Privacy Policy

Effective Date: 25 December 2025 **Version**: 1.0.1

1. Introduction

Finerty Data Limited ("Finerty," "we," "us," or "our") is committed to protecting your privacy and processing your personal data in compliance with the General Data Protection Regulation (GDPR), the Irish Data Protection Act 2018, and the UK GDPR.

This Privacy Policy explains how we collect, use, disclose, and safeguard your personal data when you visit our website (https://finerty.com) or use our Letter of Authority (LOA) platform services.

1.1 Data Controller

Finerty Data Limited The CHQ Building North Wall Quay Dublin 1, D01 Y6H7 Ireland

Data Protection Officer: contact@finertydata.com

1.2 Scope

This Privacy Policy applies to:

- Visitors to our marketing website
- Prospective customers evaluating our services
- Registered financial advisors, regulated financial services entities and their users
- Clients who sign Digital Consent letters through our platform

2. Information We Collect

2.1 Marketing Website Visitors

When you visit our marketing website, we may collect:

Data Type	Examples	Source
Technical Data	IP address, browser type, device type, operating system	Automatic collection
Usage Data	Pages visited, time spent, referral source, navigation paths	Automatic collection
Cookie Data	Consent preferences, session identifiers	Cookies (see Cookie Policy)
Newsletter Data	Email address	Direct provision (opt-in only)

2.2 Platform Services - Brokerage Data

When a brokerage registers for our services, we collect:

Data Type	Examples	Purpose
Company Information	Business name, registration number, regulatory license	Account setup, compliance verification
Contact Details	Business address, phone, email	Service delivery, communications
Billing Information	Payment method, billing address	Subscription management
Administrator Details	Name, email, phone of primary contact	Account management
Branding Assets	Logo, colour scheme	White-label customisation

2.3 Platform Services - Advisor Data

For advisors using our platform, we collect:

Data Type	Examples	Purpose
Identity Data	Full name, email address, phone number	Account creation, communications and security
Professional Data	Registered Regulator Number, Provider Agency Numbers	Regulatory compliance, Digital Consent Letter generation
Authentication Data	Username, hashed password	Secure access
Profile Photo	Uploaded image (optional)	Platform personalisation
Activity Data	Login times, actions performed	Audit trail, security

2.4 Platform Services - Client Data

For clients who interact with Digital Consent documents, we collect:

Data Type	Examples	Purpose
Identity Data	Full name, date of birth	Digital Consent document generation
Contact Data	Email address, phone number, home address	Digital Consent document delivery, communications
Policy Data	Policy numbers, provider names, detailed and specific policy details including values, premium amounts, investment holdings etc.	Digital Consent document scope definition. enough information for financial services provider and advisor to advise client accurately.
Signature Data	Digital signature, signing timestamp, IP address	Legal validation
Authentication Data	Email (for OTP delivery)	Secure access

2.5 Special Category Data

We do not intentionally collect special category data (e.g., health data, ethnic origin, political opinions). If such data is inadvertently included in uploaded documents, it will be processed only as necessary to provide the Services.

3. How We Use Your Information

3.1 Lawful Basis for Processing

We process personal data based on the following lawful bases under GDPR Article 6:

Purpose	Lawful Basis	Data Types
Providing Services	Contract performance (Art. 6(1)(b))	All platform data
Account administration	Contract performance	Account data
Processing payments	Contract performance	Billing data
Sending service notifications	Contract performance	Contact data
Marketing communications	Consent (Art. 6(1)(a))	Newsletter subscribers
Website analytics	Legitimate interest (Art. 6(1)(f))	Usage data
Security and fraud prevention	Legitimate interest	Technical, activity data
Legal compliance	Legal obligation (Art. 6(1)(c))	Audit logs, signed documents
Responding to enquiries	Legitimate interest	Contact form data

3.2 Specific Processing Activities

Service Delivery

- Creating and managing user accounts
- Generating LOA documents with client and policy data
- Facilitating electronic signature workflows via DocuSign
- Storing and retrieving signed documents

Communications

- Sending transactional emails (password resets, LOA & Digital Consents status updates)
- Delivering marketing newsletters (opt-in only)
- Responding to support requests

Security and Compliance

- Authenticating users via Keycloak
- Logging access and activities for audit purposes
- Detecting and preventing fraudulent activity
- Complying with regulatory requirements

Analytics and Improvement

- Analysing platform usage patterns (anonymised)
- Improving service functionality and user experience
- Conducting statistical analysis (aggregated, non-identifiable)

4. Third-Party Service Providers

We share personal data with the following categories of third-party service providers, each bound by Data Processing Agreements (DPAs) ensuring GDPR compliance.

4.1 Infrastructure Providers

Cloud Hosting

- **Provider**: Microsoft Azure
- **Location**: North Europe (Ireland)
- **Data Processed**: All platform data
- **Safeguards**: Standard Contractual Clauses, ISO 27001 certification, SOC 1/2/3 compliance
- **Privacy Policy**: https://privacy.microsoft.com/

4.2 Electronic Signature Provider

DocuSign, Inc.

- **Purpose**: Processing electronic signatures on LOA documents
- **Data Shared**: Signer name, email address, document to be signed

- **Data Received**: Signed document, signature audit trail, timestamps
- **Location**: United States (with EU data residency option)
- **Safeguards**: Standard Contractual Clauses, EU-US Data Privacy Framework
- **Data Retention**: DocuSign retains documents for 90 days; we download and store locally
- **Privacy Policy**: https://www.docusign.com/privacy

4.3 Identity Provider

Keycloak (Self-Hosted)

- **Purpose**: User authentication and authorisation
- **Data Processed**: User credentials (email, hashed passwords), session data
- **Location**: Our own infrastructure in Ireland/UK
- **Safeguards**: Fully controlled by Finerty as data controller
- **Data Retention**: Duration of account plus 90 days

4.4 Secrets Management

HashiCorp Vault (Self-Hosted)

- **Purpose**: Secure storage of API credentials and secrets
- **Data Processed**: API keys, SMTP credentials (encrypted)
- **Location**: Our own infrastructure in Ireland/UK
- **Safeguards**: Encryption at rest, audit logging

4.5 Payment Processing (If Applicable)

Stripe, Inc.

- **Purpose**: Processing subscription payments
- **Data Shared**: Billing name, email, payment card details
- **Note**: We do not store full payment card numbers
- **Location**: United States and Ireland
- **Safeguards**: PCI-DSS Level 1 compliance, SCCs
- **Privacy Policy**: https://stripe.com/privacy

4.6 Analytics (Conditional on Consent)

Plausible Analytics (If implemented)

- **Purpose**: Privacy-focused website analytics
- **Data Processed**: Page URLs, referrers, device type (no personal identifiers)
- **Cookies**: None (cookie-less tracking)
- **Location**: European Union
- **Privacy Policy**: https://plausible.io/privacy

5. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected:

Data Category	Retention Period	Legal Basis
Active customer data	Duration of service	Contract performance
Terminated customer data	90 days post-termination	Data portability rights
Signed LOA documents	7 years from signature	Legal obligation (insurance regulations)
Audit logs	7 years	Legal obligation (GDPR Art. 30)
Marketing analytics	24 months	Legitimate interest
Newsletter subscribers	Until unsubscribe	Consent
Website visitor data	24 months	Legitimate interest
Support ticket data	3 years after resolution	Legitimate interest
Backup data	90 days after primary deletion	Technical necessity

6. Your Rights Under GDPR

6.1 Data Subject Rights

Under GDPR, you have the following rights regarding your personal data:

Right of Access (Art. 15) You can request a copy of the personal data we hold about you, including the purposes of processing, categories of data, recipients, and retention periods.

Right to Rectification (Art. 16) You can request correction of inaccurate or incomplete personal data.

Right to Erasure (Art. 17) You can request deletion of your personal data where:

- Data is no longer necessary for its original purpose
- You withdraw consent (where consent was the lawful basis)
- You object to processing and there are no overriding legitimate grounds
- Data was unlawfully processed

Exceptions: We may retain data where required for legal compliance, establishment or defence of legal claims, or public interest archiving.

Right to Restriction (Art. 18) You can request restriction of processing while we verify accuracy of data or assess an objection.

Right to Data Portability (Art. 20) You can request your data in a structured, commonly used, machine-readable format and have it transmitted to another controller.

Right to Object (Art. 21) You can object to processing based on legitimate interests. We will cease processing unless we demonstrate compelling legitimate grounds.

Right to Withdraw Consent (Art. 7) Where processing is based on consent, you can withdraw consent at any time without affecting the lawfulness of prior processing.

Rights Related to Automated Decision-Making (Art. 22) We do not make decisions based solely on automated processing that produce legal effects concerning you.

6.2 How to Exercise Your Rights

To exercise any of these rights, please contact us:

- **Email**: contact@finertydata.com

- **Post**: Data Protection Officer, Finerty Data Limited, The CHQ Building, North Wall Quay, Dublin 1, D01 Y6H7, Ireland

Verification: We may need to verify your identity before processing your request.

Response Time: We will respond within 30 days of receiving your request. If the request is complex, we may extend this by a further 60 days, but we will inform you within the initial 30-day period.

Fees: Requests are generally free. We may charge a reasonable fee for manifestly unfounded or excessive requests.

6.3 Right to Complain

If you are not satisfied with how we handle your request, you have the right to lodge a complaint with your local supervisory authority:

Ireland: Data Protection Commission 21 Fitzwilliam Square South Dublin 2, D02 RD28 Ireland Website: https://www.dataprotection.ie Email: info@dataprotection.ie

United Kingdom: Information Commissioner's Office Wycliffe House, Water Lane Wilmslow, Cheshire, SK9 5AF United Kingdom Website: https://ico.org.uk Helpline: 0303 123 1113

7. International Data Transfers

7.1 Transfers Within EU/EEA

Personal data may be transferred within the EU/EEA without additional safeguards, as these jurisdictions provide equivalent data protection.

7.2 EU-UK Transfers

Following Brexit, the UK has received an adequacy decision from the European Commission (28 June 2021), allowing free flow of personal data between the EU and UK.

7.3 Transfers to Third Countries

Where we transfer personal data outside the EU/EEA and UK (e.g., to DocuSign's US operations), we rely on:

- **Standard Contractual Clauses (SCCs)**: Commission-approved contractual terms ensuring equivalent protection

- **EU-US Data Privacy Framework**: For US companies participating in the framework
- **Adequacy Decisions**: For countries deemed to provide adequate protection

You may request a copy of the safeguards we use for international transfers by contacting contact@finertydata.com.

8. Data Security

8.1 Technical Measures

We implement comprehensive technical security measures:

Measure	Implementation
Encryption in Transit	TLS 1.3 for all connections
Encryption at Rest	AES-256 for stored data
Authentication	OAuth2/OIDC via Keycloak, MFA support
Access Control	Role-based access (RBAC), principle of least privilege
Audit Logging	All data access and modifications logged
Intrusion Detection	Automated monitoring and alerting
Vulnerability Management	Regular security scanning and patching
Backup and Recovery	Encrypted backups with tested recovery procedures

8.2 Organisational Measures

We implement organisational security measures:

- **Staff Training**: Annual security awareness training for all employees
- **Access Reviews**: Quarterly review of access privileges
- **Background Checks**: Pre-employment screening for staff with data access
- **Vendor Management**: Due diligence and DPAs with all processors
- **Incident Response**: Documented procedures for security incidents

8.3 Data Breach Notification

In the event of a personal data breach that poses a risk to your rights and freedoms:

- We will notify the relevant supervisory authority within 72 hours
- We will notify affected individuals without undue delay if the breach poses a high risk
- We will document all breaches and remediation actions

9. Children's Privacy

Our Services are not intended for individuals under 18 years of age. We do not knowingly collect personal data from children.

If we become aware that we have collected personal data from a child without parental consent, we will take steps to delete that information. If you believe we may have collected data from a child, please contact us at contact@finertydata.com.

10. Marketing Communications

10.1 Newsletter

We offer an email newsletter for industry insights and product updates. To subscribe:

- You must actively opt-in (checkbox not pre-selected)
- You can unsubscribe at any time via the link in each email
- We will not share your email address with third parties for their marketing

10.2 Service Communications

We will send transactional and service-related communications without separate consent, as these are necessary for service delivery. Examples include:

- Account activation and password reset emails
- Digital Consent Letters status notifications (sent, signed, completed)
- Important service updates and security notices
- Billing and payment confirmations

You cannot opt out of essential service communications while using our Services.

11. Cookies and Tracking Technologies

We use cookies and similar technologies on our website. For detailed information, please see our Cookie Policy.

Summary:

- **Strictly Necessary Cookies**: Required for website functionality (no consent needed)
- **Analytics Cookies**: Help us understand website usage (consent required)
- **Marketing Cookies**: Currently not used; if added, will require consent

You can manage cookie preferences at any time via the "Cookie Preferences" link in our website footer.

12. Changes to This Privacy Policy

We may update this Privacy Policy periodically to reflect changes in our practices, technologies, legal requirements, or business operations.

Notification of Changes:

- Material changes will be communicated via email to registered users at least 30 days in advance
- We will update the "Last Updated" date at the top of this policy
- Continued use of our Services after changes take effect constitutes acceptance

Version History: Previous versions of this Privacy Policy are available upon request.

13. Contact Us

For questions about this Privacy Policy or our data practices, please contact:

General Privacy Enquiries: Email: contact@finertydata.com

Data Protection Officer: Email: contact@finertydata.com

Postal Address: Data Protection Officer Finerty Data Limited The CHQ Building North Wall Quay Dublin 1, D01 Y6H7 Ireland

We aim to respond to all enquiries within 5 business days.

14. 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. Finerty is the data controller for data processed through our Services.

Data Processor: An entity that processes personal data on behalf of a data controller.

Data Subject: An identified or identifiable natural person whose personal data is processed.

GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).

DPA: Data Processing Agreement - a contract between data controller and processor.

SCCs: Standard Contractual Clauses - EU-approved contractual terms for international data transfers.

Last Updated: 24 December 2025