Arctic Group Policies

16. December 2021

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.

In certain circumstances Arctic may transfer personal data to companies or organisations outside the European Economic Area (EEA). Arctic will only transfer data outside of EEA if compliant with data protection legislation and the means of transfer provides adequate safeguards in relation to customers' data, for example:

– transferring data to a country where there has been a finding of adequacy by the European Commission in respect of that country's levels of data protection via its legislation;

– by way of data transfer agreement, incorporating the current standard contractual clauses adopted by the European Commission; or

– where it is necessary for the conclusion or performance of a contract between Arctic and a third party and the transfer is in the customer's interests for the purposes of that contract; or

– where the customer has consented to the data transfer.

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 Securities AS, Sweden Branch	Dataprotection.ASecurities. Swed@arctic.com
Arctic Securities LLC	Dataprotection.ASecurities.LLC@arctic.com
Arctic Asset 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 Offshore Rig AS	Dataprotection.AOffshore.Rig@arctic.com
Arctic Shipping AS	Dataprotection.AShipping@arctic.com
Arctic Real Estate Development	Dataprotection.ARED@arctic.com
Arctic Alternative Investments Management AS	Dataprotection.AAIM@arctic.com
Ursus Real Estate Management AS	Dataprotection.Ursus@arctic.com
Cleanworld AS	Dataprotection.Cleanworld@arctic.com