Arctic Group Policies

8 November 2018

Table of contents

A CODE OF CONDUCT

1. Purpose

The code of conduct is an integral part of the governance structure in Arctic. The purpose of this document is to state the requirements for business practice and personal conduct of individual employees and to set out the principles on how we do business. Further requirements may be/are set out in the written procedures for each of the group companies.

The code of conduct has been approved by the board of Arctic Securities AS and shall apply to any company within the Arctic group including its subsidiaries, which include any company solely or collectively owned/controlled by more than 50 % of Arctic group companies.

The code of conduct applies to members of the board of directors, managers and employees as well as those acting on behalf of the company. The code does not apply directly to the company's business partners, but Arctic does not wish to be associated with business partners that do not have appropriate ethical standards.

Any questions regarding the code of conduct are to be addressed to one's superior or the compliance department responsible for your company.

2. Corporate Ethics

2.1 General

Our corporate ethics shall serve as a guide in our daily work to create a sound corporate culture which shall create value for our customers, investors, staff and anyone benefitting from our services.

Arctic will comply with applicable laws and regulations and act in an ethical, sustainable and socially responsible manner. Breaches of laws and ethical requirements are a threat to Arctic's competitiveness and reputation.

Arctic sets high ethical standards for everyone who acts on behalf of the company. Individuals must abide by applicable laws and regulations and carry out their duties in accordance with the requirements and standards that apply in Arctic. They shall not assist any breach of laws by business associates.

2.2 Questions regarding ethics

Ethical issues shall be handled with openness. If in doubt, the issue should be raised with one's superior. Allow time when addressing ethical decisions in order to think thoroughly through such issues.

3 Conflict of interests

3.1 General

Individual employees must behave impartially in all business dealings and not give other companies, organizations or individuals improper advantages. An individual must not become involved in relationships that could give rise to an actual or perceived conflict with Arctic's interests or could in any way have a negative effect on their own freedom of action or judgement.

An individual must not use the company's assets, property or information acquired through their position or office in Arctic for personal advantage or for the purpose of competing with the company. Suspicion of a conflict of interest should be reported to a superior.

The company's business must be operated at all times in such a way that the risk of conflicts of interest between the company and its customers or between the company's customers, will be limited to a minimum. If conflicts of interest cannot be avoided, the company should make sure that the customers' interests as far as possible have priority over the company's interests, as well as providing information to customers about the relevant conflicts of interest. No customers will be unfairly favored at the expense of other customers.

If the company or an employee has a position of a certain scope in the financial instruments related to customer services rendered, information about such position is to be made available to the customer as well as any affected third parties. The same applies where the company and/or an employees has an interest in relation to the transactions or investment the customer would like to execute.

An employee must not take any action that may prevent another employee or the company acting in the best interest of customers. Restraint must be exercised with respect to private business deals with companies or people with whom the company has business relations.

Potential conflict situations shall be submitted to the superior of the person who is faced with such conflict situation.

3.2 Directorships, employment or other assignments

All directorships, employment or other assignments held or carried out by Arctic employees in other enterprises which have, or may expect to have, commercial relations with Arctic, must be approved by Arctic. Arctic employees must not engage in other paid directorships, employment or assignments of any significance outside Arctic except by agreement with Arctic. Should a conflict of interest arise, or if the employee's ability to perform their duties or fulfill their obligations to Arctic is compromised, such approval will not be granted, or will be withdrawn.

4 Working conditions

4.1 General

Arctic supports and respects human rights and appreciates diversity, cultural and other differences.

Arctic shall create a working environment based on fair employment practices and where ethical conduct is recognized and valued. No direct or indirect discrimination shall take place based on race, color, gender, sexual orientation, age, language, religion, political or other opinions or other status.

Arctic expects individuals to treat everyone with whom they come into contact through their work or work related activities with courtesy and respect. Individuals must refrain from all conduct that can have a negative effect on colleagues, the working environment or Arctic.

This includes any form of harassment, discrimination or other behavior that colleagues or business associates may regard as threatening or degrading.

4.2 Political activity

Arctic does not support individual political parties or individual politicians. Arctic may participate in public debate when this is in the company's interest. All individuals are free to participate in democratic political activities, but this must be without reference to or connection with their relationship to Arctic.

4.3 Purchase of sexual services

Arctic is against the purchase of sexual services. Purchase of sexual services may support human trafficking. Individuals must refrain from buying sexual services when on assignments and business trips for Arctic.

4.4 Intoxicants

No one should use, or encourage others to use, intoxicants in a manner that can place the user, Arctic or any of its business associates in an unfavorable light.

5 Communications, accounting and records

5.1 Communications

Our communications shall be accurate and correct both internally and externally.

5.2 The Press & Legal questions

General enquiries about Arctic or its employees as well as all enquiries from media should be directed to the CEO of the relevant business unit. Other employees and Board Members needing to make public statements shall co-ordinate these in an appropriate way as stated above.

Enquiries from external attorneys should be passed on to the Arctic legal staff.

5.3 Accounting

All accounting information shall be correct, registered and reproduced in accordance with laws and regulations.

5.4 Maintaining records

Arctic is committed to transparency and accuracy in all its dealings, while respecting its confidentiality obligations. Individuals therefore have a responsibility to maintain necessary records of Arctic's business and business relations. No false or misleading or artificial entries may be made on Arctic's books and records. All transactions must be fully and completely recorded in Arctic's accounting records.

5.5 Information and IT systems

The individual's use of information, IT systems and, in particular, internet services must be governed by the needs of the business and not by personal interests.

Information produced and stored on Arctic's IT systems is regarded as the company's property. Arctic therefore reserves the right to access all such information except where limited by law or agreement.

Please see additional instructions regarding the use of IT systems in the IT Policy in part B of this document.

Individuals are responsible for maintaining electronic files and archives in an orderly manner. Private use is only permitted for the processing of ordinary information to a limited extent. Information that may be considered illegal, offensive or inappropriate must under no circumstances be processed, downloaded, stored or disseminated. Any downloading, storing or disseminating in breach of any copyright law or provision is prohibited. Any use of software in breach of any copyright law or provision is prohibited.

6 Anti-corruption

6.1 Corruption

The prohibition against corruption applies for individuals acting on Arctic's behalf. In case of violations, the Company may be fined and individuals may be fined and/or imprisoned.

The prohibition includes facilitation payments. However, if an individual believes that their own or others' life or health may be in danger, making a payment is not a violation of this prohibition.

Payments must be correctly described in the accounts and reported to your superior.

6.2 Gifts, hospitality and expenses

An individual must not, directly or indirectly, accept gifts except for promotional items of low value normally bearing a company logo. Other gifts may be accepted in situations where it would clearly give offence to refuse, in which case the gift must be handed over immediately to Arctic and will be regarded as Arctic property.

Hospitality such as social events, meals or entertainment may be accepted by the individual if there is a clear business reason. The cost of any hospitality must be kept within reasonable limits.

The above principles also apply in the reverse direction, so that no individual acting on behalf of Arctic may, in their dealings with customers, suppliers and other parties, offer or agree to pay for gifts, or other expenses that would violate these principles.

On special occasions where custom requires it and where there can be no perception of impropriety, the offer or the acceptance of a gift of a higher value than indicated above on behalf of Arctic may be approved.

All matters concerning the acceptance or offer of gifts, hospitality and similar advantages must be discussed and agreed between the individual and their superior.

Occasional attendance at local sporting or social events does not require such agreement, but in order to ensure openness about such attendance, the superior should be informed.

Before responding to an invitation one should consider the Awareness questions for hospitality listed in Appendix A.

6.3 Anti - corruption

Corruption includes bribery and trading in influence. Corruption undermines legitimate business activities, distorts competition, ruins reputations and exposes companies and individuals to risk. Arctic is against all forms of corruption and will make active efforts to ensure that it does not occur in its business activities.

Bribery exists when an attempt is made to influence someone in the conduct of their duties, through the provision of an improper advantage. Trading in influence exists when an improper advantage is provided to someone in order to influence the performance of a third party's duties. Such improper advantage can take different forms, for example cash, objects, credits, discounts, travel, accommodation or services.

The prohibition against bribes and trading in influence applies both to the party giving or offering an improper advantage and to the party, who requests, receives or accepts such advantage. For the matter to be considered illegal, it is sufficient that a demand or an offer of improper advantage is made.

It is not a prerequisite that the improper advantage accrues to the person upon whom an attempt is being made to exercise influence. The prohibition against bribery and trading in influence applies to both the public and private sectors.

Facilitation payments are payments aimed at expediting or securing the provision of products or services to which one has a rightful claim. Arctic is against the use of this type of payment even in cases where it may be legal.

Arctic may be held liable for bribery or any other corruptive acts by third parties contracted by Arctic or in other situations where Arctic may benefit from bribery or corruptive acts by third parties. Arctic shall thus take appropriate steps to reduce such risks.

6.4 Public officials

Arctic should not authorize any gift or payment or offer anything of value to public officials, except as expressly provided in this document or further corruption policies.

Such expenses may include reasonable costs for travel to Arctic premises, accommodation or costs related to training when there is a legitimate purpose in connection to Arctic's relationship with the relevant authorities.

Written approval from the responsible superior must be obtained in advance for all promotional, contract or training related expenditures for the benefit of public officials.

No authorization for coverage of expenses related to public officials may be made if it violates any applicable laws on corruption or the regulations of the public official's employer, or may be perceived by the public as a bribe or improper payment.

6.5 Relations with partners and customers

Arctic will conduct its business in such a way that partners and customers can have trust in Arctic. Partners are expected to adhere to ethical standards which are consistent with Arctic's ethical requirements.

6.6 Use of intermediaries

Intermediaries include agents, consultants and others who, act as links between Arctic and a third party in the company's activities.

Before entering into agreements with intermediaries, the manager in question must ensure that the intermediary's reputation, background and abilities are appropriate and satisfactory.

Agreements with intermediaries shall preferably be made in writing and describe the true relationship between the parties. The agreed compensation must be proportionate to the service rendered. Payments must only be made against satisfactory documentation, and must be accounted for in accordance with generally accepted accounting principles.

The performance of the intermediary relative to Arctic's ethical requirements should be regularly monitored and remedial action taken if performance falls short.

7 Property and confidentiality

7.1 Protection of Arctic's property and assets

The use of Arctic's time, materials, financial assets or facilities for purposes not directly related to Arctic's business is prohibited without authorization from a relevant Arctic representative. An individual must protect Arctic's property and assets against loss, damage and abuse.

7.2 Confidentiality

The duty of confidentiality should prevent unauthorized persons from gaining access to information that may harm Arctic's business or reputation. This duty should also protect individuals' privacy and

integrity. Careful consideration should therefore be given to how, where and with whom Arctic-related matters are discussed, in order to ensure that unauthorized persons do not gain access to internal Arctic information. An individual must comply with the requirements for confidential treatment of all such information, except when disclosure is authorized or required by law.

Confidential or Arctic internal information must not be disclosed to unauthorized personnel in Arctic. This also applies to sensitive information concerning security, individuals, commercial, technical or contractual matters and to information protected by law.

The duty of confidentiality continues to apply after termination of the employment relationship or after an assignment has been completed.

Information, other than general business knowledge and work experience, that becomes known to an individual in connection with the performance of their work shall be regarded as confidential and treated as such.

8 Trading in securities

8.1 Trading in securities

An employee's own trading in financial instruments shall be approved by their superior/compliance in writing. Please note that further internal regulations are implemented for companies within the Arctic group which are subject to statutory requirements

8.2 Insider information

Insider information is information capable of affecting the price of securities and which is not publicly available or generally known to the market.

No individual may use, or contribute to others using, insider information to subscribe for or trade in securities.

9 Responsibilities

9.1 Personal responsibility

Individuals must ensure that they are familiar with and perform their duties in accordance with the requirements set out in this document and applicable laws and regulations.

9.2 Responsibility of supervisors

Managers must ensure that activities within their area of responsibility are carried out in accordance with the requirements set out in this document. Managers are responsible for communicating the requirements and for providing advice with respect to the interpretation and application of the rules.

9.3 Relationship with counterparties

Arctic shall be aware of the risk of entering into relationships with counterparties and shall if deemed necessary perform a due diligence review of its counterparties.

9.4 Breaches of the code of conduct

If an individual comes across cases of ethical doubts or breaches of Arctic's ethical requirements, these concerns must be reported immediately. Individuals can report the concern through the regular channels: to their superior, or to their superior's superior, or to the internal entity whose duty it is to follow up such matters. A manager who receives such a query must consult their own superior in cases of doubt.

Arctic will not implement sanctions in any form against any individual who, in a responsible manner, informs persons in positions of responsibility, internal entities or relevant authorities about possible breaches of Arctic's ethical guidelines, applicable laws or other blameworthy circumstances in Arctic's business.

9.5 Consequences of infringement

Breaches of the company's ethical requirements or relevant statutory provisions may result in disciplinary action, or dismissal with or without notice, and may be reported to the relevant authorities.

10 Whistleblowing

10.1 Procedure

Arctic has an open door policy and encourages employees to share their questions, concerns, suggestions or complaints with their supervisor. If an employee is not comfortable speaking with their supervisor or an employee is not satisfied with the supervisor's response, the employee may speak to the CEO of the relevant entity.

Employees with concerns or complaints may also submit their concerns orally or in writing directly to the organization's compliance department, employee representatives and/or safety officer (verneombud). An employee may also notify the relevant regulatory or public authority or the law firm BAHR att. Peter Hammerich ph@bahr.no, +47 92881389 or Vibeke Svendsby, vks@bahr.no, +47 93454254. Notification about violations or suspected violations may be submitted on a confidential basis by the complainant.

Anyone filing a complaint concerning a violation or suspected violation must be acting in good faith and have reasonable grounds for believing the information disclosed indicates a violation. Arctic has the burden of proving that notice has been in violation of this provision. Retaliation against an employee who notifies in accordance with the above is prohibited. If an employee submits information that gives reason to believe that there has been retaliation in violation of the above, it should be assumed that such retaliation has taken place unless Arctic demonstrates otherwise.

Reports of violations or suspected violations will be kept confidential to the extent possible, consistent with the need to conduct an adequate investigation. The Compliance department will notify the person who submitted a complaint and acknowledge receipt of the reported violation or suspected violation. All reports will be promptly investigated and appropriate corrective action will be taken if warranted by the investigation.

10.2 Accounting and Auditing Matters

Arctic's compliance department shall immediately notify the chairman of the board of the relevant entity of any concerns or complaint regarding corporate accounting practices, internal controls or auditing

Appendix A Questions regarding hospitality

If you are invited to a hospitality event, you should consider the following questions before accepting the invitation.

1. Why am I invited? Is anything expected in return?
2. Has the hospitality/entertainment been approved by my superior?
3. What is the purpose of the hospitality? Is there a business reason to attend?
4. Who will attend the hospitality? Are other companies taking part? Am I the correct person to attend?
5. Are there ongoing negotiations or processes or other matters requiring a particularly careful approach?
6. What is the type of event? Would Arctic offer similar hospitality? Are the costs reasonable and is travel/accommodation covered by Arctic?
7. Am I offered such hospitality regularly by the same host?
9. If spouses or partners are to take part, is there sufficient reason for this and has it been approved by my superior?
10. Has the tax implications of the hospitality event been considered?

B IT Policy

1 Introduction

These instructions consist of requirements and guidelines for use of Arctic's IT systems. The instructions have been prepared for security reasons as well as to secure the rights of Arctic and third parties and to take account of ethical considerations and Arctic's reputation in society.

IT includes, among other things, servers, computers (both stationary and portable), telephones (both fixed and mobile) and other end user equipment, networks, software, data etc. that is made available by Arctic.

2 Use of Arctic's IT facilities

Before a user is given access to Arctic's IT facilities he/she is to study these instructions. An employee is obliged to use Arctic's IT facilities in a careful, professional, legal, ethical and economic manner, and otherwise in accordance with applicable laws and these instructions.

Arctic's IT facilities constitute tools that an employee can use in connection with his/her work for Arctic. This is the case whether an employee works directly on the computer system internally in Arctic or connects to the computer system via a home PC or other external PC.

Arctic permits limited private use of Arctic's IT facilities. Use that is not relevant for work must be kept to a minimum however, and must not under any circumstances be to the detriment of the employee's work for Arctic. Otherwise private use is subject to the same restrictions as apply to use of Arctic's IT in connection with work for Arctic.

3 Username, password, searches and inquiries in the systems

A person who is to use Arctic's IT facilities must have his/her own approved user name and password (user account). The user name and password are strictly personal and access to Arctic's IT facilities is not to be lent to others. This applies to a user account, password and the equipment itself. Unauthorised access, or attempts at the same, is to be notified immediately to the Head of IT of Arctic Securities AS.

A user account (user name/password) gives the right to use specified parts of Arctic's network; the right to log in on specified servers, store and read data from the specified areas and units, obtain printouts on specified printers etc. It is forbidden to go outside, or attempt to go outside these areas. This is the case even if it appears that technically there is access to areas that the user understands or ought to understand that he/she should not have access.

A user must not attempt to obtain unauthorised access to others' data. Users have a duty of confidentiality with regard to personal matters of which they become aware through use of the facilities/network.

4 Storage of data and installation of software

All data is to be stored on common network servers in order to ensure that backup copies of data are made. Data is to be stored with appropriate marking and is to be retained outside Arctic's premises. Sensitive data is only to be stored on the parts of the network that are limited to relevant user groups and files are to be password protected as required. Arctic does not take any responsibility for backup copying of private data. It is strictly forbidden to store Arctic relevant information outside Arctic's approved storage media.

All software is to be cleared with the Head of IT of Arctic Securities AS before installation. The Head of IT of Arctic Securities AS decides who is to install software. Software or data may contain unwanted elements/viruses, and users must contribute to Arctic's facilities being kept free of them. It is not permitted to move/disconnect computer equipment without this being specifically agreed with the Head of IT of Arctic Securities AS.

Private data sharing solutions/systems are not to be used on Arctic's IT facilities. Data sharing solutions/systems provided by business partners can be used after clearing from the Head of IT of Arctic Securities AS.

A virus check must always be carried out on downloaded files before these are brought into use on Arctic's computer system. No software or sound or picture files must be downloaded that are not job related. If an employee suspects that a virus has come into Arctic's computer systems or network, he/she must notify the responsible IT personnel immediately.

Arctic reserves the right in connection with investigation of a possible breach of applicable laws to deliver the content of storage disks, backup tapes and similar to the police or the prosecuting authority, if this is not in conflict with other statutory provisions.

Memory sticks represent a big security risk because they can easily be lost and because viruses and other software can easily be spread. Employees are to be careful in using memory sticks and ensure that sensitive information is not mislaid.

5 Special provisions on the use of the Internet

Each employee is to be aware that he/she is not anonymous on the Internet and that all communication on the net can be traced back to the PC such person uses. The Internet is a worldwide network that provides access to pages with all kinds of information. Many of these pages contain illegal material or material that has a clear sexual, or otherwise immoral or demeaning content. It is therefore of the greatest importance that an employee has a conscious approach to the searches and downloads of material that are made. An employee must be aware that use of the Internet takes place on his/her own responsibility. Arctic has no responsibility for anything with which the employee comes into contact on the Internet through use of Arctic's computer system.

An employee must be particularly careful with regard to what is communicated from the IT system. Display, use, storage or dissemination of announcements, advertisements and invitations, political material, pornographic material, or anything that maybe offensive, indecent, threatening, dishonest or illegal on Arctic's computer system, or from it to the Internet, must not take place.

It is forbidden for an employee to use, download, store or disseminate copy-protected material through Arctic's Internet access without Arctic's prior consent.

The purchase and sale of goods, services, shares, securities etc. that do not have any connection to the employee's work for Arctic must not take place through Arctic's Internet access without Arctic's prior consent.

Breach of copyright and other intangible rights (texts, programs, pictures, films, music), attempts at hacking or other unauthorised access to other information systems, must not take place.

Arctic may, out of consideration for its reputation, or out of consideration for certain persons or groups, block access to certain pages on the Internet if such pages contain illegal and/or demeaning material, or anything that might otherwise be regarded as improper and/or offensive, and which is not job-related.

Arctic needs to maintain control of Arctic's use of computer systems, and will therefore use logs in the computer system as a method for checking that these instructions and applicable laws, including rules made pursuant to law, as well as custom and practice, are observed – something that is important for Arctic and its reputation.

Security logs are reviewed regularly by Arctic. The review takes place at an overall level. In the event of suspicion of a security breach the security logs may be used as a basis for assessing the security breach. With regard to inspection of personal information the method referred to below for inspection in the case of email is to be followed.

6 Special provisions on the use of email

Each employee is to take sufficient care when using email. It is pointed out to employees that email, if not encrypted, can easily become available for third parties.

If Confidential Information is to be shared by email with someone outside Arctic the documents containing the Confidential Information have to be password protected. Passwords are to be shared on other media as e-mail, such as SMS, telephone etc. The documents shall to extent practicable be marked "confidential."

Personal information, i.e. information and assessments that relate to an individual, may only be sent by email to the extent that this is permitted in GDPR or similar laws abroad.

An employee is him/herself responsible for complying with the provisions in GDPR or similar laws on the use of emails. It is pointed out that a breach of these laws may involve orders and possible penalties from the Data Supervisory Authority or similar, or a compensation liability. Deliberate or gross breaches may in addition involve fines and possible imprisonment if the matter is reported to the police.

If an employee receives an email that contains something that is dishonest, demeaning, indecent, threatening or otherwise has a content that is frightening or defamatory, he/she is to delete the email immediately unless it is of such a nature that it should be reported to such person's immediate manager.

If an employee receives an email that contains something that is illegal or damaging for Arctic, its business partners or other employees, such person is immediately to report it to their immediate manager.

Attachments to emails must not be opened if there is any possibility that they contain something that could damage Arctic's IT facilities or that they have a content that means that the email is to be deleted or reported to the recipient's immediate manager.

It is not permitted to start or to transmit chain letters.

In the event of planned absence for more than one day the "out of office assistant" is to be used. In the event of absence, the holder of the email address is responsible for ensuring that business related email is not left unopened at such email address. If an employee does not ensure that business-related email is opened in the employee's absence, Arctic may carry out surveillance of such person's email to search for business related email in line with the routines for this.

7 Handling of email boxes and private files at the end of the employment relationship

On departure an employee is to redeliver to Arctic all information that belongs to Arctic irrespective of the storage medium. It is strictly forbidden to transfer Arctic relevant information to one's own storage media or otherwise to take away Arctic relevant information. If an employee already has

Arctic relevant information on his/her own storage media, this is to be redelivered to Arctic or demonstrably deleted.

Before leaving Arctic an employee is to arrange for relevant information to be transferred to the right person in Arctic. Such person is also responsible for giving any new personal email address to contacts to the extent this is necessary.

All data is stored in accordance with Arctic's routines.

8 Inspection of emails

The purpose of these Instructions' rules on inspection of emails is to ensure that Arctic obtains access to necessary information stored in emails without unnecessarily infringing employees' rights regarding personal data.

Arctic may, on the terms set out below, inspect employees' personal email boxes, i.e. the email box connected to the individual employee which such person has been allocated for use in connection with his/her work for Arctic.

Arctic's inspection right is different for business-related and private email. "Business-related email" is email connected to carrying out work tasks. "Private email" is email with contents of a private nature, for example email to personal contacts, greetings, emails sent to and from a union/professional association, employee representatives and the health service.

In order to decide whether an email is private or business-related a specific evaluation must be made. Emphasis must be placed, among other things, on whether the email is marked "private", or who is the sender and recipient and what is written in the subject field/title.

In order to be able to distinguish between private and business related email, employees are encouraged to mark email with a private content as "private", or to establish a folder marked "private" for this type of email.

When there is a business reason for so doing, for example when it is necessary in order to carry out the business's assignments, Arctic has a right of inspection of business-related email in the employee's personal email box in accordance with guidelines set out below.

In the case of inspection of business-related email the relevant employee will be notified. Such employee may be present during the opening of emails and files. If such employee is absent a representative of the employee or a neutral person is to be present during the opening of the email and files. In such a case the relevant employee is to be given information subsequently on the subject matter of the inspection. If private email is opened by accident, the file is to be closed as soon as possible.

As a starting point Arctic shall not carry out inspection of an employee's private email unless the relevant employee has given consent. In the absence of consent from the employee searches are further not to be made in information marked "private" or grouped in a folder marked "private".

If Arctic has a strong suspicion that there exists a gross breach of duty or other significant fault from the employee's side, including a breach of law or other provisions that it is important for the business to observe, Arctic may nevertheless inspect the relevant person's private email, unless the suspicion can simply be confirmed or allayed in another manner that involves a lesser infringement of the employee's personal data.

The relevant employee him/herself and an employee representative are to be present on the opening of private emails and files unless the employee him/herself does not require this. If such employee

does not wish to be present, or does not wish that an employee representative to be present, a neutral person is to be present to witness how Arctic carries out the inspection. If there would be disproportionate difficulties in notifying the relevant employee and/or giving such employee the opportunity to be present, it is sufficient that the relevant person's employee representative or another representative, possibly a neutral person, is notified and is present when inspection is carried out. In such a case the employee is subsequently to be given information on the matter that is the subject of the inspection.

A record is to be kept of any inspection carried out, where among other things, the evaluations that were the basis for the inspection as well as the procedure, including which emails were opened, are to be documented.

C Personal Data Policy

1 Policy

This Policy describes the Arctic group's standard procedure governing access to and use of personal data.

As part of this Policy, Arctic will comply in all material respects with the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR") and implementing legislation enacted by the member states of the European Union with respect to its operations in those member states.

The personal data policy applies to Arctic Securities AS and its subsidiaries (including partly owned subsidiaries where Arctic Securities AS directly or indirectly controls more than 50% of the voting interest). The personal data policy further applies to other companies in the Arctic group, to which Arctic Securities AS provides IT-services. The term "Arctic" refers herein to any company within the Arctic group.

Further requirements may apply for companies localized outside the EEA. If anything in the personal data policy is in conflict with local mandatory laws or regulations, the latter shall prevail. The local CEOs will be responsible for assessing and complying with local regulations regarding the processing of personal data.

The personal data policy applies to all processing of personal data in the Arctic group. In addition, third parties such as customers, contractors and others shall benefit from the rights granted to them herein.

2 Responsibility

The Head of Operations of Arctic Securities AS is responsible for ensuring that the personal data policy is applied in Arctic Securities AS. Each CEO of other companies in the Arctic group is responsible for the implementation of the personal data policy. All employees are responsible for adhering to this policy.

Each company of the Arctic group is responsible for ensuring that their business is conducted in compliance with the personal data policy. This includes the responsibility for ensuring the establishment and maintenance of internal control procedures as set forth herein.

3 Personal Data

Personal data means any information that may be related to an identified or identifiable individual. An identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal data includes all types of information that directly or indirectly may be linked to a person.

The Arctic group processes the following main categories of Personal data, both concerning employees and third parties:

- General contact information: (e.g. name, address, email address, phone number, picture, date of birth etc.)
- Key information necessary for employment management, e.g. salary information, CV, education level, performance reviews, recruitment information, bank account number, details of next of kin etc.)
- Registration of hours worked, absences, holiday, overtime
- Records of compulsory training

- Employment history: e.g. start date, company and corporate seniority, job grade, position, organizational unit (department), immediate superior, contract details, employee type, job location, leaving date etc.
- Other employee data for statistical purposes: (e.g. gender, nationality, age)
- Customer information (e.g. name, address, email address, phone number, picture etc.)
- Sub-contractor's information (e.g. name, address, email address, phone number, picture etc.)
- IT-related information (electronic logs regarding a person's use of IT-resources, user profile/account information etc.)
- An IP address is deemed as personal data as long as the IP address in conjunction with additional information (such as an internet provider's billing information) can identify the individual using the IP address.
- Encrypted information is also deemed to be personal data if the information can be made readable and therefore identifies an individual.

The processing of personal data has the following main purposes:

- Maintain contact information
- Employee administration
- Customer administration
- Sub-contractors administration
- IT administration and information security administration
- Authentication and authorization
- Physical security
- Administration of IT-costs per employee
- CRM-information for marketing purposes
- Reporting and compliance purposes
- Registration and reporting of HSE related information (e.g. incidents, issues etc)
- Support for the recruitment process (e.g. registering applications and CVs etc)
- Use as a collaboration tool for internal projects and organizational teams and activities (e.g. document and content management)

4 Criteria for making data processing legitimate

Personal data shall be processed fairly, lawfully and pursuant to the principles stipulated in the personal data policy. This means that personal data shall be processed in accordance with law, and that the legitimate interests of the data subject should be taken into account when processing personal data.

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Personal data can only be processed if at least one of the following applies:

- The data subject gives his/her consent.
- The processing is required by law.
- The processing is necessary:
    - to fulfil an agreement with the data subject or to take steps at the request of the data subject before entering such an agreement;
    - to comply with a legal obligation;
    - to preserve the data subject's vital interests;
    - to perform a task in the public interest;
    - to exercise public authority; or
    - for Arctic or a third party to whom the data is transferred to preserve a legitimate interest which exceeds the interest of the data subject's right to privacy.

Pursuant to Art. 6 (1)(f) of GDPR, where processing of personal data is necessary for Arctic or a third party to whom the data is transferred to preserve a legitimate interest which exceeds the interest of the data subject's right to privacy, Arctic believes it is reasonable to expect that prospects that have submitted their contact details to the company, are happy for the company to collect and otherwise use their personal data to offer its services to the prospects.

To ensure that Arctic provides the best service possible to its clients, it stores their personal data and/or the personal data of individual contacts at their organisation. Arctic also keeps records of client conversations, meetings and marketing activities. Arctic believes this is reasonable and deems these uses of the client's data to be necessary for its legitimate interests when providing its services to the client.

Arctic uses and stores the personal data of individuals within suppliers' organisations in order to facilitate the receipt of services from such suppliers. It deems all such activities to be necessary within the range of its legitimate interests as a recipient of its supplier's services.

Arctic shall use personal data only for purposes that are compatible with the original purpose of the collection and are objectively justified by the activities of Arctic (unless the consent of the data subject is obtained for the new purpose).

Below is a list of categories of personal data Arctic may collect. Please note that the list is not exhaustive and that the information described below is in addition to any personal data Arctic is required by law to process in any given situation:

- Prospect Data: Full name, Job title, Email address, Company name, Phone number, Contact details, Extra information that may be provided, the dates, times and frequency of interaction with Arctic.

- Client data:
  - Personal data received from the client such as name, date of birth, address and other contact details, settlement information and instructions, and information received from the client in order to perform Arctic's KYC-obligations.
  - Information received from the client in either written or verbal format, regarding the client's relationship, client agreement and/or transactions with Arctic or others.
  - Information regarding the client's interactions with Arctic and client's usage of its services; including trading activity and information gathered via online data gathering tools.
  - Recorded telephone conversations where Arctic provides investment services to Arctic's clients. (Arctic records all conversations with its clients).
  - Arctic use cookies to support the operation of its Web site, Research Web, LEI-services and Onboarding application (https://www.arctic.com/secno/en/cookies). Arctic collects and saves information about its clients' activities, including date and time of visits, pages viewed and which browser and device type the client uses.
- Supplier data: Arctic will collect the details for its contacts within suppliers' organisations, such as names, telephone numbers and email addresses. Arctic's calls with a supplier may be recorded and retained, depending on the applicable local laws and requirements.

5 Processing of special categories of data (Sensitive Data)

It is prohibited to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

The special categories of data mentioned above may only be processed if:

- The data subject has given his/her explicit consent to the processing of those data, except where the local laws applicable provide that the prohibition above may not be lifted by the data subject's giving such consent; or

- Processing is necessary for the purposes of carrying out the obligations and specific rights of Arctic according to employment, tax or securities law in so far as it is authorized by local law providing for adequate safeguards; or

- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent.

6 Arctic as main data processor

Arctic Securities AS operates and delivers IT services, finance, HR and administration management services to most companies within the Arctic group. When providing such services Arctic Securities AS regularly processes personal data on behalf of the other Arctic group companies.

As a general rule each Arctic group company will thus be considered a controller deciding the means and purposes for the processing, while Arctic Securities AS will be the processor which processes data on behalf of the Arctic group companies. Each of the Arctic group companies has entered into an agreement with Arctic Securities AS for intra group services, that regulates processing of data.

During the performance of its tasks as processor for the Arctic group companies, Arctic Securities AS is obliged to treat each Arctic group company as an independent entity and to keep the respective personal data adequately and securely separated.

In a situation where Arctic uses a subcontractor, Arctic is responsible for ensuring that the legal grounds for the transfer of the personal data are in place. Parties who have access to, or a role in relation to, the information system, shall sign a declaration of confidentiality. Any third parties that process personal data on behalf of Arctic shall enter into a data processor agreement.

7 Data quality and proportionality

Personal data shall be:

- adequate, relevant and not excessive in relation to the purposes for which they are collected and /or further processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

The Head of Operations of Arctic Securities AS and the local CEO's of the Arctic group companies have overall responsibility for the personal data being as correct and up-to-date as possible in relation to the purpose of the processing.

8 Security objectives

Appropriate technical and organizational measures shall be implemented to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Arctic Securities AS must, where processing is carried out on its behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred above shall be in writing or in another equivalent form.

Examples of events that Arctic wishes to prevent:

- Events involving a breach of confidentiality, integrity and availability, including:
    - A break-in to the business's premises or network
    - Third parties' use of user accounts
    - An attack by a computer virus or other malware
- Breach of confidentiality (personal information is lost), including:
    - Loss of portable equipment
    - Loss of a storage medium
    - Printouts left on a printer
    - Unintended delivery of employee information via email
- Breach of integrity (personal information is changed), including:
    - Different versions of documents
    - Incorrect registration
- Breach of availability (personal information is not available), including:
    - Network or system is not in operation
    - Fire, water damage and power cut
    - Vandalism
    - Service attack (Denial of service)

9 Security strategies

Third parties shall not to have physical access to personal information or equipment on which this is stored.

Personal information about employees and customers shall only be available internally for employees who need it as part of their work, for example department managers and personnel staff.

In the event of a need for prioritisation, protection of employee information has a higher priority than customer information.

Access control shall ensure that access to information about employees and customers shall be limited to those who have a need for it.

The IT network shall be protected against intrusion from external networks by firewalls that only allow through necessary data traffic. The IT network shall be protected against use by third parties, for example by securing wireless networks.

Extra measures, beyond measures based on the security strategies above, shall be implemented for information that requires special protection such as:

- Sick notes.
- Information on the arrangement of the workplace.
- Employee assessments.
- Remarks and warnings.

10 Access to Personal Data

Arctic will allow the subjects of the registration reasonable access to personal data about themselves during normal working hours and upon reasonable request, and will be allowed to update and/or correct any inaccurate information.

Employees may request a printout of all information that is stored about the relevant person. Customers on making a request are to be sent a printout of all information that is stored about the relevant person. Such inspection and/or printouts are to be given without undue delay and at the latest within 30 days of the request being received. The request may be oral, but Arctic may require a written request in order to be able to document the response time.

Employees and employee representatives can only inspect sound recordings of customer orders or indications of customer orders if execution of the service makes this is necessary.

Requests for inspection are to be passed to the Head of Operations of Arctic or the CEO of other Arctic group companies.

11 Deletion of Personal Data

Personal information shall be deleted when there is no longer a business need to retain it. Arctic shall ensure that no more personal information about customers is stored than is necessary for the purpose.

When assessing the need to retain the information Arctic shall take into consideration whether the information may become useful in the event of a lawsuit or if the client has entered into long-term agreements that still may be in force, such as if Arctic is responsible as the investor account operator in VPS etc.

The following principles for deletion shall apply:

- There are back-up systems on the servers operated by Arctic, which will retain the information for 10 years after deletion. The IT department will after deletion have to obtain back-up material from an external supplier.
- Personal information related to a customer relationship is to be deleted after 10 years' inactivity in the customer relationship. However, the data may not be deleted if the client holds an account with Arctic, but is not using it; e.g. an account in VPS.

- Folders on corporate finance projects containing mandate agreements, insider lists etc. shall be deleted after ten years from completion of the project.
- Recording of telephone conversations and text messages will be deleted:
  - After five years if the conversation took place by cell phone.
  - After ten years if the conversation took place by office phone.
- Chat on Reuters, Bloomberg will be deleted after five years.
- E-mail will be deleted after fifteen years.
- Accounting material shall be kept for a minimum of 10 years.
- Information about applicants to a position shall be deleted when the application process has ended.
- One year after termination of the employment relationship Arctic shall make an assessment of the need to store the information about an employee. The information shall be deleted within five years of termination unless there is a need to retain the information on file.
- Personal information about employees that is not relevant for administration of the employment relationship shall not be stored.

12 Electronic communications (cookies)

Electronic communications networks cannot be used for the storage of information on the user's communications equipment or to obtain access to such information, unless the user is both informed and provided information on the purpose of the processing and given an opportunity to object to the processing. However, this does not apply to technical storage or access to information, which is either exclusively for the purpose of transmitting or facilitating the transmission of communications on an electronic communications network, or necessary to provide an information society service at the user's express request.

13 Transfer of Personal Data – Data Processor Agreements

A transfer of personal data to third parties shall only take place in compliance with local laws and regulations. Any third parties that process personal data on behalf of Arctic shall enter into a data processor agreement.

The Head of Operations and the local CEOs shall as part of the yearly review prepare a list of the parties that process data on behalf of Arctic.

14 Information to registered employees and customers

When collecting personal data Arctic must inform the data subject of

- the name and address of the company responsible for the data processing.
- the purpose of the processing.
- whether the data will be disclosed and the identity of the recipient(s), if applicable.
- the fact that the provision of data is voluntary.
- any other information that will enable the data subject to exercise his/her rights pursuant to the personal data legislation in the best possible way, including information on the right to demand access to data and the right to demand that data be rectified.

Persons applying for a position and other relevant candidates for an appointment are to be informed

in the interview about Arctic's policy and the information that may be stored about the employee during the employment relationship, about the right of inspection and the right to have data corrected and added to.

Customers are informed about the storage of personal information in connection with an agreement on services and have an opportunity to make reservations against such storage within the limits permitted by the law and regulations.

15 Corrections and additions

Personal information about employees and customers is to be sufficient and relevant for the purpose of the processing. The requirement as to relevance sets an outer limit for the personal information that can be included in such processing and cannot be waived by consent from the registered person. The requirement as to sufficiency means that one must have enough information in order to be able to carry out the purpose of the processing.

When processing personal information that is incorrect, incomplete or which it is not permitted to handle, Arctic shall at the request of the registered person correct the relevant error.

The following routines shall be followed when processing requests for correction and addition:

- Receipt of the request for correction or addition for an employee or customer is to be registered in writing.
- The request is to be communicated to the head of the unit to which it relates.
- The Head of Operations shall verify the accuracy of the requested changes in information.
- If the changes are verified work orders are to be issued for updating the relevant system(s).

16 Complaints & Deviations

Employees and third party beneficiaries may contact the Head of Operations of Arctic Securities AS or the local CEOs of the Arctic group companies with inquiries or compliance questions regarding processing of personal data.

Security breaches and any use of the information system that is contrary to established routines are considered to be a deviation. Arctic must take steps to re-establish the normal state of affairs, eliminate the cause of the deviation and prevent its recurrence. If the deviation has resulted in the unauthorised disclosure of personal data for which confidentiality is necessary, the Data Inspectorate must be notified.

17 Internal control - Yearly review

Arctic uses a self-assessment approach to assure compliance with this personal data policy and periodically verifies that the policy is accurate, comprehensive with respect to the information intended to be covered, prominently displayed, completely implemented and accessible. Arctic shall maintain an overview of personal information that is processed in Arctic and all of the Arctic group companies.

Each year the Head of Operations shall prepare, convene and document the results from a review of internal control and information security on a group level. The review may be performed by compliance or the internal audit function.

18 Contact information

Please contact one of the following group companies if you have any questions concerning Arctic's data processing or this Personal Data Policy:

Arctic Securities AS	Dataprotection.ASecurities@arctic.com
Arctic Fund Management AS	Dataprotection.AFM@arctic.com
Arctic Insurance AS	Dataprotection.AInsurance@arctic.com
Arctic Capital AS	Dataprotection.ACapital@arctic.com
Arctic Business Management AS	Dataprotection.ABM@arctic.com
Arctic Offshore International AS	Dataprotection.AOffshore@arctic.com
Arctic Shipping AS	Dataprotection.AShipping@arctic.com
Arctic Real Estate Development AS	Dataprotection.ARED@arctic.com