Internal Privacy Policy

B & P Fund Services AB

Adopted by:	The Board of Directors of B & P Fund Services AB
Date:	18 January 2019
Replaces (if any):	Internal Privacy Policy, 17 May 2018
Content owner:	Data Protection Manager
Info. security classification:	Public

Update and approval

This Privacy Policy shall be updated annually or, if deemed necessary, whenever there is a need or requirement to do so. This instruction shall be updated in respect of changes within the privacy field, other regulatory changes, changes in the market where the company operates, and internal changes within the company. Any changes to this Privacy Policy is subject to approval by the Board of Directors.

Table of contents

1. Introduction

This Privacy Policy has been adopted by B & P Fund Services AB (the "**Company**" or "**we**").

Our aim is to ensure that all personal data processed by us should be kept safe and secured at all times and that the personal integrity is respected.

This Privacy Policy sets out how we seek to protect personal data and ensure that our personnel understand the rules governing their use of personal data to which they have access in the course of their work.

In particular, the Privacy Policy sets out certain basic principles that we and our employees and hired consultants must follow when processing personal data (Section 8), and contains an instruction on what our employees and consultants shall consider in this regard (Section 9).

Further, the Privacy Policy contains information to all our employees and consultants about our processing of their personal data (Section 10).

Therefore, as an employee or consultant, you should carefully read this Privacy Policy to learn what we expect from you when you process personal data in your employment with or assignment for us and how we process your personal data within our business.

We process personal data in accordance with the general data protection regulation ("**GDPR**")[1] and all relevant local laws on data protection.

Please note that this Privacy Policy requires all personnel to ensure that the Data Protection Manager (DPM) be consulted before any significant new data processing activity is initiated to ensure that relevant data protection compliance steps are properly addressed, and if applicable that a Privacy Impact Assessment is undertaken.

2. To whom does this policy apply

This Privacy Policy applies to all our personnel[2] and consultants. You must read, understand and comply with this Privacy Policy when processing Personal Data on our behalf. Your compliance with this Privacy Policy is mandatory.

[1] 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).

[2] For the purpose of this Privacy Policy, the terms “personnel” and “employees” shall be deemed to include all equivalent terms such as for example “workers” under UK law.

3. Who is responsible for this policy on a day-to-day basis

Our Data Protection Manager (DPM) has the overall responsibility for the day-to-day implementation of this Privacy Policy.

4. Contact Information

If you have any questions about this Privacy Policy or regarding the processing of your personal data or if you wish to exercise any of your rights under applicable data protection regulation, you may contact our Data Protection Manager (DPM). On the date of the adoption of this policy our DPM is:

Fredrik Stjernström, Head of Legal, B & P Fund Services AB
fredrik.stjernstrom@brummer.se, phone: +46 761 111405

If you would have any questions of a general nature you may come in contact with the data privacy team on email: DataProtection@brummer.se.

5. Roles and Responsibilities

Data protection manager (DPM): The DPM shall follow-up on the compliance with the GDPR on a Company group level. The DPM shall also advice the Company's management on GDPR and Data Protection matters and shall be responsible for coordinating governance within the Privacy Field together with the Contact Persons of individual business areas and support functions (see below). As part hereof, the DPM shall ensure that personal data processing records are maintained, that agreement templates, group routines etc., are updated for use by the group entities and that a central training program is available within the Company group. The DPM shall coordinate with the Chief Technology Officer in respect of any technical aspects within the Privacy Field.

Contact Persons: A Contact Person shall be appointed for each business unit and group support function. The Contact Person is the point of contact for the DPM and individuals in privacy matters relating to the individual business unit or support function. The Contact Person shall report to the DPM on a regular basis (as further agreed between the DPM and the Contact Person) and shall immediately notify the DPM of any processing activities in violation of the GDPR, local legislation or governing documents.

Compliance: The Company has a separate Compliance function, which operates independently of the Company's other operations. The Compliance function ensures compliance with applicable rules and regulations, including those within the Privacy Field.

Internal Audit: The Company has established an Internal Audit function that is separate and independent from the Company's other activities. The Internal Audit function may perform audits within the Privacy Field as deemed appropriate from time to time.

6. Data Security

Data Security is a high-priority for us. We will at all times ensure that personal data are kept secure, both against external threats and internal threats. Please see our Intranet for further policies and procedures relating to Data Security.

7. Concepts

A number of concepts that are key to the processing of personal data and therefore important to be aware of, are set out below:

Consent	Means that the data subject agrees by a statement or positive action to the processing of his or her personal data by a clear affirmative act that is freely given, specific, informed and unambiguous.
Data controller	Means the legal entity that decides the purpose and means of a certain kind of processing of personal data.
Data processor	Means a legal entity who processes personal data on behalf of the controller, i.e. not for its own purposes.
Data subject	Means the natural living identified or identifiable person about whom we hold Personal data.
Personal data	Means any information relating to a data subject that we can identify (directly or indirectly) from that data alone or in a combination with other identifiers we possess or can reasonably access, e.g. name, address, birth date, employee number, photographs, IP address, information about education, training, role and salary, sickness and leave records, health data, online activities, KYC and AML information.
Processing	Means any operation or set of operations performed on personal data, whether or not by automated means, e.g. collection, recording, organisation, storage, adaptation or alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment or combination, blocking, erasure or destruction.
Special categories of personal data	Means personal data revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, data concerning health or a person's sex life or sexual orientation, biometric or genetic data, and Personal data relating to criminal convictions and offences.

8. General Principles

8.1 SUMMARY OF PRINCIPLES UNDER THE GDPR

We adhere to the principles relating to the Processing of Personal Data as set out in the GDPR which require Personal data to be:

- Processed lawfully, fairly and in a transparent manner;
- Collected only for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed;
- Accurate and where necessary kept up to date;
- Not kept in a form which permits identification of Data Subjects for longer than necessary for the purposes for which the data is Processed;
- Processed in a manner that ensures security using appropriate technical and organisational measures to protect against unlawful or unauthorised Processing and against accidental loss, destruction or damage;
- Not transferred to other countries without appropriate safeguards being in place; and
- Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data.

8.2 ACCOUNTABILITY

We shall implement, comply with and apply this Privacy Policy. Further, we shall carry out the training, monitoring, auditing and other compliance activities related to the areas of data privacy, as described in this Privacy Policy.

8.3 LAWFULNESS OF THE PROCESSING

Each processing activity requires a legal basis. We will only collect, Process and share Personal data fairly and lawfully and for specified purposes. Typically, we process personal data when it is necessary (i) for the performance of a contract with the data subject or to fulfil a request from the data subject, or (ii) to comply with a legal or regulatory obligation. Personal data may also be processed when it is necessary for the purposes of a legitimate interest, including such as to maintain our operational security and to manage risks. If a certain data process requires the prior consent by the data subject, we will collect such consent before carrying out the relevant processing activity. We will document in our records of processing activities (the IT Tool DPOrganizer) the legal basis relied upon for each Processing activity.

Special categories of personal data may only be processed if the data subject has given his or her explicit consent. If consent has not been given, special categories of personal data may, in principle, only be processed if it is necessary to exercise employment law rights or obligations or to justify a legal claim. Social security numbers[3] shall only be processed in exceptional cases when it is necessary in respect of (i) the purpose, (ii) the importance of secure identification or (iii) another important reason.

8.4 INFORMATION TO THE DATA SUBJECTS ABOUT THE PROCESSING OF THEIR PERSONAL DATA

A person whose data is to be processed, has the right to receive certain information before the processing activity is carried out. Such information shall include e.g. the identity of the data controller, the purposes of the processing and the legal basis, any recipients of the personal data and intentions to transfer the data outside EU/EEA.

We process personal data relating to for example: employees, consultants, private customers (individuals) and representatives of institutional customers, distributors, counterparties and suppliers as well as the general public (e.g. visitors at our external websites). Information on processing activities relating to you as an employee or consultant, is set forth in Section 10 in this Privacy Policy. Other categories of data subjects are informed by policies and information provided through available interfaces.

8.5 PURPOSE LIMITATION AND DATA MINIMIZATION, QUALITY AND ACCURACY

Personal data shall only be processed for a specified, explicit and legitimate purpose. Only personal data that are necessary for the specified purpose may be processed. If a purpose changes over time, it shall be considered as a new processing activity that requires a separate legal basis.

Further, personal data shall be adequate, relevant, accurate, up to date and limited to what is necessary in relation to the purposes for which it is collected. It must not be processed further in a manner incompatible with those purposes. Therefore, in addition to the deletion routines (see Section 8.6), we shall ensure that we use reliable sources when collecting the data and we will not collect excessive data. Where relevant, we will allow the data subject to update his/her own personal data. See also Section 8.7 regarding the measures implemented from a privacy by design perspective to avoid that data is processed which is not relevant for the specified purpose.

8.6 STORAGE LIMITATION

Personal data shall not be processed for a longer period than necessary for the purposes for which the personal data was collected. Therefore, we have adopted the routines set out

[3] Note: this would not include for example UK national insurance numbers.

in Section 14 and the guidelines set out in Schedule 1, specifying how personal data shall be erased when the purpose of the processing of the personal data has been fulfilled. We will maintain retention policies and ensure that Data subjects are informed of the period for which data is stored and/or how that period is determined.

8.7 INTEGRITY AND CONFIDENTIALITY, INCLUDING DATA PROTECTION BY DESIGN AND DEFAULT

To ensure appropriate integrity, confidentiality and security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, the Company has implemented certain security measures, including requirements on data protection by design and default, which we are required to comply with. Those security measures shall be applied in the procurement, development, production and maintenance as well as the sun-setting of systems (whether operated internally or procured as a service).

Also, we have established a routine for notification to the supervisory authorities in case of data breaches as well as routines for carrying out risk assessments and data protection impact assessments.

8.8 DATA TRANSFERS WITHIN OUR ORGANIZATION AND/OR OUTSIDE OF THE EU/EEA

When personal data is processed by a data processor on behalf of a data controller, a written data processing agreement (DPA) needs to be concluded between the data controller and data processor. When we act as a data controller, we shall ensure that relevant DPAs are entered into with data processors (within or outside of our organization) that will process personal data on our behalf.

Furthermore, personal data may not be transferred from the EU to countries outside of the EU/EEA, unless an available derogation is applicable to such transfer. Before transferring any personal data outside of the EU/EEA (within or outside of our organization), we shall ensure that at least one of the derogations are applicable, e.g. by ensuring that the standard contractual clauses issued by the EU Commission are entered into with the entity receiving the personal data.

8.9 WHERE WE ACT AS DATA PROCESSOR

Where we process personal data on behalf of another entity, i.e. acts as a data processor, we must:

- Only act on the controller's documented instructions.
- Impose confidentiality obligations on all personnel who process the relevant data.
- Ensure the security of the personal data that we process.

- Follow the rules regarding appointment of sub-processors.
- Implement measures to assist the controller in complying with the rights of data subjects.
- At the controller's election, either return or destroy the personal data at the end of the relationship.
- Provide the controller with all information necessary to demonstrate compliance with the data protection regulation.

8.10 THE RIGHTS OF THE DATA SUBJECTS

Data subjects have certain rights, as are further detailed in the applicable data protection legislation. These rights are (i) a right to access (a record that shows, *inter alia*, what data is being processed about him/her), (ii) rectification, (iii) erasure (right to be forgotten), (iv) restriction of processing, (v) portability, (vi) objection and (vii) a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly affects him/her. Data subjects may contact us to exercise these rights.

9. Instructions to you as an employee or consultant

9.1 INSTRUCTIONS APPLICABLE TO ALL EMPLOYEES AND CONSULTANTS

As an employee or consultant, you shall comply with the following instructions when you process personal data in your employment with or assignment for us:

- Consider the principles, described above in Section 8, on how personal data may be processed and keep them in mind when you process personal data.
- Keep in mind that "processing" of personal data is every operation or set of operations performed on personal data, both those performed automatically and manually, e.g. collecting, storing, reading, generating, changing and deleting personal data.
- Limit the collection and processing of personal data, do not collect personal data that are "nice to have" but only what you "need to have" for the specific purpose.
- Limit the processing of special categories of personal data (as defined above), such as information on health and ethnic origin.
- Only use social security numbers when it is necessary for a secure identification or another important reason (and necessary for the purpose of the processing).
- Make sure that the persons whose data you process have been informed about the contemplated processing. Contact the Contact Person if in doubt.

- Make sure that there is a legal basis to process the personal data in the manner you intend. Contact the Contact Person if in doubt.
- Make sure that the personal data that you process is correct and up to date.
- Maintain the information security for the personal data that you use or are responsible for, e.g. by using complex passwords and locking your computer when you leave it unattended.
- Erase personal data that you have stored on your computer which are no longer necessary to process taking into account the purpose for which they were collected.
- Your job computer and email account are the firm's property and should be used as relevant for your work. To a limited extent and within reason, they may be used for private purposes. However, if you use those for private purposes, the Company will treat any such private files or emails as data belonging to the Company and that data will be treated and delated in the same manner as other data belonging to the Company, as there is no reasonable manner in which the Company can distinguish between your data and other data belonging to the Company.
- Only share personal data to colleagues which are authorised and in need to have them.
- Make sure personal data processing agreements (and data transfer agreements) are in place with service providers that have access to personal data when providing its services to us.
- If you are involved in the procurement of IT systems/services where personal data will be processed, keep in mind to include requirements on the system/service that will make it possible to restrict access, protect and erase personal data. Also ensure that you are informed of any sub-contractor of the service provider that will process the personal data and where the personal data will be processed. Pay particular attention to privacy requirements when procuring or using cloud services.
- Please also refer to our Vendor Management Process which includes several requirements in respect of privacy matters where we on-board new vendors.
- All our employees and consultants are expected to participate in GDPR and information security training. You will find more information about available courses on our Intranet.

9.2 WHAT TO CONSIDER WITHIN A CRM AND MARKETING COMMUNICATION CONTEXT

Legal Framework

The GDPR applies to the collection and processing of personal data for the purpose of managing customer relationships. It also applies to direct marketing activities, i.e. marketing communication directed to selected recipients, e.g. by means of e-mails or postal mails to professionals in a certain geographical area.

In addition to the GDPR, direct marketing activities are also subject to marketing legislation, which may be different in different countries, and could for instance include requirements to obtain consent prior to sending email marketing or to include the source in the mail from which the contact details were acquired.

Furthermore, the collection of data by means of cookies (e.g. used for presenting banners to website visitors) is, in addition to the GDPR, regulated by separate e-privacy legislation within the EU, which requires that the individual has consented to the use of cookies.

Instructions

As an employee or consultant working within a CRM and marketing communication context, you shall comply with the following instructions when you process personal data in your employment with or assignment for us:

- Prior to acquiring data from a third party (such as lists of contact details acquired from suppliers of such information), make sure that the third party provider confirms that it has obtained the data lawfully and has the right to provide the data to us for marketing purposes.
- When collecting data from individuals by means of placing a cookie on the individual's device, make sure that the individual has been informed of and consented to the use of cookies.
- When using information collected by means of cookies, make sure that you only use the information in accordance with the consent from the individual (e.g. for the purposes covered by the consent).
- Be careful of what information you include in a CRM system – unless the information is harmless, the individual's consent may be required for including and using the information. In particular avoid the following:
    - large amount of, or categories of, personal data which go beyond what is necessary for managing an existing customer relationship or for pursuing a potential customer. Strive to limit the data in respect of potential customers to contact details and work-related data (e.g. job email addresses);

- information obtained from publicly available sources which has not been published for marketing purposes, e.g. information from public Facebook profiles, discussion forum, etc.; and/or
- data revealing political opinions, religious beliefs, trade union membership, data concerning health or sex life/sexual orientation or other special categories of personal data.

- Make sure to use drop-down lists and other predefined options when available in the CRM system (and other systems) instead of adding personal data in text boxes.
- Prior to contacting a possible customer, consider whether the individual needs to have consented to being contacted from a marketing law perspective. Typically, consent is required when sending marketing material via email, unless you send it to his/her job email and the material is relevant in his/her professional role.

10. Our processing of your personal data as an employee or consultant

10.1 WHAT PERSONAL DATA IS PROSESSED?

In respect of you as an employee or consultant, we will typically process the following categories of personal data about you: employee number, social security number, photos, address and other contact details, including telephone numbers, email addresses and IP addresses of your computer, bank account number, payroll data, the terms of your contract with us, data linked to your position such as e.g. role, job description, hours worked, training and courses completed, closely related and absence data. User ID and log files are used for security purposes to protect personal data and other information held in our IT systems/services.

For more detailed information on the personal data we process in relation to our employees and consultants, you may ask to obtain an extract from the records of our processing activities, the IT Tool DPOrganizer.

At some entrances and reception areas, we use surveillance cameras 24/7 for security reasons, e.g. to prevent, detect and investigate security incidents, injuries and physical damages. There will be signs of surveillance cameras posted in these areas.

Some of the personal data that we request from you may be "mandatory" to provide for statutory, contractual, administrative, technical or similar reasons.

10.2 WHAT ARE THE PURPOSES FOR THE PROCESSING OF YOUR PERSONAL DATA?

The purpose of our processing is to enable us to plan, organise, manage, monitor and quality assess work, protect you and our colleagues and customers' integrity, protect our

information, administer and fulfil our obligations in employment terms and conditions or the consultant contract with you and to meet our other contractual or statutory obligations by law and by collective agreements, both in relation to you as an employee/consultant and towards the relevant data inspection authority and other authorities.

Processing is also done for reporting purposes and to produce statistics, such as number of employees over time, gender balance and payroll statistics. Personal data are also processed in connection with the operations, management, development and testing of our IT systems.

10.3 WHEN IS YOUR PERSONAL DATA DELETED?

We will process your personal data for as long as it is necessary for the purposes for which it was initially collected. When an employment or consultancy relationship terminates, there is normally no reason to keep the personal data other than in accordance with our standard document retention periods, and it will therefore be deleted once those periods have expired.

10.4 WHAT IS THE LEGAL BASIS FOR THE PROCESSING OF YOUR PERSONAL DATA?

We will always process your data in accordance with applicable law. The majority of the data processed is for the purpose of fulfilling legal obligations whether under your employment contract or laws and regulations. Some processing activities are based on a balance of interests, e.g. processing for the purpose of operational risk management and IT security. If your explicit consent is necessary for a certain processing activity, we will collect such consent before we begin that activity.

10.5 TO WHOM DO WE TRANSFER OR DISCLOSE YOUR PERSONAL DATA?

Your personal data will only be transferred to others if there is a legal basis for it. We may engage third parties for the provision of services to us, including IT-systems, services and other activities. Your data may be shared with and processed by such service providers on behalf of us as required for the provision of the services to us.

We will enter into a data processing agreement with any data processor processing data on our behalf. If relevant, in relation to transfer to any third parties and to our affiliates located outside of the EU/EEA a data transfer agreement based on standard contractual clauses issued by the EU Commission, will be entered into.

Personal data may be disclosed to a third party if we are required to do so according to applicable laws and regulations or in order to detect and prevent fraud or other security or technical problems. Additionally, we may disclose your data to a third party as required in order to provide employment benefits to you that you are entitled under your employment agreement with us.

10.6 ACCESS TO EMAIL ACCOUNTS AND COMPUTER USAGE

We can access the work email accounts of our employees as well as their work computer usage. The reason for this is to allow us to investigate and prevent disloyal or criminal behavior which may cause harm to us or our customers or employees. We will access any email accounts and computers with caution and only after careful consideration, including following a certain internal approval process. This processing activity is based on our legitimate interest.

10.7 YOUR RIGHTS UNDER APPLICABLE LEGISLATION

You have certain rights under applicable law in relation to the processing of your personal data (see Section 8.10). If you wish to exercise any of these rights, please send a written request to the DPM.

You have also the right to file a complaint with a supervisory authority if you believe your personal data has been processed in violation of applicable data protection regulation.

11. Records of Processing Activities

The processing of personal data shall be documented in our records of processing activities (the "**Processing Records**"), maintained in the IT tool "DPOrganizer". The Processing Records contain information such as a description of the categories of data subjects and the types of personal data, the purposes of the processing, the legal basis for each processing activity and information regarding any transfer of data to third parties.

The Processing Records shall be reviewed and updated from time to time, in accordance with Section 19, so that the information contained in the Processing Records is always up to date. Only the Contact Persons and the DPM shall have access to edit the Processing Records.

The DPM is responsible for maintaining the Processing Records of the processing activities taking place on a group level. Furthermore, the DPM shall make sure that any updates on the information that shall be included in the Processing Record is communicated to all Contact Persons and that all Processing Records within the Company are at the same level as regards the quality of the information. All Contact Persons shall follow the instructions given by the DPM if the DPM finds that the Processing Records need to be supplemented or otherwise edited. Each Contact Person shall inform the DPM in case there is a need to update the Processing Records, for instance if, as part of the Company's Vendor process, a new data processor will process personal data on behalf of the Company.

12. Information to Data Subjects

The categories of data subjects whose personal data is processed by the Company are informed in different ways, as further described below. All governing documents in this Section 12 shall be reviewed by the DPM and Contact Persons, as applicable, at least annually to make sure that the information contained in the privacy notices is kept up to date. If they are changed, the DPM and Contact Persons shall be responsible for communicating the changes to the affected data subjects.

As regards employees and consultants, see this **Internal Privacy Policy**.

As regards candidates (internal or external) the relevant information will be provided as part of the application process.

As regards private customers of the Company that are natural persons with whom the Company has a direct relationship, information is provided to the customer in a privacy notice accompanying the customer agreement, by referencing the **External Privacy Policy**. The External Privacy Policy is available on our website.

As regards professional customers and institutions as well as distributors, counterparties and suppliers of the Company being companies and organizations that are legal persons, the processing of personal data is in general limited to contact details of their employees and representatives. The processing of personal data shall be regulated in the agreement entered into with the customer/distributor/supplier where the customer/distributor/supplier shall be held responsible for informing their employees and representatives of the processing that will take place.

As regards visitors of the Company's website, an external **Website Privacy Policy** shall be available at the website, which includes information on the use of cookies.

13. Rights of the Data Subjects

Each data subject is entitled to certain rights (see Section 8.10). The data subject shall have the possibility to contact the Company and exercise his/her rights. In order to handle these requests from a data subject, an email address (currently DataProtection@brummer.se) shall be provided in the applicable information texts (see Section 12 above) to which the data subject may send its requests and exercise his/her rights. The DPM shall be responsible for ensuring that the request is addressed and responded to. Once the data subject's identity is verified, the request shall be responded to as soon as possible and at the latest within a month.

14. Retention Routines and Guidelines

The Processing Records contain information about how long the data for a particular processing activity is kept. The manner and technical means of the erasure shall be agreed between the head of each department and the Chief Technology Officer (and relevant data processors in data processing agreements). As the personal data shall be erased when the purpose for which they were collected is fulfilled, different personal data in a single system may need to be erased at different times if the system/service contains personal data which has been collected for different purposes. However, if there is a legal requirement to keep parts of the data, the data shall be retained for the purpose of complying with the legal requirement. This will also include keeping records if they may be required for the establishment, exercise or defence of a legal claim.

The Company has established retention period guidelines (see Schedule 1) that contain guiding examples of retention periods within an HR, customer relationship and regulatory specific context.

15. Data breach routine and records of data breaches

A data breach is deemed to occur where there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data processed (hereafter a "**Data Breach**").

If an employee or consultant suspects that a Data Breach may have occurred, the DPM shall be informed as soon as possible, without any delay. You should not attempt to investigate the matter yourself. The employee or consultant shall make sure that the DPM acknowledges receipt of the information either by phone or physically. An email should also be sent to the following email address: GDPRnotification@brummer.se[4]. The e-mail shall clearly state that a Data Breach may be suspected.

The above routine will allow the appropriate personnel to investigate the possible breach further and take the appropriate steps.

The DPM shall as soon as possible inform the CEO of the Company, the Chief Technology Officer, Head of Legal, Head of Risk Control and the Head of Operational Risk.

In case a Data Breach has occurred, the supervisory authority shall be notified within 72 hours after we became aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the personal data breach is likely to result

4 E-mail group always to include the DPM, the CEO of the Company, the Chief Technology Officer, the Head of IT, the Head of Legal, the Head of Risk Control and the Head of Operational Risk.

in a high risk to the rights and freedoms of natural persons, the data subject shall also be notified, without undue delay. The DPM shall ensure that such notifications are carried out, however, the Contact Person shall assist and provide relevant information to the DPM.

Furthermore, all breaches that occur shall be registered in a record of data breaches, which shall comprise the facts relating to the personal data breach, its effects and the remedial action taken. The **Data Breach Record** shall enable the supervisory authority to verify compliance with the GDPR. Thus, the record shall be completed with all the information requested and shall not be modified. The Data Breach Record is subject to confidentiality and is kept and maintained by the DPM.

Additionally, the Company will handle data breaches in accordance with its general incident management processes.

16. Risk assessments

Risk assessments shall be carried out when completing the Processing Records, and otherwise as relevant. The Contact Persons shall be responsible for ensuring that the Processing Records within their respective business unit contain documentation of risk assessments.

A data protection impact assessment (DPIA) shall be conducted if a specific processing of personal data (as carried out or intended) is likely to result in a high risk to the rights and freedoms of natural persons (as typically indicated by the general risk assessment documented in the Processing Records). The DPM shall be responsible for performing DPIAs on the data processing activities carried out on group level. The Contact Persons shall inform the DPM if a DPIA may be required in respect of data processing activities carried out within their respective business unit and the DPM shall assist in such DPIA.

17. Data processing agreements (DPA) and data transfer agreements

When a data processor processes data on behalf of a data controller, a data processing agreement (DPA) shall be entered into between the data controller and the data processor. A DPA Template has been prepared by the Company and that template shall be used as a starting point. The DPM and the person responsible for the relevant procurement process shall ensure that a DPA is entered into with such processor.

The standard contractual clauses issued by the EU Commission shall be used if personal data is transferred to a country or company outside the EU/EEA. The standard contractual clauses are in such case in addition to the DPA (note that there are two versions of the

clauses; one to be used when transferring personal data to another data controller and the other to be used when transferring personal data to a data processor).

The DPA Template is available on our Intranet and the standard contractual clauses are available on:

Controller to controller:

http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_set_ii_c2004-5721.doc

Controller to processor:

http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc

18. Training

To raise awareness of privacy issues, make data protection a part of the Company's culture and improve the organisational security for the personal data processed, all employees and, as relevant, consultants, specifically the DPM and Contact Persons, shall be aware of the requirements set out in the GDPR and the adopted governing documents within the Privacy Field.

Training packages have been adopted for different roles within the Company's organisation. Such training packages may consist of, e.g. the following:

- **Introduction courses**: An introductory course on data privacy matters and rules shall be held for all employees and consultants, for the purpose of ensuring that everyone is aware of the governing documents and instructions within the Privacy Field. It is mandatory for all employees and consultants to complete the course annually. The course is provided online.

- **Advanced courses**: Tailor made courses adapted to specific departments, such as IT, HR, IR, Sales and Client Desk, shall be held on a regular basis, covering questions and topics within the Privacy Field particularly relevant for the individual department.

Completion of training is compulsory.

19. Updating the Data Privacy Documents and Records

To verify that the governing documents within the Privacy Field are correct and up to date, the following procedures shall be applied for updating the documents:

- Policies are reviewed each year by the DPM. Updated versions are to be adopted by the Board of Directors of the Company where deemed necessary or appropriate.
- Routines are reviewed each year by the DPM.
- Records are reviewed each year by the DPM for records on group level and by the Contact Persons for records made on business unit level. If there are special events in between the reviews, such as a Data Breach, implementation of a new IT system or a decision to broaden the scope of the business or the purposes for which the data is processed, the records shall be updated in connection with that event. The records shall be updated and correct at all times.
- Templates shall be reviewed each year by the DPM.

******

SCHEDULE 1
RETENTION PERIOD GUIDELINES

Introduction

Personal data shall be erased (destroyed or anonymized) as soon as the purpose for which the data was collected has been fulfilled. Thus, it is vital to know from which sources personal data processed within the organization has been collected and the purpose of the processing.

HR related data

As for HR related information, there are several laws and regulations which govern how an employer shall administer its business, e.g. with respect to salary reporting to the Swedish Tax Authority, rehab for employees, administration of sick leave, etc. In order for the employer to abide by these legal requirements, the employer must have access to certain personal data related to the employee for a certain time period. The table below is intended to serve as support in the inventory of all HR related personal data processing undertaken by a company and/or in the drafting of a registry of the personal data processing within HR. The table lists provisions in different HR related laws and regulations which contain requirements related to an employer's processing of data pertaining to its employees and the time periods for which such data may be processed. The table also lists some general processing areas and advises on how the company shall approach erasure of personal data collected for different purposes.

See also the Swedish Data Protection Authority's guidelines for data processing related to employment on http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/arbetslivet/

Other data

Although less guidance is available for retention of personal data outside of an HR context, the table below also includes a few guidelines regarding on other matters. At the end, the table includes regulatory specific guidelines regarding e.g. anti-money laundering and terrorism.

Legal requirements and consent

Please note that this list is not exhaustive and that it shall serve solely as guidance; if there is a legal requirement that information is to be retained for a certain amount of time, the legal requirement takes precedence over the guidelines.

The applicability of the guidelines may be affected where the data subject has consented to a longer retention period than what is set out below. This requires a clear consent from the data subject at the time when the personal data was collected, and the data subject must have been informed of the purposes of the processing of his or her personal data. A consent to retain personal data indefinitely or for a very long time is likely not valid. Also, consents from employees are often not regarded as freely given and therefore not valid – therefor, ensure that the employee has a real option (without negative consequences for the employee) to choose to consent or not. Furthermore, if the person withdraws a consent (including to opt-out from receiving direct marketing), the data may need to be deleted in case no other legal basis is applicable for the purpose of retaining the data.

Acting as a data processor

If we process personal data as a data processor to an external data controller, the erasure routines and retention periods shall be specified in the data processing agreement with the controller.

HR Process	Personal Data and Processing	Retention Period
0. General HR data	Any data which is collected to administer an employment and which is not specifically covered below, such as name, age, gender, next of kin contact details, all personal data processing pertaining to the employee's email account, grades, CV, references, etc.	With respect to HR data, the fundamental principle is that data shall be erased when the employee is no longer employed by the employer, i.e. personal data shall be erased **as soon as the employment terminates.** When an employment is terminated, there is normally no reason to keep the employee's email account or information about the employee on the company's website. The information shall therefore be removed within reasonable time, typically **within one (1) month**. However, individual emails that are relevant for the business may be archived for as long as relevant (typically up to ten years), provided that the archiving does not require the email account to be kept.
1. Recruitment	Receipt of work applications. Applications may be submitted to the company or through a recruitment agency. Data typically processed in connection herewith is name, CV, interview notes, etc. Occasionally, tests are performed where the test results are kept by the employer.	In order to defend against legal claims from the applicant regarding an employment decision, the personal data may be kept for **two (2) years** from the decision. For recruitment purposes, personal data in an application, interview notes and information from references may be registered and kept for **six (6) months** or as long as they are relevant in the recruitment process. The applicant's consent is required if the employer wishes to keep data for a longer period, e.g. for future recruitments. The information text to which the applicant consents shall contain information on how long the company will keep the application documents, e.g. for two years.
2.1 Absence - Parental Leave and care of sick child (*Sw: VAB*)	Receipt of notification and registration of employees' outtake of parental leave and care of sick child days (*Sw: VAB*).	Data regarding employees' outtake of parental leave and care of sick child days (*Sw: VAB*) should be erased after **two (2) years** from the time of the outtake of parental leave and care of sick child days. Information in payroll system shall be kept in accordance with the rules of the Bookkeeping Act (see point 3.1 below).
2.2 Absence - Vacation	Registration of employees' vacation day outtake and payment of vacation pay.	Upon termination of employment, data regarding employees' vacation day outtake shall be erased **two (2) years** from the end of the relevant vacation year. During current employment, data of employees' vacation day outtake shall be kept in accordance with the rules for vacation days.
2.3 Absence - Sick Leave	Registration and administering employees' sick leave.	Personal data on sick leave / sick pay in the payroll system must be kept in accordance with the Bookkeeping Act (see point 3.1 below). Other personal data shall be erased two (2) years from the sick leave.

2.4 Absence - Administration of rehab for employees	Registering and administration of rehab for employees and follow-up related hereto.	Information on sick leave in payroll systems for the administration of correct sick pay shall be stored/erased in accordance with the Bookkeeping Act (see point 3.1 below). Assurance of sick pay (*Sw. försäkran för sjuklön*) and sick notification (*Sw. sjukanmälan*) is erased as soon as the employment ends; Other personal data relating to the rehab shall be erased **as soon as the employment is terminated**.
2.5 Absence/injury - Report of work related injury/incident	Reporting of work related injury and incident to managers and safety officers.	Personal data relating to the injury/incident shall be erased **ten (10) years** after the injury/incident occurred.
3.1 Finance – Bookkeeping	Accounting records, e.g .balance sheets, books of prime entry and general ledgers, annual reports, agreements and other information which is significant in order to explain the financial circumstances of the operations.	Personal data included in the accounting record shall be kept for **seven (7) years + present year** according to the *Bookkeeping Act (SFS 1999:1078)*, *Sw: bokföringslagen*. The personal data should be erased upon expiry of this period.
3.2 Finance - Administration of occasional pension payments	Administration and payment of occupational pension to employees.	Any data that may be necessary for the calculation and administration of correct pension provisions at an individual level shall not be erased.
3.3 Finance - Payroll	Administration of salary payments.	Information on salary payments relevant for the calculations of pensions shall not be erased (see point 3.2 above). Other information containing personal data relevant for the administration of salary payment shall be kept in accordance with the Bookkeeping Act (see point 3.1 above).
3.4 Finance - The Tax Authorities	Mandatory HR related reporting, such as income statements, tax deduction, attendance records, etc.	Personal data shall be kept in accordance with the Bookkeeping Act (see point 3.1 above).
4.1 Development and planning - Skills and competency database	Registration of employees' skills and competences.	During the course of employment, erasure should occur at a certain time interval, tentatively every **third (3) to fifth (5) years**. Upon termination of employment, the data may not be kept except if it is kept to defend against legal claims in accordance with point 5 below.
4.2 Development and planning - Appraisals and performance measuring	Registration of protocol from appraisals and performance measuring.	During the course of employment, erasure should occur at a certain time interval, tentatively every **third (3) to fifth (5) years**. Upon termination of employment, the data may not be kept except if it is kept to defend against legal claims in accordance with point 5 below.

4.3 Development and planning - Succession planning	Right of priority list for personnel (*Sw: turordningslista*).	The data shall be erased **two (2) years** from termination of employment in accordance with the *Employment Protection Act (SFS 1982:80)*.
4.4 Development and planning - Documentation in accordance with discrimination legislation	Documentation of actions undertaken in accordance with Section 3 of the Discrimination Act, e.g. pay surveys.	During the course of employment, erasure should occur at a certain time interval, tentatively every **third (3) to fifth (5) years**. Upon termination of employment, the data shall be deleted **two (2) years** from the termination.
5. Termination employee	Collection of background information in relation to termination of employee, termination documentation, negotiation protocols from negotiations with the union.	Personal data relevant for the termination shall in general be erased **two (2) years** after the employment is terminated. In case of termination initiated by the employee him/herself, the information shall be erased **four (4) months** after the termination. Information that may need to be kept to answer requests regarding unemployment fund (*Sw: a-kassa*) from the Swedish Social Insurance Agency (*Sw: Försäkringskassan*), e.g. period of employment, job attendance and cause of termination, may be kept and erased in accordance with the Bookkeeping Act (see point 3.1 above). The employer may retain factual information pertaining to the employment after the termination of the employment, such as "employment terminated due to redundancy", "dismissal" and "termination for personal reasons" and grades and employment certificates with appraisals that the employer has given to the employee.
6. Consultants	Processing of personal data pertaining to individual consultants in order to administer the work performed by the consultant.	Personal data shall in general be erased **as soon as the agreement is terminated**. However, to the extent that the personal data of the consultant has been stored among employee data, such data shall be erased after two (2) years from the completion of the consultant's assignment. The consultancy agreement (which is concluded with a legal entity) shall be stored in accordance with regular routines that the company applies to business contracts.
7. Camera surveillance (CCTV)	Camera recording	Recordings shall be deleted upon **two (2) months** from the date of recording (the company may submit an application with the relevant supervisory authority for an extended retention period), in accordance with the Camera Surveillance Act (2013:460) (*Sw. Kameraövervakningslagen*).
8. Miscellaneous - examples of other types of HR related processing of personal data.	Benefit portals, travel planner for work-related travel, logging of employees' use of work computer, access control system, preventive health care, etc.	Personal data shall be erased **as soon as the employment is terminated**. Remember to check legal requirements and consider how the company's business is structured to ensure that all processing within HR is covered and that all such data is erased within the stipulated time frame.

Customer related	Personal Data and Processing	Retention Period
9. Direct marketing	Processing of personal data pertaining to an existing or potential customer for direct marketing actions directed at such individual.	Personal data processed for direct marketing purposes shall be erased no later than **one (1) year** after the customer relationship has expired, or earlier if the customer has objected to direct marketing. Please note however that longer retention periods may be permitted if there is consent from the individual.
10. Information on potential customers / investors	Information on potential customers / investors such as name, contact details, employer and position.	Provided that the information only includes work related information on the potential customer / investor (e.g. job email address and not private email addresses), the personal data may be kept for as long the company considers the individual as a prospect (note that contact details should be kept up to date and that the individuals have certain rights, e.g. a right to be forgotten and a right to request not to be contacted for marketing purposes).
11. Customers / Investors	Administration of customer / investor relationship, e.g. delivery of information, communication with customer / investor (including maintaining the customer / investor relationship).	The company may process personal data pertaining to a customer / investor while there is an on-going relationship with that customer. As a general matter, once the relationship has ended, e.g. because the customer / investor has cancelled its account / investment or the customer / investor has exercised its right to withdraw from the contract, the data should be erased after 10 years. This would mean that all customer / investor data shall be erased following the expiry of a **10-year period staring upon the termination of the customer / investor relationship** (e.g. from the most recent transaction, provided that the customer / investor no longer has any holdings with us). The length of this 10-year period has been established in order for us to ensure a high level of customer service and to allow us to maintain capability to report to relevant authorities.
11. Customer complaints	Maintaining the Complaints Register	Documentation regarding customer complaints shall be kept so that it is possible to follow the handling of the complaint and shall be kept as long as the dispute continues with the customer, and for a period of **3 years** thereafter.
12. Inactive account	Processing of personal data pertaining to an inactive customer.	Over the course of time, some customers will become inactive or unresponsive. An email or other appropriate communication should be sent after **twelve (12) months** of inactivity asking the user to log in to its account in order to keep it. If the user does not act upon this then the user account and information retained therein should be deleted.

		However, make sure the above practice complies with terms and conditions applicable to the account, including the termination and expiration provisions contained therein. This is particularly important if the user has paid for the service.
13. Credit rating	Collecting of financial information pertaining to a natural individual or sole proprietorship (*Sw. enskild firma*) with the purpose of obtaining a credit rating on such individual or sole proprietorship.	Personal data collected, e.g. from credit rating institutes, with the purpose of obtaining a credit rating shall be erased within **three (3) months** of collection.

Industry specific and regulatory	**Personal Data and Processing**	**Retention Period**
14. Know your client	Collecting personal records and data as part of know your client.	Personal records and data collected as part of actions taken for retaining customer knowledge shall be kept for at least **five (5) years** after the end of the business relationship with the customer or after the date of an occasional transaction. In accordance with FFFS 2017:11, the data shall be kept for **ten (10) years** if (i) it indicates that money-laundering or financing of terrorism has occurred or property otherwise is derived from criminal activities (ii) it has been reported to the police authority in accordance with anti-money laundering and terrorist financing legislation and (iii) a public authority has informed the company that the data needs to be kept for the extended time period.
15. Know your client	Collecting personal records and data as part of transactions carried out with the customers in the context of a business relation or in individual transactions that are subject to customer knowledge.	Personal records and data collected as part of transactions carried out with customers in the context of a business relation or in individual transactions that are subject to customer knowledge shall be kept for at least **five (5) years** after the end of the business relationship with the customer or after the date of an occasional transaction. In accordance with FFFS 2017:11, the data shall be kept for **ten (10) years** if (i) it indicates that money-laundering or financing of terrorism has occurred or property otherwise is derived from criminal activities (ii) it has been reported to the police authority in accordance with anti-money laundering and terrorist financing legislation and (iii) a public authority has informed the company that the data needs to be kept for the extended time period.
16. FATCA related information	Information regarding activities performed to identify whether an account is subject to the reporting requirements	The information shall be kept for a period of at least **five (5) years** from the date the relevant account is closed.