PRIVACY NOTICE – INFORMATION ABOUT DNB CARNEGIE'S PERSONAL DATA PROCESSING

In this notice we describe which personal data we process, why we process the personal data and what your rights are. If you have any questions about our processing of your personal data, please contact us or our data protection officer via the contact details provided in section 1 below.

It is of great importance to us that you feel safe with our processing of your personal data. We implement relevant and suitable measures to ensure that your personal data is protected and that the processing takes place in accordance with applicable data protection legislation and our internal policies.

Content

1 Who is the data controller and who should you contact? 3

2 Who do we process personal data about and what personal data do we process? 3

2.1 The individuals we process data about 3

2.2 The personal data we process 4

3 Why do we process your personal data, based on what legal basis and for how long do we process your personal data? 5

3.1 Investment Banking 5

3.1.1 Entering into a contract 5

3.1.2 During the time of the agreement 5

3.1.3 Compliance with our legal obligations 6

3.2 Securities 9

3.2.1 Entering into a contract 9

3.2.2 During the time of the agreement 10

3.2.3 Compliance with our legal obligations 11

3.3 Office visitors 14

3.4 Website visitors 14

3.5 Marketing 15

3.6 Evaluate and improve our business, products and services 16

3.7 Supervision, legal claims, acquisitions, exercise of rights etc. 16

3.8 Suppliers 18

3.9 Others and public information 19

4 Who do we share your data with? 20

4.1 General 20

4.2 Suppliers and partners 20

4.3 Other third parties 20

5 Processing we in particular would like to draw your attention to 21

5.1 Automated decision-making 21

6 Where is your data processed? 21

7 How do we get your personal data? 21

8 Do you have to provide your personal data? 22

9 Your rights 22

9.1 General 22

9.2 Right of access 22

PUBLIC

9.3 Right to rectification 22
9.4 Right to erasure (to be forgotten) 22
9.5 Right to restriction 23
9.6 Right to object 23
9.7 Right to data portability 24
9.8 Right to object against decisions based on automatic decision-making 24
9.9 Right to withdraw consent 24
10 Changes to the information 24

PUBLIC

1 Who is the data controller and who should you contact?

DNB Carnegie Investment Bank AB, Finland filial reg. no. 1439605-0 ("DNB Carnegie", "we", "us", or "our") is the data controller of the processing of your personal data and is accountable for ensuring that your personal data is processed in accordance with applicable data protection legislation. DNB Carnegie is part of the DNB Group.

Carnegie Investment Bank AB, Finland filial
Eteläesplanadi 2
00130 Helsinki
Finland
+358 9 6187 13 11

Our data protection officer is assigned to monitor our compliance with applicable data protection legislation. If you have any questions or would like to make a complaint about our processing of your personal data, please contact our data protection officer at dpo@dnbcarnegie.fi.

2 Who do we process personal data about and what personal data do we process?

2.1 The individuals we process data about

We process personal data about individuals who come in contact with our business in different ways. To make it easy for you to find the information concerning the processing of your personal data, we have structured the information into categories of individuals in the tables below. It may therefore be sufficient for you to only read the sections that apply to you. Please note that you may be included in more than one category of individuals depending on your relationship with us.

When using the term customer in this notice, we mean any private individual or individual working for a company/foundation/institution with which we have a contractual relationship with and who falls within the categories below.

When using the term GDPR in this notice, we mean the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

Category of individuals	Explanation	Reading reference for information on our processing of personal data
Investment Banking	You who are the contact person, representative or authorised signatory of a company, foundation or institution using our Investment Banking services. You may also be a person who comes into contact with insider information and is involved in market soundings. The Investment Banking category also includes you who report to DNB Carnegie in our role as an issuing institution or settlement agent. For example, upon a new share issue where the shareholders have pre-emption rights, you report your subscription to DNB Carnegie, or in a takeover, you accept via a subscription form to DNB Carnegie in accordance with the offer document/prospect.	See section 3.11 and the general information in sections 3.33 - 3.79.

PUBLIC

Securities	You who are (i) a private individual and a professional customer or (ii) a contact person, representative or authorised signatory for institutional clients using our Securities services.	See section 3.2 and the general information in sections 3.33 - 3.79.
Office visitors	You who visit our offices.	See section 3.33 and the general information in section 3.77.
Website visitors	You who visit our website or use our online services.	See section 3.44 and the general information in section 3.77.
Suppliers	You who are in contact with us in your role as a representative/contact person for a supplier or similar.	See section 3.88 and the general information in section 3.33-3.79.
Individuals related to a customer	You who have a connection to a customer of ours in your role as a guardian, trustee, mandatary/proxy, family member (if politically exposed person), beneficiary of the estate, beneficial or alternative owner, main shareholder, guarantor, endowment insurance policy holder or other such connection.	See sections for the relevant service **Error! Reference source not found.**-**Error! Reference source not found.**2 and the general information in section 3.77.
Family members	You who are a family member or other close relative of one of our employees.	See section 3.77
Potential customers	You who have shown interest in, or who we think may be interested in, our services or products. For example you who subscribe to our newsletters and similar mailings.	See section 3.55 and the general information in section 3.33-3.79.
Individuals who speak with us on the phone	You who get a call from or make a call to DNB Carnegie's recorded telephone numbers intended for order placement, complaints or direct marketing.	See sections **Error! Reference source not found.**, **Error! Reference source not found.**, and 3.5

2.2 The personal data we process

The personal data we process about you depends on how you interact with us and our relationship. The types of personal data we process are structured into the following categories. However, please note that this does not mean that we necessarily process all data about you listed under each category.

Category of personal data	Example
Identification details	Personal data used for identification such as name, personal identification number, customer number, passport/ID number, copy of identity document, digital identity document, place of residence and nationality.
Contact details	Personal data used for communication such as address, telephone number and e-mail address.
Financial information	Personal data relating to financial transactions of money or securities such as bank and account details, securities account, holdings, assets, liabilities, financial instruments, liquid assets, brokerage and time of closing.
Credit information	Personal data relating to credits such as credit applications and credit information.
Company information	Personal data relating to a company such as registration certificates, share register, share certificates and annual reports.
Employment information	Personal data relating to your employment, such as employment contracts and salary specification.

PUBLIC

Know Your Customer (KYC)	Personal data relating to customer due diligence for individuals and legal entities such as information regarding identity, financial information, tax residency, citizenship, tax liability, politically exposed person (PEP), profession/employment, property ownership, managed assets, assets from insurances, ownership in companies, income, investment horizon, purpose and nature of the business relationship (assets, origin and foreign transactions), beneficial owner, check against sanctions lists.
Communication	Personal data provided in communication with us such as the content of e-mails, recorded telephone calls, video meetings, chats and received documents.
Technical data	Personal data obtained from your use of electronic devices such as IP address, log in data, website behaviour, website settings and video/image from our camera surveillance.

3 Why do we process your personal data, based on what legal basis and for how long do we process your personal data?

3.1 Investment Banking

3.1.1 Entering into a contract

Purpose	Personal data	Legal basis	Storage time
Verify identity and authorisation before entering into a contract	Identification details, Contact details	Legitimate interest (GDPR, article 6.1(f)) – be able to verify your identity and authorisation to represent the company/foundation/institution with which we are to enter into a contract with. Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for eleven years after the end of the business relationship

3.1.2 During the time of the agreement

Purpose	Personal data	Legal basis	Storage time
Document, administer and perform the contract	Identification details, Contact details, Know Your Customer (KYC)	Legitimate interest (GDPR, article 6.1(f)) – be able to document, administer and perform the contract with the company/foundation/institution you represent. Be able to establish, exercise or defend DNB Carnegie's or your legal claims Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for eleven years after the end of the business relationship

PUBLIC

Communicate with you	Identification details, Contact details, Communication	Legitimate interest (GDPR, Article 6.1(f)) – be able to communicate with you on matters concerning the company/foundation/institution you represent. Be able to establish, exercise or defend DNB Carnegie's or your legal claims. Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for eleven years after the end of the business relationship
On request, purchase and sell securities, manage the securities portfolio and provide financial advice	Identification details, Contact details, Communication, Financial information	Legitimate interest (GDPR, article 6.1(f)) - be able to act at your request and document the advice we give at your request on behalf of the company/foundation/ institution you represent. Legitimate interest (GDPR, article 6.1(f)) – be able to establish, exercise or defend DNB Carnegie's or your legal claims. Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for eleven years after the end of the business relationship
Provide analyses in the online service DNB Carnegie Edge	Identification details, Contact details, Technical data	Legitimate interest (GDPR, article 6.1(f) - be able to provide analyses in the online service DNB Carnegie Edge at your request for the company/foundation/institution you represent. Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for five years after you close your account and your use of our online service Edge, or terminate your customer engagement with DNB Carnegie

3.1.3 Compliance with our legal obligations

Purpose	Personal data	Legal basis	Storage time
Take measures to know our customers	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 10) - the Finnish Act on Preventing Money Laundering and Financing of Terrorism (444/2017)	The personal data is stored for five years after the end of the business relationship or conclusion of the suspicious transaction, unless retentionis

PUBLIC

			necessary for reasons of criminal investigation, pending judicial proceedings or securing the rights of obliged entities or their employees. Need for continued retention shall be reviewed every three years.
Record and store telephone calls and video meetings with us relating to transactions	Identification details, Contact details, Communication	Compliance with a legal obligation (GDPR, article 6.1(c)) – Directive (2014/65/EU) and Regulation (600/2014) on Markets in Financial Instruments, EU Market Abuse Regulation no 596/2014 (MAR) and the Finnish Securities Market Act (746/2012)	Recorded telephone calls are stored for five years. If a criminal investigation has been initiated, ,a trial is pending or for protection of the official investigation or the rights of the person making the notification or the person subject to the notification the retention period can be extended if it is necessary
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 no 596/2014 (MAR)	The personal data is stored for five 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)) – EU Market Abuse Regulation no 596/2014 (MAR)	The personal data is stored for five years
Carry out checks against compiled lists of politically exposed persons (PEP) and EU sanctions lists	Investment Banking and Individuals related to a customer: Identification details, Know Your Customer (KYC)	Compliance with a legal obligation (GDPR, article 6.1(c)) and the Finnish Act on Preventing Money Laundering and Financing of Terrorism (444/2017)	The personal data is stored for five years after the end of the business relationship or conclusion of the suspicious transaction, unless retentionis necessary for reasons of

PUBLIC

			criminal investigation, pending judicial proceedings or securing the rights of obliged entities or their employees. Need for continued retention shall be reviewed every three years.
Carry out checks against other international sanctions lists	Identification details, Know Your Customer (KYC)	Legitimate interest (GDPR, article 6.1(f) – be able to perform checks against international lists (such as the consolidated list from UN's Security Council as well as counterparts from other international organisations) in order to obtain more detailed customer information in accordance with the the Finnish Act on Preventing Money Laundering and Financing of Terrorism (444/2017) Contact us if you would like to know more about how we have balanced your interests against ours. Personal data relating to criminal convictions and offences are processed in accordance with Finnish Data Protection Act (1050/2018) containing supplementary provisions to the EU General Data Protection Regulation	The personal data is stored for five years after the end of the business relationship or conclusion of the suspicious transaction, unless retentionis necessary for reasons of criminal investigation, pending judicial proceedings or securing the rights of obliged entities or their employees. Need for continued retention shall be reviewed every three years
Monitor and review transactions to prevent our business from being used for financing of terrorism or money laundering	Identification details, Know Your Customer (KYC), Financial information	Compliance with a legal obligation (GDPR, article 6.1(c)) – the Finnish Act on Preventing Money Laundering and Financing of Terrorism (444/2017)	The personal data is stored for five years after the end of the business relationship or conclusion of the suspicious transaction, unless retentionis necessary for reasons of criminal investigation, pending judicial proceedings or securing the rights of obliged

PUBLIC

			entities or their employees. Need for continued retention shall be reviewed every three years
Report to regulatory authorities	Identification details, Contact details, Financial information, Credit information, Know Your Customer (KYC)	Compliance with a legal obligation (GDPR, article 6,1(c)) – multiple legal obligations.	The personal data is stored for a maximum of ten years after the end of business relationship.

3.2 Securities

3.2.1 Entering into a contract

Purpose	Personal data	Legal basis	Storage time
Verify your identity and authorisation before entering into a contract	Identification details, Contact details	Private individual: Performance of a contract (GDPR, article 6.1(b)). Consent to the processing of biometric data (GDPR, article 6.1 (a)) Contact person, representative or authorised signatory: Legitimate interest (GDPR, article 6.1(f) – be able to verify your identity and authorisation to represent the company with which we will enter into a contract with. Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for eleven years after the end of the business relationship
Credit assessment for trading limit on a cash account	Identification details, Contact details, Financial information, Know Your Customer (KYC), Credit information, Employment information, Communication, Company information	Compliance with a legal obligation (GDPR, article 6.1(c)) – Act on the registration of certain credit providers and credit intermediaries (186/2023), Finnish Accounting Act (1336/1997)	The Documents and informatiin are stored for the duration of the credit and five years thereafter, however, after a dispute, the documents and information must be kept until the matter is settled or solved Accounting information (financial statements, management

PUBLIC

			report, ledgers, chart of accounts and the list of ledgers and materials) is stored at ten years after the accounting period. Accounting information (e.g. the vouchers for the financial year, correspondence regarding transactions) is stored at least six years after the accounting period.

3.2.2 During the time of the agreement

Purpose	Personal data	Legal basis	Storage time
Document, administer and perform the contract	Identification details, Contact details, Know Your Customer (KYC)	Private individual: Performance of a contract (GDPR, article 6.1(b)) Contact person, representative or authorised signatory: Legitimate interest (GDPR, article 6.1(f)) – be able to document, administer and perform the contract with the company/foundation/institution you are representing Legitimate interest (GDPR, article 6.1(f)) – be able to establish, exercise or defend DNB Carnegie's or your legal claims Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for eleven years after the end of the business relationship
Communicate with you, e.g. via customer service and 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)) to handle complaints , The Finnish Financial Supervisory Authority's general guidelines regarding complaints management concerning financial	The personal data is stored for eleven years

PUBLIC

		services to consumers (JC/2014/43 FI) Contact person, representative or authorised signatory: Legitimate interest (GDPR, article 6.1(f)) – be able to communicate with you on matters concerning the company/foundation/institution you represent Contact us if you would like to know more about how we have balanced your interests against ours.	
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)) Contact person, representative or authorised signatory: Legitimate interest (GDPR, article 6.1(f)) – be able to act at your request on behalf of the company/foundation/institution you represent Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for eleven years after the end of the business relationship
Provide analyses in the online service DNB Carnegie Edge	Identification details, Contact details, Technical data	Private individual: Performance of a contract (GDPR, article 6.1(b)) Contact person, representative or authorised signatory: Legitimate interest (GDPR, article 6.1(f) - be able to provide analyses in the online service DNB Carnegie Edge at your request for the company/ foundation/institution you represent. Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for five years after you close your account and your use of our online service Edge, or terminate your customer engagement with DNB Carnegie

3.2.3 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)) - Finnish Act on Preventing Money Laundering and Financing of Terrorism (444/2017)	The personal data is stored for five years after the end of the business relationship or conclusion of the

PUBLIC

			suspicious transaction, unless retentionis necessary for reasons of criminal investigation, pending judicial proceedings or securing the rights of obliged entities or their employees. Need for continued retention shall be reviewed every three years
Record and store telephone calls and video meetings relating to transactions	Identification details, Contact details, Communication	Compliance with a legal obligation (GDPR, article 6.1(c)) – Directive (2014/65/EU) and Regulation (600/2014) on Markets in Financial Instruments, EU Market Abuse Regulation no 596/2014 (MAR) and the Finnish Securities Market Act (746/2012)	Recorded telephone calls and video meetings are stored for five years. If a criminal investigation is initiated, the retention period can be extended if it is necessary for the investigation
Continuously follow-up on trading limit	Identification details, Contact details, Financial information, Know Your Customer (KYC), Communication, Company information	Compliance with a legal obligation (GDPR, article 6.1(c)) – FFFS 2018:16, Act on the registration of certain credit providers and credit intermediaries (186/2023), Finnish Accounting Act (1336/1997)	The Documents and information are stored for the duration of the credit and five years thereafter, however, after a dispute, the documents and information must be kept until the matter is settled or solved Accounting information (financial statements, management report, ledgers, chart of accounts and the list of ledgers and materials) is stored ten years after the accounting period.

PUBLIC

			Accounting information (e.g. the vouchers for the financial year, correspondence regarding transactions) is stored at least six years after the accounting period.
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 no 596/2014 (MAR)	The personal data is stored for five 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)) – EU Market Abuse Regulation no 596/2014 (MAR)	The personal data is stored for five years
Carry out checks against compiled lists of politically exposed persons (PEP) and EU sanctions lists	Identification details, Know Your Customer (KYC)	Compliance with a legal obligation (GDPR, article 6.1(c)) – Finnish Act on Preventing Money Laundering and Financing of Terrorism (444/2017	The personal data is stored for five years after the end of the business relationship
Carry out checks against other international sanctions lists	Identification details, Know Your Customer (KYC)	Legitimate interest (GDPR, article 6.1(f)) - be able to perform checks against international sanction lists (such as the consolidated list from UN's Security Council as well as counterparts from other international organisations) in order to obtain more detailed customer information in accordance with the Finnish Act on Preventing Money Laundering and Financing of Terrorism (444/2017) Contact us if you would like to know more about how we have balanced your interests against ours. Personal data relating to criminal convictions and offences are processed in accordance with Finnish Data Protection Act (1050/2018) containing supplementary provisions to the	The personal data is stored for five years after the end of the business relationship

PUBLIC

		EU General Data Protection Regulation	
Monitor and review transactions to prevent our business from being used for financing of terrorism or money laundering	Identification details, Financial information, Know Your Customer (KYC)	Compliance with a legal obligation (GDPR, article 6.1(c)) – the Finnish Act on Preventing Money Laundering and Financing of Terrorism (444/2017)	The personal data is stored for a maximum of ten years after the end of the business relationship
Monitor and review transactions to prevent, detect and report market abuse, suspicious trade orders or transactions such as insider dealing and market manipulation	Identification details, Contact details, Financial information, Company information, Technical data	Compliance with a legal obligation (GDPR, article 6.1(c)) – EU Market Abuse Regulation no 596/2014 (MAR), Commission delegated regulation (EU) 2016/957, Finnish Securities Market Act (746/2012)	Data is sotored 5 years
Report to regulatory authorities	Identification details, Contact details, Financial information, Credit information, Know Your Customer (KYC)	Compliance with a legal obligation (GDPR, article 6,1(c)) – multiple legal obligations.	The personal data is stored for a maximum of ten years after the end of business relationship.

3.3 Office visitors

Purpose	Personal data	Legal basis	Storage time
Greet you at our premises and register you in our systems so you may get the help you need from us	Identification details and food preferences	Legitimate interest (GDPR, article 6.1(f)) – be able to assist you in the matter you have visited us for Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data will be stored for 18 months from your visit
Camera surveillance of certain limited areas around our premises to maintain the security and prevent and investigate offences	Technical data (video without audio)	Legitimate interest (GDPR, article 6.1(f)) – to maintain the security of our premises and to investigate any offences against us Contact us if you would like to know more about how we have balanced your interests against ours.	The recorded material is automatically deleted after one month unless the material is needed for further investigation, and then it is deleted when the investigation is closed

PUBLIC

3.4 Website visitors

Purpose	Personal data	Legal basis	Storage time
Contact you who have filled in a notice of interest on our website and help you with your enquiry	Identification details, Contact details	Legitimate interest (GDPR, article 6.1(f)) – be able to fulfil your request Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for up to five years after you have submitted the notice to us (unless there is an ongoing contractual relationship)
Display relevant marketing messages to you. The data is collected via cookies or other tracking technologies ***Please read more in our cookie policy on our website***	Technical data	Your consent (GDPR, article 6.1(a))	Your personal data is stored for a maximum of ten years or until you withdraw your consent
To facilitate your user experience. The data is collected via cookies or other tracking technologies ***Please read more in our cookie policy on our website***	Technical data	Your consent (GDPR, article 6.1(a))	Your personal data is stored for a maximum of ten years or until you withdraw your consent

3.5 Marketing

Purpose	Personal data	Legal basis	Storage time
Provide you with subscriptions to our newsletter and similar mailings	Identification details, Contact details	Legitimate interest (GDPR, article 6.1(f)) – be able to provide you with our newsletter Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for the duration of your subscription to our newsletter. Once you have chosen to unsubscribe, the mailing will stop after 24 hours Personal data stored on our

PUBLIC

			website is deleted after 60 days and the data is permanently deleted from backups after a maximum of nine months
Compile a list of participants to our events	Customers and Potential customers: Identification details, Contact details	Legitimate interest (GDPR, article 6.1(f)) – be able to administrate a list of participants to our events Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for five years
Promote products and services through different channels, e.g. our call centre	Identification details, Contact details	Legitimate interest (GDPR, article 6.1(f)) – be able to market the services and products we think you might be interested in Contact us if you would like to know more about how we have balanced your interests against ours.	Customers: The personal data is stored for eleven years after the end of the business relationship Potential customers: The personal data is stored for five years
Record and store telephone calls with DNB Carnegie's Call centre, for training and quality enhancement purposes.	Identification details, Contact details, Communication	Legitimate interest (GDPR, article 6.1(f)) –- be able to evaluate and improve our business operations, to assure the quality of communication and marketing as well as educate the staff. Contact us if you would like to know more about how we have balanced your interests against ours.	Recorded telephone calls are stored for 30 days

3.6 Evaluate and improve our business, products and services

To develop our internal operations and provide the best possible services and products to our customers, we process your personal data in the following ways.

Purpose	Personal data	Legal basis	Storage time
Develop, streamline, monitor and quality-assure our processes, systems and tools, and carry out statistical processing and compilations	Customers: Identification details, Contact details, Financial information, Know Your Customer (KYC)	Legitimate interest (GDPR, article 6.1(f)) – be able to evaluate and improve our business operations Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data is stored for eleven years after the end of the business relationship

PUBLIC

3.7 Supervision, legal claims, acquisitions, exercise of rights etc.

Purpose	Personal data	Legal basis	Storage time
Investigate incidents, respond to requests and provide requested information to a supervisory authority in the event of supervision	The categories of individuals and personal data requested in relation to the incidents and supervision	Compliance with a legal obligation (GDPR, article 6.1(c)) – GDPR, articles 33-34 and 58 respectively, and FIVA/2023/483, The Finnish Financial Supervisory Autohority´s regulations and guidelines regarding Management of operational risk in supervised entities of the financial sector	The personal data is stored for the duration of the incident or supervision and up to two years thereafter
Protect our interests in the event of a dispute	The categories of individuals and personal data necessary with regard to the subject matter of the dispute and the parties involved	Legitimate interest (GDPR, article 6.1(f)) – be able to establish, exercise or defend legal claims, debt collection cases and manage complaints. Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data are normally stored for eleven years after the end of the business relationship or for the duration of a dispute and ten years thereafter
The categories of individuals and personal data covered by the merger or acquisition	The categories of individuals and personal data covered by the merger or acquisition	Legitimate interest (GDPR, article 6.1(f)) – be able to carry out a merger or acquisition Contact us if you would like to know more about how we have balanced your interests against ours.	Not applicable
Accommodate your request to exercise any of your privacy rights	Contact details, Identification details and other personal data about you that you provide in your request and that are necessary to fulfil your request	Compliance with a legal obligation (GDPR, article 6.1(c)) – GDPR, Chapter III	The personal data is stored for 12 months after we have handled your request
Record and store telephone calls and video meetings relating to advice and order placement	Identification details, Contact details, Communication	Legitimate interest (GDPR, article 6.1(f)) – be able to follow up on advice and verify customer orders and to comply with industry regulations on securities transactions by employees and their relatives Contact us if you would like to know more about how we have balanced your interests against ours.	Recorded telephone calls and video meetings are stored for ten years. If a criminal investigation has been initiated, the retention period can be extended if it is necessary for the investigation
Perform calculations due to legal obligations	Identification details, Financial information	Compliance with a legal obligation (GDPR, article 6.1(c)) – Regulation (575/2013) on prudential requirements for	The personal data is stored up to and including the seventh year after

PUBLIC

regarding capital adequacy		credit institutions and investment firms and Directive (2013/36) on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms	the end of the year during which the data was registered
Store accounting information	Financial information	Compliance with a legal obligation (GDPR, article 6.1(c)) - Finnish Accounting Act (1336/1997)	Accounting information (financial statements, management report, ledgers, chart of accounts and the list of ledgers and materials) is stored at least ten years after the accounting period. Accounting information (e.g. the vouchers for the financial year, correspondence regarding transactions) is stored at least six years after the accounting period.

3.8 Suppliers

Purpose	Personal data	Legal basis	Storage time
Verify your identity and authorisation before entering into a contract	Identification details, Contact details	Legitimate interest (GDPR, article 6.1(f)) – be able to verify your identity and authorisation to represent the company with which we are to enter into a contract with Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data will be stored for the duration of our contract with the company you represent and ten years thereafter
Document, administer and perform the contract	Identification details, Contact details	Legitimate interest (GDPR, article 6.1(f)) – be able to document, administer and perform the contract with the company you represent Contact us if you would like to know more about how we have	The personal data will be stored for the duration of our contract with the company you represent and ten years thereafter

PUBLIC

		balanced your interests against ours.	
Communicate with you regarding our co-operation	Identification details, Contact details, Communication	Legitimate interest (GDPR, article 6.1(f)) – be able to communicate with you on matters relating to our co-operation with the company you represent Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data will be stored for the duration of our contract with the company you represent and ten years thereafter
Evaluation of our co-operation	Identification details, Contact details, Communication	Legitimate interest (GDPR, article 6.1(f)) – be able to continuously evaluate the performance of the contractual obligations by the company you represent Contact us if you would like to know more about how we have balanced your interests against ours.	The personal data will be stored for the duration of our contract with the company you represent and ten years thereafter
Record and store telephone calls and video meetings relating to order placement	Identification details, Contact details, communication	Compliance with a legal obligation (GDPR, article 6.1(c)) – Directive (2014/65/EU) and Regulation (600/2014) on Markets in Financial Instruments, EU Market Abuse Regulation no 596/2014 (MAR) and the Finnish Securities Market Act (746/2012)	Recorded telephone calls and video meetings are stored for ten years. If a criminal investigation has been initiated, the retention period can be extended if it is necessary for the investigation

3.9 Others and public information

This section sets out the purposes for which DNB Carnegie is the controller.

Purpose	Personal data	Legal basis	Storage time
Establish a register of individuals who come into contact with inside information	Insiders Identification details, Contact details	Compliance with a legal obligation (GDPR, article 6.1(c)) – EU Market Abuse Regulation no 596/2014 (MAR)	The personal data is stored for five years
Establish a register of individuals involved in market soundings and who thereby come into contact with inside information	Insiders Identification details, Contact details	Compliance with a legal obligation (GDPR, article 6.1(c)) – EU Market Abuse Regulation no 596/2014 (MAR)	The personal data is stored for five years

PUBLIC

4 Who do we share your data with?

4.1 General

DNB Carnegie is part oh the DNB Group. In order to provide our products and services to you, and to comply with laws and regulations, we sometimes need to share your personal data with others, including other companies within the DNB Carnegie Group, the DNB Group and third parties who assist us in various aspects of our business.

Where we appoint third parties to act as our processor, we ensure that we put in place the necessary documentation required under the GDPR and require them to only process the data on our behalf.

4.2 Suppliers and partners

We share your personal data with our suppliers and partners, such as:

- *IT service providers*: companies that manage the necessary operation, technical support and maintenance of our IT solutions.
- *KYC service providers*: companies that provide us with services to enable us to fulfil our legal obligation to conduct customer due diligence measures.
- *Credit-rating agencies*: companies that conduct credit-ratings on our behalf.
- *Debt collection agencies*: companies that manage our cases regarding debt collection.
- *Marketing*: companies that help us with the printing and distribution of marketing materials, managing our social media and other digital channels, and advertising agencies.
- *Banking and insurance partners*: companies that provide, for example, insurance or loans distributed through us.
- *Banks, payment service providers, securities companies and central securities depositories*: such banks, securities companies and central securities depositories to which DNB Carnegie delivers securities, receives securities from or registers information regarding securities with. For example, we provide information to Euroclear when registering voting rights before a general meeting and when they request a list of asset managers.
- *Companies that organise analyst meetings for DNB Carnegie's institutional clients:* such companies that seeks investors among DNB Carnegie's institutional clients. Personal data is only shared with such companies regarding the contact persons, representatives or authorised signatories of institutional clients who have informed DNB Carnegie that they wish to attend the relevant analyst meeting.

4.3 Other third parties

We may also share your personal data with other third parties, such as:

- *Authorities*: such as the Finnish Tax Authority (Verohallinto), the Police, Finnish Financial Supervisoty Authority (Finanssivalvonta), the Bank Of Finland, the Finnish Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto) and equivalent authorities in other countries, and other authorities when required by law.
- *Courts and arbitration boards:* in the event of a dispute or other proceedings.
- *Central Security Depository (CSD):* such as Euroclear Nordics.
- *Professional advisers:* such as our lawyers, accountants and insurers.
- *Issuer*: upon request information about custodian registered shareholders
- *AI services*: At your request, we share your personal data with AI services. The AI service you connect to acts as an independent controller in respect of the personal data processed

through its service. DNB Carnegie is unable to request the deletion of personal data transferred to your AI service and has no control over how your personal data is processed by the AI service. The provider of the AI assistant may be established outside the EU/EEA, and we recommend that you review the AI provider's privacy notice before enabling the connection. If your personal data is transferred outside the EU/EEA, you may not benefit from the same level of legal protection as within the EU/EEA.

5 Processing we in particular would like to draw your attention to

5.1 Automated decision-making

Automated decision-making means a fully automated process where the decision in question is made using algorithms, i.e. without the involvement of a human being. We have automated processes for applications for account opening and Know Your Customer (KYC).

We use automated decision-making when it comes to accepting/rejecting your application. Such automated decision-making is based on the information you provide in your application and is used solely to assess whether our acceptance criteria are met or not.

You always have the right to contact us if you are not satisfied with the decision and want to challenge it. We will then review the information behind the decision and any additional information you provide us. The review will be conducted by a human who is authorised to change the decision if it turns out that it was made on incorrect grounds.

In the case of automated decision-making, your application may not provide us with the sufficient information to approve your application. You will then be asked to contact us. This does not mean that your application has been rejected, but only that we need additional information to be able to complete your application.

6 Where is your data processed?

We always strive to process and store your personal data within the EU/EEA. However, in certain situations we may need to transfer your personal data to partners or service providers located outside the EU/EEA (third countries). The third countries to which we may transfer personal data are Australia, Brazil, Canada, Czech Republic, Hong Kong, India, Malaysia, Switzerland, Serbia, Singapore, Sri Lanka, UK, Ukraine and the USA.

Regardless of where your personal data is processed, we implement all reasonable and/or required contractual, technical and organisational measures to ensure that the level of protection is equivalent to that of the EU/EEA. We always ensure that there is an appropriate transfer mechanism in place and we therefore generally use the European Commission's standard contractual clauses. We also take additional technical and organisational security measures where necessary, such as encryption and pseudonymisation. For transfers to Switzerland and the USA, an adequacy decision of the European Commission is applied.

7 How do we get your personal data?

We collect personal data directly from you, for example when you communicate with us, use our website or enter into a contract with us. We also collect personal data about you from other sources, such as:

- Address information from private and public registers to ensure that we have the correct contact details for you in our registers, e.g. from the Population Information System.
- Your holdings with other banks/asset managers when you ask us to produce such a report.
- Information from sanctions lists or international organisations to prevent money laundering.

- Image or video of you from camera surveillance conducted at our premises.
- Financial information from credit-rating agencies.
- Shareholder information from central securities depositories when, in our role as an issuing institution, in connection with specific company transactions, we receive personal data on all shareholders of the specific company on behalf of the company. The personal data we receive are name, address, personal identification number, securities account and linked bank account and holdings in the specific company.
- Information on potential customers from database companies such as Salezure AB, Wealth Monitor, Holdings Modular Finance AB and Valu8 Group.

8 Do you have to provide your personal data?

To enter into and perform our contract with you, to comply with legal requirements and to enable you to visit our premises, events and interact with us on our website, you need to provide the personal data we request. If you do not provide us with the personal data we request, this may, in some cases, result in us not being able to provide you with the services and products you request and/or that we cannot comply with the legal requirements imposed on us as a financial institution. We will clearly inform you of what information is mandatory when you, for example, enter into a contract with us.

9 Your rights

9.1 General

We are accountable for your personal data being processed in a legal, transparent and open manner in relation to you, and that your personal data is accurate and up to date. You have certain rights regarding our processing of your personal data. If you want to exercise any of your rights, you can contact us by using the contact details in section 1 above.

We will get back to you as soon as we can, and at the latest within one month of receiving your request. If we cannot answer your request or need more time, we will explain why.

9.2 Right of access

You have the right to know if we process personal data about you or not. If we do, you also have the right to receive information about what personal data we process and how we process it. You also have the right to receive a copy of the personal data we process about you.

If you are interested in any specific information, please indicate this in your request. For example, you can specify if you are interested in a certain type of information or if you want information from a certain time period.

9.3 Right to rectification

If the personal data we hold about you is inaccurate, you have the right to have the personal data corrected. You also have the right to complete incomplete personal data with supplementary information needed for the personal data to be correct. Once we have corrected or completed your personal data with new information, we will inform those we have shared your personal data with about the update, if it is not impossible or too cumbersome. If you ask us, we will also tell you who we have shared your personal data with. If you request rectification, you also have the right to request that we restrict our processing during the time we investigate the matter.

9.4 Right to erasure (to be forgotten)

In certain cases, you have the right to request that we erase the personal data we have about you. You have the right to have your personal data erased if:

- The personal data is no longer necessary for the purposes for which they were collected or otherwise processed,
- We process your personal data on the basis of your consent and you withdraw your consent,
- The personal data is processed for direct marketing purposes and you object to the processing,
- You object to the processing of personal data based on our legitimate interest and we cannot demonstrate that our reasons for processing outweigh your interests,
- The personal data is processed unlawfully, or
- We have a legal obligation to erase the personal data.

If we erase the personal data following your request, we will also inform those we have shared your personal data with of the erasure, if it is not impossible or too cumbersome. If you ask us, we will also tell you who we have shared your personal data with.

9.5 Right to restriction

Restriction means that the personal data is marked so that it can only be processed for certain limited purposes in the future. The right to restriction applies:

- When you believe the personal data is inaccurate and you have requested rectification. You can also request that we restrict our processing while we investigate if the personal data is accurate or not,
- If the processing is unlawful and you do not want the personal data to be erased,
- When we no longer need to process the personal data for the purposes for which we collected it, but you need it to be able to establish, exercise or defend legal claims,
- If you have objected to processing based on our legitimate interest. Then you can request that we restrict the processing while we investigate whether our interest in processing your personal data outweighs your interests.

Even if you have requested that we restrict our processing, we have the right to use it for storage, if we have your consent to the processing, to assert or defend legal claims or to protect someone else's rights. We may also use the personal data for reasons relating to important public interest. We will let you know before the restriction expires.

If we restrict the processing of your personal data, we will also inform those we have shared your personal data with, if it is not impossible or too cumbersome. If you ask us, we will also tell you who we have shared your personal data with.

9.6 Right to object

You have the right to object to our processing of your personal data that is based on our legitimate interest. If you object to the processing, we will, based on your specific situation, evaluate whether our interests in processing the personal data outweigh your interests in not having your personal data processed for that purpose. If we cannot demonstrate compelling legitimate grounds that outweigh yours, we will stop the processing to which you object - provided that we do not need to process the personal data for the establishment, exercise or defence of legal claims.

You always have the right to object to the processing of your personal data for direct marketing. We are then no longer permitted to process your personal data for direct marketing.

If you object to the processing, you also have the right to request restriction while we investigate the matter, please read more under section 9.5 above.

9.7 Right to data portability

Data portability means that you have the right to obtain the personal data we have collected about you, from you, in a structured, publicly available and machine-readable format and that you have the right to transfer it to another controller.

The right to data portability only applies:

- for data collected from you, about you,
- if the processing takes place due to the performance of a contract with you or with your consent, and
- the processing is automated.

9.8 Right to object against decisions based on automatic decision-making

You have the right to request that we shall review the decision that is based solely on automated decision-making and which has legal effects for you or significantly affects you in a similar way. You also have the right to object against the decision. Please read more about automated decision-making in section 5.1.

9.9 Right to withdraw consent

You have the right to withdraw a given consent for a particular processing based on the legal basis of consent at any time. A withdrawal does not affect the lawfulness of our processing before the consent was withdrawn.

Right to complain

If you have any objections or complaints about the way we process your personal data, please contact us and we will try to resolve your issue, see our contact details in section 1 above.

You also have the right to lodge a complaint with the supervisory authority. The Finnish Office of the Data Protection Ombudsman (Finnish: Tietosuojavaltuutettu) is the Finnish supervisory authority for our processing of your personal data. You also have the right to lodge a complaint with the supervisory authority in the country where you live, work or where you believe an infringement has taken place.

10 Changes to the information

We reserve the right to change and update this information from time to time. In case of material changes, we will clearly inform you of this in a suitable way.

The information text was last updated October 16th, 2026.

PUBLIC