be based on derogations under Article 49 GDPR, such as where the transfer is necessary for the performance of a contract with you, for important reasons of public interest, or where you have explicitly consented to the transfer after being informed of the possible risks.

8. Data Retention

Van Sterling retains personal data only for as long as it is necessary to fulfil the purposes for which it was collected, or to comply with legal and regulatory obligations.

8.1 Client Relationship Data

Identification documents, KYC records, and due diligence documentation are retained for a minimum period of **five years** following the termination of the business relationship, in line with AML requirements under the PMLFTR and FIAU guidance.

8.2 Transaction Records

Transaction records, order records, and related documentation are retained for at least **five years** after the execution of the transaction, in accordance with MiFID II requirements (Article 16(6) MiFID II Directive).

8.3 Recorded Communications

Telephone recordings and electronic communications relating to transactions are retained for a period of **five years**, extendable to seven years upon request by the MFSA, in accordance with MiFID II requirements (Article 16(7) MiFID II Directive).

8.4 Suitability Assessments

Suitability reports and related documentation are retained for a minimum of **five years** from the date of preparation or last update, as required under MiFID II conduct of business rules.

8.5 Accounting and Tax Records

Accounting records, financial statements, tax records, and audit documentation are retained for a period of **ten years** as required by Maltese and EU law, including the Companies Act and tax legislation.

8.6 Complaint Records

Records of complaints, including MiFID II complaints, are retained for a period of **five years** from the date of resolution to enable regulatory oversight and dispute resolution.

8.7 Secure Deletion

At the end of the retention period, personal data is securely deleted, destroyed, or anonymised to ensure that it can no longer be linked to identifiable individuals. We maintain records of data deletion activities as part of our accountability obligations.

9. Data Security and DORA Compliance

We recognise that the security of personal data is integral to client trust and regulatory compliance. To this end, Van Sterling has implemented robust technical and organisational measures designed to protect personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage.

9.1 Technical Security Measures

These include:

- End-to-end encryption for data in transit and at rest
- Multi-factor authentication for system access
- Firewalls and intrusion detection/prevention systems
- Regular security patching and updates
- Secure backup and disaster recovery procedures
- Network segmentation and access controls
- Monitoring and logging of system activities

9.2 Organisational Security Measures

These include:

- Strict access controls based on the principle of least privilege and need-to-know
- Role-based access management
- Confidentiality agreements for all staff and contractors
- Regular staff training on data protection and information security
- Clear policies and procedures for data handling
- Incident response and breach notification procedures
- Regular risk assessments and audits

9.3 ICT Risk Management and DORA Compliance

Our ICT infrastructure is managed in line with the **Digital Operational Resilience Act (DORA)**. We maintain a comprehensive ICT risk management framework, including:

- Documented ICT risk assessments
- Incident detection, logging, and response procedures
- Business continuity and disaster recovery plans
- Regular testing of backup and recovery procedures
- Third-party ICT service provider oversight
- ICT-related incident reporting to the MFSA where required

9.4 Vulnerability Management

We conduct regular penetration testing, vulnerability assessments, and security audits to evaluate the resilience of our systems and identify potential weaknesses. Remediation actions are prioritised based on risk.

9.5 Third-Party Oversight

Third-party service providers are subject to ongoing due diligence, contractual arrangements requiring them to maintain standards of operational resilience and data security equivalent to those imposed on Van Sterling, and periodic audits or assessments.

9.6 Data Breach Response

In the event of a personal data breach, Van Sterling will follow established incident response procedures. Where a breach is likely to result in a risk to the rights and freedoms of individuals, we will notify the Office of the Information and Data Protection Commissioner (IDPC) without undue delay and where feasible within **72 hours** of becoming aware of the breach, in accordance with Article 33 GDPR. Where the breach is likely to result in a high risk, we will also notify affected clients without undue delay, in accordance with Article 34 GDPR, providing information about the nature of the breach, its likely consequences, and the measures taken or proposed to address it.

10. Rights of Data Subjects

As a client of Van Sterling, you enjoy a series of rights under the GDPR. These rights are fundamental to ensuring transparency and accountability in the processing of personal data.

10.1 Right of Access (Article 15 GDPR)

You have the right to request confirmation as to whether we process your personal data and, if so, obtain access to that data and detailed information about its processing, including the categories of data, purposes of processing, recipients, retention periods, and your rights.

10.2 Right to Rectification (Article 16 GDPR)

You have the right to request the correction of inaccurate or incomplete personal data to ensure the information we hold is accurate and up to date.

10.3 Right to Erasure ('Right to be Forgotten') (Article 17 GDPR)

You may request the erasure of your personal data in circumstances where:

- It is no longer necessary for the purposes for which it was collected
- You have withdrawn consent and there is no other legal basis
- You object to processing based on legitimate interests and there are no overriding legitimate grounds
- The processing is unlawful
- Erasure is required to comply with a legal obligation

Please note that this right is not absolute and we may be required to retain certain data to comply with legal obligations, particularly under MiFID II record-keeping requirements and AML regulations.

10.4 Right to Restriction of Processing (Article 18 GDPR)

You may request that we restrict the processing of your personal data in certain situations:

- If you contest the accuracy of the data, for a period enabling us to verify accuracy
- If the processing is unlawful but you prefer restriction over erasure
- If we no longer need the data but you require it for legal claims
- If you have objected to processing pending verification of whether our legitimate grounds override yours

10.5 Right to Data Portability (Article 20 GDPR)

Where processing is based on consent or contract and carried out by automated means, you have the right to receive your personal data in a structured, commonly used, and machine-readable format (such as CSV, JSON, or XML), and to transmit that data to another controller.

10.6 Right to Object (Article 21 GDPR)

You have the right to object to the processing of your personal data where it is based on legitimate interests, including for profiling related to those interests. We will cease processing unless we can demonstrate compelling legitimate grounds that override your interests, rights, and freedoms, or for the establishment, exercise, or defence of legal claims.

You have an absolute right to object to processing for direct marketing purposes at any time.

10.7 Right to Withdraw Consent (Article 7(3) GDPR)

Where processing is based on consent, you have the right to withdraw your consent at any time without affecting the lawfulness of processing based on consent before its withdrawal. You can withdraw consent by contacting us using the details below.

10.8 Exercising Your Rights

All requests may be submitted to **gdpr@vansterling.com** or by post to our registered address. We will respond within **one month** of receipt, or within **two additional months** where requests are complex or numerous. We will inform you if an extension is necessary.

We may request additional information to verify your identity before processing your request, to ensure personal data is disclosed only to the data subject or their authorised representative.

There is no charge for exercising your rights unless requests are manifestly unfounded or excessive, in which case we may charge a reasonable administrative fee or refuse to act on the request.

11. Automated Decision-Making and Profiling

Van Sterling does not engage in automated decision-making, including profiling, that produces legal effects concerning clients or similarly significantly affects them, without human intervention.

Where we use automated processing for risk assessment, suitability analysis, or fraud detection purposes, such processing is subject to appropriate safeguards including regular review by qualified staff, the opportunity for you to express your point of view, and the ability to contest decisions.

Should our practices change to include automated decision-making with legal or similarly significant effects, we will:

- Provide clear notice in advance
- Explain the logic involved and the significance and envisaged consequences of such processing
- Obtain explicit consent where required
- Implement suitable measures to safeguard your rights and freedoms
- Provide the right to human intervention, to express your point of view, and to contest the decision

12. Data Protection Impact Assessments

Where we undertake processing activities that are likely to result in a high risk to your rights and freedoms, particularly when using new technologies, we conduct a Data Protection Impact Assessment (DPIA) in accordance with Article 35 GDPR. This assessment evaluates the necessity and proportionality of the processing, the risks to data subjects, and the measures in place to mitigate those risks.

Where appropriate, we consult with the IDPC prior to processing, as required under Article 36 GDPR.

13. Cookies and Website Technologies

Our website uses cookies and similar technologies to enhance user experience, analyse website usage, and improve our services. Detailed information about the cookies we use, their purposes, and your choices regarding cookies is available in our separate **Cookie Policy**.

You can manage cookie preferences through your browser settings, though please note that disabling certain cookies may affect the functionality of our website.

14. Marketing Communications

We may send you marketing communications about our services, investment opportunities, market insights, and events where you have consented to receive such communications or where we have another lawful basis.

You have the right to opt out of receiving marketing communications at any time by:

- Clicking the 'unsubscribe' link in any marketing email
- Contacting us at gdpr@vansterling.com
- Writing to our registered address

Please note that even if you opt out of marketing communications, we will still send you service-related communications that are necessary for the performance of our contract with you or to comply with legal obligations.

15. Changes to the Privacy Policy

We reserve the right to amend or update this Privacy Policy from time to time to reflect changes in law, regulation, technology, or our internal practices. Any changes will be notified to clients through our website and, where material changes affect your rights, through direct communication.

The most recent version will always be available upon request and at www.smarter-investments.com, www.vansterling.com and www.intokia.com and will display the date of the last update. We encourage you to review this policy periodically.

Your continued use of our services after such modifications constitutes your acknowledgment of the modified Privacy Policy and agreement to abide by it.

16. Complaints and Supervisory Authority

16.1 Internal Complaints

If you have concerns about the processing of your personal data, you may contact us directly at:

- **Email:** gdpr@vansterling.com
- **Postal Address:** Van Sterling Capital Ltd., Data Protection Officer, Nu Bis Centre, Mosta Road, LJA 9012 Lija, Malta

We will investigate your concern and respond within a reasonable timeframe.

16.2 Supervisory Authority

If you are not satisfied with our response, or wish to raise a concern directly with a supervisory authority, you have the right to lodge a complaint with:

Office of the Information and Data Protection Commissioner (IDPC)

- Address: 2, Airways House, Second Floor, High Street, Sliema SLM 1549, Malta
- Email: idpc.info@idpc.org.mt
- Telephone: +356 2328 7100
- Website: https://idpc.org.mt

You may also lodge a complaint with the supervisory authority in your country of residence, place of work, or place of alleged infringement if you are located outside Malta.

17. Legal Framework and Definitions

17.1 Applicable Legal Framework

This Privacy Policy and our data processing activities are governed by:

- Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR)
- Data Protection Act (Chapter 586 of the Laws of Malta)
- Investment Services Act (Chapter 370 of the Laws of Malta)
- Prevention of Money Laundering Act (Chapter 373 of the Laws of Malta)
- Prevention of Money Laundering and Funding of Terrorism Regulations (S.L. 373.01)
- MiFID II Directive (2014/65/EU) and MiFIR Regulation (EU) No 600/2014
- Digital Operational Resilience Act (DORA) (Regulation (EU) 2022/2554)
- Other applicable EU and Maltese laws and regulations

17.2 Key Definitions

- **Personal Data:** Any information relating to an identified or identifiable natural person
- **Processing:** Any operation performed on personal data, including collection, storage, use, disclosure, and deletion
- **Data Controller:** The entity that determines the purposes and means of processing personal data
- **Data Processor:** An entity that processes personal data on behalf of the controller
- **Data Subject:** The individual to whom personal data relates

18. Contact Information and Further Assistance

If you have any questions about this Privacy Policy or our data protection practices, please contact:

Van Sterling Capital Ltd.
Data Protection Officer
Nu Bis Centre
Mosta Road
LJA 9012 Lija
Malta

Email: gdpr@vansterling.com
Telephone: +356 27 289 615

19. Conclusion

Van Sterling Capital Ltd. takes its obligations under data protection law seriously and strives to maintain the highest standards of privacy, transparency, and accountability. This policy is designed to provide clients with a clear understanding of how their personal data is handled, the safeguards in place, and the rights available to them.

We are committed to protecting your privacy while delivering excellent investment services in full compliance with all applicable regulatory requirements. Your trust is fundamental to our relationship, and we handle your personal data with the utmost care and respect.

Van Sterling Capital Ltd.
MFSA Licence Number: VANS-IF-9616
Nu Bis Centre, Mosta Road, LJA 9012 Lija, Malta