INTEGER WEALTH GLOBAL

Policy on Responsible Disclosure (Client & Investor Data)

Date: 11 February 2023

Policy Statement

Integer Wealth Global is committed to protecting the confidentiality and integrity of information related to our clients and investors.
This policy outlines our approach to responsible disclosure, ensuring compliance with the General Data Protection Regulation (GDPR) and other relevant laws. Unauthorised disclosure of classified information is strictly prohibited and will result in disciplinary action.

1. Scope

This policy applies to all employees, contractors, and third-party service providers who handle client and investor information.

2. Core Principles

2.1 **Confidentiality**: All client and investor information is classified and must be protected from unauthorized access or disclosure.
2.2 **Compliance**: We adhere to GDPR and other applicable regulations to ensure the lawful processing and protection of personal data.
2.3 **Integrity**: We maintain the accuracy and completeness of client and investor information.

3. Information Handling

3.1 **Access Control**: Access to classified information is restricted to authorized personnel only. Access rights are granted based on job responsibilities and are regularly reviewed.
3.2 **Data Encryption**: All classified information must be encrypted both in transit and at rest to prevent unauthorized access.
3.3 **Secure Storage**: Physical and digital records of classified information must be stored securely to prevent unauthorized access or tampering.

4. Disclosure Protocols

4.1 **Authorized Disclosure**: Information may only be disclosed to authorized parties with a legitimate need to know, and only after obtaining necessary approvals.

4.2 **Third-Party Agreements**: Any third-party service providers must sign confidentiality agreements and demonstrate compliance with GDPR and our security standards.
4.3 **Incident Reporting**: Any suspected or actual unauthorized disclosure must be reported immediately to the Data Protection Officer (DPO).

5. Compliance with GDPR

5.1 **Data Subject Rights**: We respect the rights of data subjects under GDPR, including the right to access, rectify, and erase their personal data.
5.2 **Data Breach Notification**: In the event of a data breach, we will notify the relevant supervisory authority and affected data subjects in accordance with GDPR requirements.

6. Data Retention

6.1 **Retention Periods**: Client and investor information will be retained only for as long as necessary to fulfil the purposes for which it was collected, or as required by law.
6.2 **Review and Deletion**: Regular reviews will be conducted to ensure that data is not held longer than necessary. Data that is no longer required will be securely deleted or anonymized.
6.3 **Legal Requirements**: Data retention practices will comply with all applicable legal and regulatory requirements, including GDPR.

7. Data Access Requests

7.1 **Right to Access**: Clients and investors have the right to request access to their personal data held by Integer Wealth Global.
7.2 **Request Process**: Data access requests must be submitted in writing to the Data Protection Officer. Requests will be processed within the timeframe specified by GDPR.
7.3 **Verification**: We will verify the identity of the requester before providing access to ensure the security of the data.
7.4 **Response**: We will provide a copy of the requested data, along with information about how it is being used and who it has been shared with, if applicable.

8. Procedures for Handling Access Requests

8.1 **Submission**: Access requests can be submitted via email, postal mail, or through our secure online portal.
8.2 **Acknowledgment**: We will acknowledge receipt of the request within 5 business days.
8.3 **Processing**: The DPO will coordinate with relevant departments to gather the requested information.
8.4 **Delivery**: The requested data will be provided in a secure format within one month of the request. Extensions may be granted in complex cases, with notification to the requester.

9. Data Portability Rights

9.1 **Right to Portability**: Clients and investors have the right to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit that data to another controller.
9.2 **Request Process**: Data portability requests must be submitted in writing to the Data Protection Officer.
9.3 **Verification**: We will verify the identity of the requester before providing the data.
9.4 **Response**: We will provide the data in a secure format within one month of the request. Extensions may be granted in complex cases, with notification to the requester.

10. Data Security Measures

10.1 **Network Security**: We implement robust network security measures, including firewalls, intrusion detection systems, and regular vulnerability assessments.
10.2 **Access Controls**: Strict access controls are in place to ensure that only authorized personnel can access sensitive information. This includes multi-factor authentication and role-based access controls.
10.3 **Data Encryption**: All sensitive data is encrypted both in transit and at rest using industry-standard encryption protocols.
10.4 **Regular Audits**: We conduct regular security audits and assessments to identify and mitigate potential vulnerabilities.
10.5 **Employee Training**: All employees receive regular training on data security best practices and are required to adhere to our security policies.
10.6 **Incident Response**: We have a comprehensive incident response plan to address any data breaches or security incidents promptly and effectively.

11. Data Breach Response

11.1 **Immediate Action**: Upon discovering a data breach, immediate steps will be taken to contain and mitigate the breach.
11.2 **Assessment**: The DPO will assess the scope and impact of the breach, including the type of data involved and the potential risks to data subjects.
11.3 **Notification**: Relevant supervisory authorities and affected data subjects will be notified within 72 hours of discovering the breach, in accordance with GDPR requirements.
11.4 **Investigation**: A thorough investigation will be conducted to determine the cause of the breach and to implement measures to prevent future incidents.
11.5 **Documentation**: All breaches and responses will be documented, including the details of the breach, actions taken, and lessons learned.

12. Roles in Data Protection

12.1 **Data Protection Officer (DPO)**: The DPO is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR and other data protection laws. The DPO acts as the main point of contact for data subjects and supervisory authorities.

12.2 **Liaison Department**: This department is responsible for coordinating data protection efforts across the organization, ensuring that all departments adhere to data protection policies and procedures.

12.3 **Chief Liaison Officer**: The Chief Liaison Officer leads the Liaison Department and works closely with the DPO to implement and monitor data protection measures. This role includes managing data access requests, overseeing data security measures, and ensuring compliance with data protection regulations.

13. Penalties for Non-Compliance

13.1 **Investigation**: All reports of unauthorized disclosure or non-compliance will be thoroughly investigated by the DPO.

13.2 **Consequences**: Violations of this policy may result in disciplinary action, up to and including termination of employment or contract. Legal action may also be pursued if warranted.

13.3 **Fines and Penalties**: Non-compliance with GDPR can result in significant fines and penalties. Integer Wealth Global will take all necessary steps to avoid such penalties by ensuring strict adherence to this policy.

14. Continuous Improvement

We are committed to continuously improving our data protection practices. This policy will be reviewed and updated regularly to ensure ongoing compliance with legal requirements and industry best practices.

15. Training and Awareness

15.1 **Employee Training**: All employees must undergo regular training on data protection and responsible disclosure practices.

15.2 **Awareness Programs**: We will conduct periodic awareness programs to reinforce the importance of data protection and compliance with this policy.

16. Contact Information

For further inquiries or detailed explanations regarding this policy, clients are encouraged to contact our Chief Liaison Officer at info@integerwealth.global or the legal officer at legal@integerwealth.global.