PRIVACY POLICY

Fearnley Securities

Last updated: 01.05.2026

Fearnley Securities

PRIVACY POLICY

Protecting your privacy is of great importance to Fearnley Securities. Accordingly, Fearnley Securities attaches great care to the protection of the data you give us, and to process it correctly and in compliance with applicable rules defined in the General Data Protection Regulation ("GDPR").

The GDPR sets out the rules governing how Fearnley Securities may collect, use, store and otherwise process personal data. Based on these requirements, Fearnley Securities has established additional internal privacy rules. These rules supplement the terms and conditions that apply to our customer relationships and apply to all our services, both current and future.

This Privacy Policy explains how Fearnley Securities collects, processes and stores personal data relating to our customers, prospective customers, users of our services and visitors to our website. We encourage you to familiarize yourself with this Privacy Policy. By using Fearnley Securities' services, you consent to the processing of your personal data in accordance with this Policy and the legislation applicable at any given time.

Please contact dataprotection@fearnleys.no if you have any questions concerning Fearnley Securities' data processing or this Privacy Policy.

Contents

1. Introduction

Protecting your privacy is of paramount importance to Fearnley Securities ("Fearnley", "we", "us", or "our"). We are committed to safeguarding the personal data you provide to us and ensuring that all processing is carried out lawfully, correctly, and in accordance with applicable confidentiality obligations and the requirements set out in the General Data Protection Regulation ("GDPR"). The GDPR establishes the rules governing how Fearnley may collect, use, store, and otherwise process personal data. Based on these requirements, Fearnley has established supplementary internal privacy rules. These rules apply in addition to existing customer agreements and govern all current and future services offered by Fearnley.

Personal data includes any information or assessments that can be linked to you as an individual, such as your name, address, telephone number, email address, IP address, national identification number (including both date of birth and social security number). Information relating to your behavioral patterns or usage of our services may also constitute personal data.

This Privacy Policy explains how Fearnley collects, processes, uses, and stores personal data obtained from our customers and from users of our services and/or our website.

Fearnley acts as a data controller when processing personal data. The Board of Directors is responsible for approving this Privacy Policy and for ensuring that it is reviewed annually to maintain compliance with applicable legislation and relevant regulatory guidance. The Chief Executive Officer is responsible for implementing the Policy, enforcing its requirements, and promoting a strong culture of data protection within the organization. All employees of Fearnley are required to act with integrity and to comply with this Privacy Policy at all times.

Fearnley may amend this Privacy Policy at any time. The most recent version will always be available on our website.

If we make any material changes that significantly affect how personal data is processed, stored, or otherwise handled, we will notify you in advance by email and/or by posting a notice on our website before such changes take effect.

By familiarizing yourself with this Privacy Policy and by using the services of Fearnley Securities, you consent to the processing of your personal data in accordance with this Policy and with the applicable data protection legislation in force at any given time

2. The Data Controller

Fearnley Securities AS, organization number 945 757 647, is the data controller for the processing of your personal data and is responsible for ensuring that all processing is carried out in accordance with applicable data protection legislation. Our contact details are as follows:

Fearnley Securities AS
Att: Data Protection Officer
P.O. Box 1158 Sentrum, N-0107 Oslo
Telephone: +47 22 00 93 00

Fearnley has appointed a Data Protection Officer (DPO) with the mandate to monitor and oversee our compliance with the GDPR and other relevant data protection requirements. If you have questions regarding our processing of personal data, wish to exercise your rights, or would like to submit a complaint, you may contact our DPO at: dataprotection@fearnleys.no.

3. Treatment of Personal Data

Fearnley Securities processes personal data primarily for purposes related to customer administration, customer relationship management, and the fulfilment of our obligations to provide appropriate and compliant investment services. Personal data is processed strictly in accordance with applicable data protection legislation and only to the extent necessary for the specific services we offer within our business areas.

3.1 The individuals for whom we process personal data

Category of individuals	Explanation	Reading reference
Investment Banking	Individuals acting as a contact person, representative, or authorized signatory for a company, foundation, or institution using our Investment Banking services. This also includes individuals who may be in possession of inside information or are involved in market soundings. Furthermore, it includes individuals reporting to us when we act as issuing agent or settlement agent, e.g., shareholders exercising pre-emption rights in a capital increase, or individuals submitting acceptance or subscription forms in a takeover process pursuant to an offer document or prospectus.	See section 4.1 and the general information in sections 4.5 - 4.7.
Securities and Project Finance	(i) Private individuals and professional or non-professional customers, and (ii) individuals acting as a contact person, representative, or authorized signatory for a corporate, institutional, or foundation customer using our Securities services	See section 4.2 and the general information in sections 4.5 - 4.7.
Office visitors	Individuals visiting our office premises.	See section 4.7 for general information.
Website visitors	Individuals visiting our website or using our digital and online services.	See section 4.3 and the general information in section 4.7.
Suppliers	Individuals acting as a representative or point of contact for a supplier or similar service provider interacting with Fearnley.	See section 4.4 and the general

Individuals related to a customer	Individuals connected to a customer in the capacity of guardian, trustee, mandatary/proxy, family member of a politically exposed person (PEP), estate beneficiary, beneficial or alternate owner, main shareholder, guarantor, endowment insurance policy holder or similar roles.	See sections 4.1.3, 4.2.3 and the general information in section 3.8.
Family members	Family members or other close relatives of Fearnley employees where processing is required for internal administrative or compliance-related purposes.	See section 4.7
Potential customers	Individuals who have expressed interest in our services or products or who otherwise qualify as potential customers.	See sections 4.5 and the general information in section 4.7.
Individuals in contact with us by phone	Individuals contacting us via recorded telephone lines used for advisory services, order placement, complaint handling, or Investment Banking communication.	See sections 4.5 and the general information in section 4.7.
Individuals in contact with us by Teams-meetings/calls	Individuals participating in Microsoft Teams calls or meetings with our employees in connection with our Investment Banking services.	See sections 4.5 and the general information in section 4.7.
Recruitment	Individuals whose personal data is processed in connection with recruitment activities, including job applicants nd the references they provide.	See sections 4.8 and the general information in section 4.5 - 4.7.

3.2 Types of Personal Data We Process

Category of personal data	Example
Identification details	Personal data used for identification, such as name, gender, national identity number, date of birth, customer number, passport or ID number, copies of identity documents (passport or other approved ID), digital identity documentation, place of residence, country of birth, tax residency and nationality.
Contact details	Personal data used for communication, including address, telephone number and email address.
Financial information	Personal data relating to financial transactions involving money or securities, such as bank account details, securities accounts, holdings, assets, liabilities, financial instruments, cash balances and other related financial data.
Credit information	Personal data relating to credit assessments, credit ratings and other information relevant to credit decisions.

Company information	Personal data linked to corporate entities, such as registration numbers and certificates, shareholder registers, share certificates, annual reports, information regarding board members and senior management, VPS details, LEI information and similar documentation.
Employment information	Personal data relating to an individual's employment relationship, including employment agreements, salary specifications and related employment documentation.
Know Your Customer (KYC)	Personal data collected for customer due diligence purposes, including identity information, financial data, tax residency and citizenship, tax obligations, politically exposed person (PEP) status, profession/employment, property ownership, managed assets, ownership in companies, income, investment horizon, purpose and nature of the customer relationship (including origin of assets and foreign transactions), beneficial owners and results from checks against sanctions lists.
Needs analysis	Personal data used to assess suitability and appropriateness, including information on source of funds, knowledge and experience in financial instruments and markets, investment objectives, risk tolerance, sustainability preferences and target returns.
Communication	Personal data contained in communications with us, including the content of emails, recorded telephone calls, Teams meetings/calls, Bloomberg messages and documents provided to us.
Technical data	Personal data collected through the use of electronic devices or interaction with our website, including IP address, device identifiers, browsing behavior, session data and website settings.
Recruitment Profile	Information about a candidate's profile such as gender, age, current position, and details of current employer or principal.
Recruitment Qualifications	Information relating to a candidate's competencies and qualifications, such as education, work experience, language skills and professional certifications.

3.3 Personal Data Collection

We primarily collect personal data directly from you, for example when you communicate with us, use our website, or enter into an agreement or customer relationship with us. In addition to information obtained directly from you, we also collect personal data from other sources where permitted by law and necessary for our services and regulatory obligations. These sources include:

- Address and contact information obtained from private and public registers to ensure that our customer records are accurate and up to date (e.g., Bisnode, 1881 or similar service providers).
- Information from sanctions lists and international organizations used for the prevention of money laundering, terrorist financing, and breaches of international sanctions regimes.
- Information from publicly available sources, including Google searches and other open sources, used to support the customer due diligence (KYC) process.

- Financial information from credit-rating agencies, collected for credit assessments, risk evaluation and other regulatory requirements.
- Shareholder information from the Central Securities Depository (CSD) obtained when Fearnley acts as issuing agent or in other company-related transactions. In such cases, we may receive personal data relating to all shareholders of a company on behalf of the issuer. This may include name, address, national identification number, securities account number, linked bank account information and details of shareholdings in the relevant company

3.4 Data Retention

We retain personal data only for as long as necessary for the purposes described in this Policy, or for as long as required by statutory obligations such as securities regulations, anti-money laundering legislation, accounting rules or legal claims. Once the retention period expires, personal data is securely deleted or anonymized.

4. Purpose of Processing Personal Data

4.1 Investment Banking

4.1.1 Entering into a contractual relationship

Purpose	Personal data	Legal basis	Storage time
Identity verification and authorization prior to entering into a contractual relationship.	Identification details, Contact details.	Legitimate interest (GDPR, Article 6.1(f)) – to ensure your identity and confirm your authority to represent the company, foundation or institution with which we are establishing a contractual relationship	Stored for five years after the end of the contractual relationship.

4.1.2 During the time of the contractual relationship

Purpose	Personal data	Legal basis	Storage time
Documenting, administrating and performing contractual and legal obligations.	Identification details, Contact details, Know Your Customer (KYC).	Legitimate interest (GDPR, Article 6.1(f)) – to document, administer and fulfil contractual and legal obligations for the company, foundation or institution you represent. Legitimate interest (GDPR, Article 6.1(f)) – to establish, exercise or defend legal claims.	Stored for five years after the end of the contractual relationship.
Ongoing communication.	Identification details, Contact details, Communication.	Legitimate interest (GDPR, Article 6.1(f)) – to communicate with you regarding matters related to the company, foundation or institution you represent.	Stored for five years after the end of the contractual relationship.
Acting upon your instructions, including purchasing/selling	Identification details, Contact details, Communication,	Legitimate interest (GDPR, Article 6.1(f)) – to act on your instructions on behalf of the	Stored for five years after the end of the

financial instruments, underwriting/placing instruments and providing financial advice.	Financial information.	company, foundation or institution you represent.	contractual relationship.

4.1.3 Compliance with our legal obligations

Purpose	Personal data	Legal basis	Storage time
Take measures to know our customers (KYC).	Investment Banking and Individuals related to a customer: Identification details, Contact details, Financial information, Know Your Customer (KYC).	Compliance with a legal obligation (GDPR, Article 6.1(c) and Article 10) – the Norwegian Anti-Money Laundering Act.	Stored for 5–10 years after the end of the contractual relationship (depending on risk classification).
Establish a register of individuals who come into contact with inside information.	Identification details, Contact details, Technical data.	Compliance with a legal obligation (GDPR, Article 6.1(c)) – EU Market Abuse Regulation (MAR) 596/2014.	Stored for 5 years.
Establish a register of individuals involved in market soundings and who thereby come into contact with inside information.	Identification details, Contact details, Technical data.	Compliance with a legal obligation (GDPR, Article 6.1(c)) – MAR 596/2014.	Stored for 5 years.
Record and store telephone calls and/or Teams meetings/calls, or meeting notes, relating to investment services and investment activity, including all transactions.	Identification details, Contact details, Communication.	Compliance with a legal obligation (GDPR, Article 6.1(c)) – MiFID II (Directive 2014/65/EU), MiFIR (Reg. 600/2014), MAR 596/2014, and the Norwegian Securities Trading Act.	Recorded calls stored for 5 years. Retention may be extended if necessary for an ongoing criminal investigation.
Screening against PEP ("politically exposed person") lists and EU sanctions lists.	Identification details, Know Your Customer (KYC) – relating to Investment Banking and	Compliance with a legal obligation (GDPR, Article 6.1(c) and Article 10) – the Norwegian Anti-Money Laundering Act, the EU Commission consolidated sanctions list; the Norwegian	Stored for up to 5 years after the end of the contractual relationship.

	Individuals related to a customer.	Sanctions Act and associated regulations.	
Monitor and review transactions to prevent the business from being used for money laundering or terrorist financing.	Identification details, Know Your Customer (KYC), Financial information.	Compliance with a legal obligation (GDPR, Article 6.1(c) and Article 10) – the Norwegian Anti-Money Laundering Act.	Stored for 5–10 years after the end of the contractual relationship (depending on risk classification).
Conduct checks against additional international sanctions lists.	Identification details, Know Your Customer (KYC).	Legitimate interest (GDPR, Article 6.1(f)) – to perform checks against international sanctions lists (e.g., UN Security Council lists and other international authorities) for enhanced customer risk assessment in accordance with the Norwegian Anti-Money Laundering Act. Processing of data relating to criminal offences is carried out under the exemption in Chapter 4 of the Norwegian Personal Data Act.	Stored for 5 years after the end of the contractual relationship.

4.2 Securities and Project Finance

4.2.1 Entering into a contractual relationship

Purpose	Personal data	Legal basis	Storage time
Verify your identity and authorization before entering into a contractual relationship.	Identification details, Contact details.	Private individual: Performance of a contract (GDPR, article 6.1(b)). Contact person, representative or beneficial owner: Legitimate interest (GDPR, Article 6.1(f)) – to verify your identity and your authority to represent the company with which we will enter into a contractual relationship.	Stored for 5 years after the end of the contractual relationship.

4.2.2 During the time of the contractual relationship

Purpose	Personal data	Legal basis	Storage time
Documenting, administrating and performing	Identification details, Contact	Private individual: Performance of a contract (GDPR, article 6.1(b))	Stored for 5 years after the end of

contractual and legal obligations.	details, Know Your Customer (KYC).	Contact person, representative or beneficial owner: Legitimate interest (GDPR, Article 6.1(f)) – to document, administer and perform contractual and legal obligations for the company, foundation or institution you represent. Legitimate interest (GDPR, Article 6.1(f)) – to establish, exercise or defend Fearnley's or your legal claims.	the contractual relationship.
Communication, e.g., via customer services or assistants.	Identification details, Contact details, Communication.	Private individual: Performance of a contract (GDPR, Article 6.1(b)). Compliance with a legal obligation (GDPR, Article 6.1(c)) – obligation to handle complaints pursuant to the Norwegian Securities Trading Act and Finanstilsynet Circular 4/2019 (Guidelines for complaints handling).	Stored for 5 years after the end of the contractual relationship.
		Contact person, representative or beneficial owner: Legitimate interest (GDPR, Article 6.1(f)) – to communicate with you regarding matters concerning the company, foundation or institution you represent.	
On request, provide brokerage, sales trading, and perform stock market related transactions.	Identification details, Contact details, Communication, Financial information.	Private individual: Performance of a contract (GDPR, article 6.1(b)).	Stored for 5 years after the end of the contractual relationship.
		Contact person, representative or beneficial owner: Legitimate interest (GDPR, Article 6.1(f)) – to act at your request on behalf of the company, foundation or institution you represent.	
Provide analyses in the online service Fearnley Securities Research Portal.	Identification details, Contact details, Technical data.	Legitimate interest (GDPR, Article 6.1(f)) – to provide you with relevant online services linked to the investment services we supply.	Stored for 5 years after you close your account, end your use of the online service, or terminate your customer relationship.

4.2.3 Compliance with our legal obligations

Purpose	Personal data	Legal basis	Storage time
Take measures to know our customers.	Securities and Individuals related to a customer: Identification details, Contact details, Know Your Customer (KYC).	Compliance with a legal obligation (GDPR, Article 6.1(c) and Article 10) – the Norwegian Anti-Money Laundering Act.	Stored for 5–10 years after the end of the contractual relationship (depending on risk classification).
Establish a register of individuals who come into contact with inside information.	Identification details, Contact details, Technical data.	Compliance with a legal obligation (GDPR, Article 6.1(c)) – EU Market Abuse Regulation (MAR) 596/2014.	Stored for 5 years.
Establish a register of individuals involved in market soundings and who thereby come into contact with inside information.	Identification details, Contact details, Technical data.	Compliance with a legal obligation (GDPR, Article 6.1(c)) – MAR 596/2014.	Stored for 5 years.
Record and store telephone calls and meeting notes relating to investment services and investment activity, including all transactions.	Identification details, Contact details, Communication.	Compliance with a legal obligation (GDPR, Article 6.1(c)) – MiFID II (Directive 2014/65/EU), MiFIR (Reg. 600/2014), MAR 596/2014, and the Norwegian Securities Trading Act.	Recorded calls stored for 5 years. May be extended if required for a criminal investigation.
Conduct mandatory screening against PEP lists and EU sanctions lists.	Identification details, Know Your Customer (KYC).	Compliance with a legal obligation (GDPR, Article 6.1(c) and Article 10) – the Norwegian Anti-Money Laundering Act; the EU Commission's consolidated list of financial sanctions; and the Norwegian Sanctions Act with associated regulations.	Stored for 5 years after the end of the contractual relationship.
Monitor and review transactions to prevent money laundering and terrorist financing.	Identification details, Financial information, Know Your Customer (KYC).	Compliance with a legal obligation (GDPR, Article 6.1(c) and Article 10) – the Norwegian Anti-Money Laundering Act.	Stored for 5–10 years after the end of the contractual relationship (depending on risk classification).
Carry out checks against other international sanctions lists.	Identification details, Know Your Customer (KYC).	Legitimate interest (GDPR, Article 6.1(f)) – to perform checks against additional international sanctions lists (e.g., UN Security Council lists	Stored for 5 years after the end of the contractual relationship.

		and other international authorities) to obtain enhanced customer information in line with the Norwegian Anti-Money Laundering Act. Processing of personal data relating to criminal convictions and offences is carried out under the exemption in Chapter 4 of the Norwegian Personal Data Act.	

4.3 Website Visitors

Purpose	Personal data	Legal basis	Storage time
Process contact information submitted in a notice of interest on our website and/or assist with your enquiry.	Identification details, Contact details.	Legitimate interest (GDPR, Article 6.1(f)) – to be able to fulfil your request.	Stored for up to 5 years after you submit the notice (unless an ongoing contractual relationship exists).
Display relevant marketing messages to you. The data is collected via cookies or other tracking technologies.	Technical data.	Your consent (GDPR, Article 6.1(a)).	Stored for a maximum of 10 years or until you withdraw your consent.
Facilitate and improve your user experience on our website. Data is collected via cookies or other tracking technologies.	Technical data.	Your consent (GDPR, Article 6.1(a)).	Stored for a maximum of 10 years or until you withdraw your consent.

4.4 Suppliers

Purpose	Personal data	Legal basis	Storage time
Identity verification and authorization before entering into a contractual relationship.	Identification details, Contact details.	Legitimate interest (GDPR, Article 6.1(f)) – to verify your identity and authority to represent the company with which we are entering into a contractual relationship.	Stored for the duration of our contract with the company you represent and 5 years thereafter.

Documenting, administrating and performing contractual and legal obligations.	Identification details, Contact details.	Legitimate interest (GDPR, Article 6.1(f)) – to document, administer and perform the contractual and legal obligations associated with the co-operation with the company, foundation or institution you represent.	Stored for the duration of our contract with the company you represent and 5 years thereafter.
Communicate with you regarding our co-operation.	Identification details, Contact details, Communication.	Legitimate interest (GDPR, Article 6.1(f)) – to communicate with you on matters relating to our co-operation with the company you represent.	Stored for the duration of our contract with the company you represent and 5 years thereafter.
Evaluation of our co-operation.	Identification details, Contact details, Communication	Legitimate interest (GDPR, Article 6.1(f)) – to continuously evaluate the performance of the contractual obligations by the company you represent	Stored for the duration of our contract with the company you represent and 5 years thereafter.

4.5 Marketing

Purpose	Personal data	Legal basis	Storage time
Compile a list of participants to our events.	Identification details, Contact details — for Customers and Potential customers.	Legitimate interest (GDPR, Article 6.1(f)) – to create and maintain participant lists for our events.	Stored for 5 years.
Promote products and services through various channels.	Identification details, Contact details — for Customers and Potential customers.	Legitimate interest (GDPR, Article 6.1(f)) – to market services and products we believe may be relevant or of interest to you.	Customers: Stored for 5 years after the end of the contractual relationship.
			Potential customers: Stored for 5 years.

4.6 Evaluate and Improve Our Business, Products and Services

Purpose	Personal data	Legal basis	Storage time
Develop, streamline, monitor and quality-assure our processes, systems and tools, and carry out	Identification details, Contact details, Financial information, Know Your Customer (KYC).	Legitimate interest (GDPR, Article 6.1(f)) – to evaluate and improve our business operations.	Stored for 5–10 years after the end of the contractual relationship (depending on risk classification).

statistical processing and compilations.			

4.7 Supervision, Legal Claims, Acquisitions, Exercise of Rights, etc.

Purpose	Personal data	Legal basis	Storage time
Investigate incidents, respond to requests and provide required information to a supervisory authority during supervision.	The categories of individuals and personal data requested in connection with the specific incident or supervisory process.	Compliance with a legal obligation (GDPR, Article 6.1(c)) – GDPR Articles 33–34 and 58; the Norwegian Securities Trading Act; and the Financial Supervision Act.	Stored for the duration of the incident or supervisory process, and up to 5 years thereafter, or longer if required by law.
Protect our interests in the event of a dispute.	The categories of individuals and the personal data necessary for handling the dispute, depending on the subject matter and parties involved.	Legitimate interest (GDPR, Article 6.1(f)) – to protect our interests in the event of a dispute.	Stored for the duration of the dispute and 5 years thereafter, or longer if required by law.
Carry out a merger or acquisition.	The categories of individuals and personal data covered by the merger or acquisition.	Legitimate interest (GDPR, Article 6.1(f)) – to carry out a merger or acquisition.	Not applicable.
Accommodate your request to exercise any of your GDPR rights.	All categories of individuals: Contact details, Identification details and any other personal data you provide that is necessary to fulfil your request.	Compliance with a legal obligation (GDPR, Article 6.1(c)) – GDPR Chapter III (rights of the data subject).	Stored for 1 year after your request has been handled.
Legal obligation to record and store telephone calls relating to advice and order placement.	Family members: Identification details, Contact details, Communication.	Legitimate interest (GDPR, Article 6.1(f)) – to follow up on advice, verify customer orders and comply with industry regulations applicable to securities transactions by employees and their relatives.	Recorded calls stored for 5 years. May be extended if required for a criminal investigation.

Legal obligation to save accounting information.	Financial information.	Compliance with a legal obligation (GDPR, Article 6.1(c)) – the Norwegian Accountants Act.	Stored for up to 10 years and retained until year-end.

4.8 Recruitment

Purpose	Personal data	Legal basis	Storage time
Manage the recruitment process.	Identification data, Communication, Qualifications, Contact details, Profile data.	Performance of a contract (GDPR, Article 6.1(b)) – taking steps at your request prior to entering into an employment contract. Legitimate interest (GDPR, Article 6.1(f)) – to manage and administer the recruitment process.	Stored during the recruitment process and for 24 months thereafter to fulfil our legitimate interest in managing and responding to potential legal claims.
Save your application for future recruitment.	Identification data, Communication, Qualifications, Contact details, Profile data.	Legitimate interest (GDPR, Article 6.1(f)) – to retain your information for future recruitment opportunities.	Stored for 24 months after the recruitment process, and extended further for any period to which you expressly agree.
Taking references.	Identification data, Contact details, Communication, Profile data.	Legitimate interest (GDPR, Article 6.1(f)) – to contact your references and obtain information relevant to the recruitment process.	Stored during the recruitment process and for 24 months thereafter to manage and respond to legal claims.
Carry out controls and tests.	Identification data, Test data.	Legitimate interest (GDPR, Article 6.1(f)) – to conduct assessments, including personality or ability tests, as part of the recruitment process.	Stored during the recruitment process and for 24 months thereafter to manage and respond to legal claims.
Monitor and evaluate the recruitment process.	Identification data, Profile data, Qualifications.	Legitimate interest (GDPR, Article 6.1(f)) – to monitor, evaluate and improve the recruitment process.	Stored during the recruitment process and for 24 months thereafter. Statistical data (non-personal) is

			kept until further notice.
Manage and respond to legal claims related to our recruitment process.	Only those categories of personal data necessary for the specific legal claim.	Legitimate interest (GDPR, Article 6.1(f)) – to manage and respond to legal claims.	Stored for as long as necessary to manage the specific legal claim.
Fulfilling legal obligations.	Only those categories of personal data necessary for compliance with the relevant legal obligation.	Compliance with a legal obligation (GDPR, Article 6.1(c)) – including obligations under the Norwegian Anti-Money Laundering Act.	Stored for as long as necessary to fulfil the particular legal obligation.

5. Cookies

We use cookies to facilitate and improve your experience when using our website. A cookie is a small text file placed on your device by your web browser at the request of our web server. Cookies enable the website to recognize your device and gather information about how you use our services, including which pages you visit and what content you interact with.

Our website also uses third-party cookies, which are cookies set by external service providers. These may be used for purposes such as measuring visitor numbers, analyzing web traffic, conducting market surveys, improving website performance, tailoring content, and enhancing the functionality of our website. The information collected through cookies, or other similar technologies, is not used to identify you as an individual.

The primary purpose of our use of cookies is to adapt, maintain, and further develop our online services based on user behavior and needs, and to enable more relevant marketing.

We may also use cookies from external partners to conduct market analyses, traffic analysis, targeted marketing, and functional enhancements to the website.

You can delete cookies stored on your device at any time. Doing so may, however, remove your saved settings and preferences. You may also configure your browser to block cookies from being stored. Please note that disabling cookies may reduce the functionality of certain websites, prevent access to login-protected areas, and limit the availability of certain features and content.

6. Disclosure of Personal Data

6.1 General

In order to provide our products and services, and to comply with applicable laws and regulations, we may need to disclose your personal data to third parties. Fearnley Securities may also share personal data with its subsidiaries — Fearnley Securities Inc., Fearnley Securities Ltd., and other entities within the Astrup Fearnley Group — where such disclosure is necessary to comply with group-wide management, control, reporting or governance requirements pursuant to law or regulation.

Any disclosure of personal data is subject to strict confidentiality obligations. Personal data will only be shared where the receiving entity is legally or contractually bound to ensure an adequate level of confidentiality and protection.

6.2 Suppliers and Partners

We may disclose personal data to suppliers and partners who process personal data on our behalf. These service providers act as data processors and may only process personal data according to our instructions and subject to contractual data protection obligations. Such suppliers and partners include:

- IT service providers: Companies responsible for the operation, maintenance, hosting, technical support and security of our IT systems and digital platforms.
- KYC service providers: External providers that support us in fulfilling statutory Customer Due Diligence (CDD/KYC) obligations.
- Credit-rating agencies: Companies that carry out credit assessments on our behalf.
- Marketing service providers: Companies assisting with the printing and distribution of marketing materials, management of social media and digital channels, and advertising activities.
- Banks, securities firms and central securities depositories: Entities through which we deliver or receive securities, or where we register securities-related information (e.g., settlement agents, custodians).
- Companies organizing analyst meetings for institutional investors: Third parties arranging investor meetings for institutional clients. Personal data is shared only regarding the contact persons, representatives or authorized signatories of institutional clients who have confirmed their participation.

All such disclosures are limited to what is necessary to perform the relevant service.

6.3 Other Third Parties

We may also disclose personal data to additional third parties where required by law or necessary to safeguard our rights or the rights of others. These include:

- Public authorities and supervisory bodies: Such as the Norwegian Tax Administration (Skatteetaten), the Police (Politiet), the Financial Supervisory Authority of Norway (Finanstilsynet), and the National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim).
- Courts and arbitration bodies: If disclosure is required in connection with legal proceedings, disputes, or arbitration.
- Euronext Securities Oslo (Verdipapirsentralen ASA): Where necessary for e.g. securities registration, settlement, or corporate actions.
- Construo: Where necessary for e.g. securities registration, settlement, or corporate actions for Project Finance projects.

Any such disclosure will only occur to the extent required and in accordance with applicable legislation.

7. Geolocation of Data

We strive to ensure that your personal data is processed and stored within the EU/EEA. All our primary data storage solutions are located within the EU/EEA, and our standard practice is to avoid transfers to countries outside this area.

In certain circumstances, however, it may be necessary to transfer personal data to partners or service providers located outside the EU/EEA ("third countries"). Such transfers may occur, for example, when we use service providers that operate globally or when support and maintenance services require access from outside the EU/EEA.

Regardless of the country in which your personal data is processed, we implement all necessary contractual, technical and organizational measures to ensure that the level of protection is equivalent to that required within the EU/EEA. We always ensure that an appropriate transfer mechanism is in place before any transfer occurs. This includes the use of the European Commission's Standard Contractual Clauses (SCCs) for international data transfers.

Where required, we supplement SCCs with additional technical and organizational safeguards, such as encryption, pseudonymization, and strict access controls, to ensure an adequate level of protection.

For transfers to the United States, we rely on the European Commission's adequacy decision, where applicable, or other valid transfer mechanisms when necessary.

8. Information Security

Fearnley Securities maintains robust organizational, technical and physical security measures to protect personal data against loss, misuse, unauthorized access, disclosure, alteration and destruction. Our information security framework is designed to ensure confidentiality, integrity and availability of personal data, and is regularly reviewed and updated to meet current regulatory and industry standards.

We have implemented the following safeguards:

- Encryption: Fearnley Securities uses encryption across many of its services to ensure that personal data is protected during transmission and storage, reducing the risk of unauthorized access.
- Confidentiality obligations: All employees are bound by strict confidentiality requirements. They sign confidentiality agreements and receive training on data protection and information security obligations.
- Penetration testing: Fearnley Securities conducts regular penetration testing to assess and strengthen the resilience of its information systems, ensuring that potential vulnerabilities are identified and remediated.
- Audits: Our information systems are subject to regular internal and external audits in accordance with recognized market standards. These audits help verify compliance with legal and regulatory requirements as well as internal policies.
- Information security governance: In line with information security policies based on ISO 9001 standards, Fearnley Securities performs ongoing internal and external audits and conducts risk-based controls related to information security to ensure continuous improvement and effective risk management.

Our commitment to information security means that we continuously evaluate and adapt our security practices in line with technological developments, operational needs and regulatory expectations.

9. Your Privacy Rights

9.1 General

Fearnley Securities is responsible for ensuring that your personal data is processed lawfully, transparently and in a manner that is fair to you. You have specific rights under data protection legislation regarding how we process your personal data. If you wish to exercise any of these rights, you may contact us using the details provided in Section 1.

Contact us if you would like to know more about how we have balanced your interests against ours.

We will respond to your request as soon as possible and no later than one month from the date we receive it. If we cannot respond within this period, you will be informed of the reason and the expected timeline for completion.

9.2 Right of Access

You have the right to know whether we process personal data about you. If we do, you are entitled to receive information about what data we process and how the processing is carried out. You also have the right to obtain a copy of the personal data we hold about you.

If you are seeking specific information, please indicate this in your request — for example, a certain category of data or data relating to a specific time period.

9.3 Right to Rectification

If you believe that the personal data we process about you is inaccurate or incomplete, you have the right to request that we correct or supplement it.
If we update your personal data following your request, we will attempt to notify third parties with whom we have shared the data, unless this proves impossible or requires disproportionate effort. Upon request, we will provide you with information about the parties with whom your data has been shared.

If you request rectification, you may also request that we restrict processing while we handle your request (see Section 9.5).

9.4 Right to Erasure

In certain circumstances, you have the right to request that we erase your personal data. This right applies if:

- The data is no longer necessary for the purposes for which it was collected.
- We process the data based on your consent and you withdraw consent.
- We process the data for direct marketing and you object to the processing.
- You object to processing based on our legitimate interest and we cannot demonstrate overriding legitimate grounds.
- The data has been processed unlawfully; or
- We are required by law to erase the data.

If your data is erased, we will also notify third parties with whom your personal data has been shared, unless this proves impossible. Upon request, we can inform you of the parties with whom your data has been shared.

9.5 Right to Restriction

You may request that we restrict our processing of your personal data. Restriction means the data will be marked to ensure it is processed only for limited purposes in the future. This right applies if:

- You believe the data is inaccurate and we are verifying its accuracy.
- The processing is unlawful and you request restriction instead of deletion.
- We no longer need the data for the original purpose, but you require it for legal claims.
- You have objected to processing based on legitimate interest, and restriction is required while we evaluate your objection.

During a restriction period, we may process the data only for storage, with your consent, for legal claims, to protect another person's rights, or for reasons of important public interest. You will be notified before any restriction is lifted.

We will also attempt to notify third parties with whom we have shared the restricted data, unless this is impossible or requires disproportionate effort. Upon request, you may receive a list of these third parties.

9.6 Right to Object

You have the right to object to processing that is based on our legitimate interest. If you object, we will evaluate whether our compelling legitimate grounds override your interests, rights and freedoms. If we cannot demonstrate compelling legitimate grounds, we will stop the processing in question — unless the data is required for legal claims.

You always have an unconditional right to object to processing for direct marketing purposes. If you object to such processing, we will cease processing your personal data for direct marketing immediately. You may also request restriction on processing while we consider your objection.

9.7 Right to Data Portability

You have the right to receive the personal data you have provided to us in a structured, commonly used and machine-readable format and to transfer this data to another controller. This right applies only to:

- Personal data you have provided directly to us.
- Processing based on performance of a contract with you.
- Processing carried out by automated means.

9.8 Right Not to Be Subject to Decisions Based Solely on Automated Decision-Making

You have the right to request a manual review of any decision that is based solely on automated processing and that produces legal effects or similarly significant consequences for you. You also have the right to object to such a decision.

9.9 Right to Withdraw Consent

If we process your personal data based on your consent, you may withdraw that consent at any time. Withdrawal applies only to future processing and does not affect the lawfulness of any processing carried out before consent is withdrawn.

9.10 Right to Complain

If you believe your personal data has been processed incorrectly or you are dissatisfied with our handling of your personal data, we encourage you to contact us so we can address your concerns. Our contact details are provided in Section 1.

You also have the right to lodge a complaint with supervisory authority.
In Norway, the supervisory authority is the Norwegian Data Protection Authority (Datatilsynet).

You may also submit a complaint to the supervisory authority in your country of residence, place of work or where you believe a violation has occurred.
More information, as well as Datatilsynet's contact details, can be found at: www.datatilsynet.no

10. Contact Information

Please contact dataprotection@fearnleys.no if you have any questions concerning Fearnley Securities' data processing or this Privacy Policy.

11. Changes to This Policy

We reserve the right to change and update this information at our discretion.