Background
On May 25, 2018, the General Data Protection Regulation (GDPR) started to apply in Sweden.

The regulation applies as law in all EU member states and aims to improve the protection of the individual in the processing of personal data. It contains, inter alia, rules about what rights to information and access to personal data you have, rules about correcting incorrect personal data and in some cases the ability to limit the processing of personal data.

Proxy P Management AB ("**Proxy**") has a personal data protection policy ("**Policy**") that is updated as a result of GDPR. Below we describe the main features of the Policy.

Principles for collecting personal data
Proxys operations consist of management of funds. We will only process personal data as part of running our normal day-to-day operations.

Proxy is responsible for personal data and we protect the protection of your individual rights and personal data.

We process personal data in a legal, accurate and transparent manner. The requirement that the processing of personal data be legal implies, among other things, that there must be a legal basis for every treatment. That personal data should be processed in an open manner means, among other things, that it should be clear how personal data is collected and otherwise processed.

Personal data must only be collected for special, explicit and justified purposes. This means that we must have the objectives ready for us even before the collection of personal data begins. The personal data must then not be processed in a manner incompatible with these purposes.

We must follow the principle of data minimization, which means that personal data must be adequate, relevant and not too comprehensive in relation to the purposes for which they are processed. In other words, we do not collect personal information for indefinite future needs. Furthermore, personal data collected may not be processed if, for example, the data are so old that it is no longer relevant for the original purposes.

The personal data must be accurate and up to date. We take all reasonable steps to ensure that erroneous personal data is erased or rectified without delay. In addition, if required for the purposes, the personal data must be updated.

We must adhere to the principle of storage minimization, which means that personal data must not be stored, i.e. stored in a form that enables identification, for a longer period of time than is necessary for the purposes for which the personal data is processed. When the personal data is no longer needed for these purposes, it must be deleted or de-identified.

According to the principle of privacy and confidentiality, personal data must be protected, among other things, against unauthorized or unauthorized treatment and against loss, destruction or injury by accident.

We have a responsibility to comply with the principles of personal data processing. We should be able to show how the principles are followed. For our part, this is primarily done through the Policy and the measures taken based on the Policy.

Categories of personal data and how the data is collected
Processing of personal data should primarily be done with regard to customers and potential customers, including representatives and real principals, and representatives of companies and organizations with whom we have or may have a business relationship, as well as authorities.

The personal data we process can be divided into the following categories:

- Identification information: social security number and name
- Contact information: for example, telephone numbers and addresses
- Financial information: for example, transaction information
- Information required by law: for example tax residence or foreign tax registration number, information required for basic customer knowledge and combating money laundering
- Special categories of personal data: for example, certain information about employees

As a starting point, personal data should be collected directly from you or generated by your activities with us. As a new customer, for example, we ask for personal information such as name, social security number, e-mail address and telephone number. If you send e-mails to us, it may contain personal data that we process in such cases.

However, sometimes information is required from a third party. For example, information may need to be collected to keep data up-to-date or to verify the information we have collected from the data subject. These may be public or other externally available sources in the form of registers kept by authorities (for example, SPAR), sanctions lists (at EU and UN) and other commercial information providers of information on, for example, real principals and persons in political positions. In connection with payments, we collect information from banks.

Purpose and legal basis for processing personal data
We will use your personal information to fulfill legal and contractual obligations, as well as to provide you with information, offers and other services.

The legal bases for our processing of personal data are as follows:

- Personal data is used to carry out agreements.
- In addition to the execution of agreements, we process personal data in order to fulfill obligations laid down by law, other regulations or governmental decisions.
- Personal data is also processed following a balance of interests in connection with marketing and product and customer analyzes. The purpose of this

treatment is partly marketing and business development. We do this to improve our product range and offerings. We believe that both the customer and Proxy have an interest in using personal data in this way.

- There may be times when we ask for your consent to process your personal information. This may be the case, for example, at customer meetings or if you choose to subscribe to information from us. If you have consented to the processing of your personal data, you can always withdraw the consent.

Change of purpose
We will only use your personal information for the uses and purposes set out above, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original uses and purposes. If we need to use your personal information for an unrelated purpose, we will notify you and will explain the legal basis which allows us to do so.

Automated decision making
We do not apply automated decision making.

Information shared
Except with your consent as described above, we will not provide any of your personal information to any other third parties not listed below without your specific consent. Information collected may be shared with our staff, partners, affiliates, attorneys, third party service providers and where applicable accountants and auditors and as otherwise required or permitted by law.

How we protect your information
We understand the importance of appropriately safeguarding information you provide to us. It is our practice to protect the confidentiality of this information, limit access to this information to those with a business need, and not disclose this information unless required or permitted by law.

We have security practices and procedures in place to protect data entrusted to us. These procedures and related standards include limiting access to data and regularly testing and auditing our security practices and technologies.

All employees are required to complete privacy, security, ethics and compliance training. We also offer a wide variety of other training to all employees and temporary workers to help us achieve our goal of protecting your information. Ultimately, no website, mobile application, database or system is completely secure or "hacker proof." While no one can guarantee that your personal information will not be disclosed, misused or lost by accident or by the unauthorized acts of others, we continuously review and make enhancements to how we protect client information. Further, we cannot control dissemination of personal information you post on or through our website using any social networking tools we may provide and you should have no expectation of privacy in respect of such information.

Retention of data
It may not always be possible to completely remove or delete all of your information from our databases without some residual data because of backups and other reasons. We will retain your information for as long as your information is necessary for the purposes for which it was collected. For example, we may retain your personal

data if it is reasonably necessary to comply with any legal obligations, meet any regulatory requirements, resolve any disputes or litigation, or as otherwise needed to enforce the Policy and prevent fraud and abuse. If requested by a law enforcement authority, we may also be required to retain your personal data for a period of time.

Your legal rights
Under certain circumstances, you have rights under EU data protection laws in relation to your personal information:
- Right to withdraw consent at any time.
- Right to request access to your personal data.
- Right to object to processing of your personal data.
- Right to request correction of your personal data. • Right to request erasure of your personal data.
- Right to request transfer of your personal data.
- Right to request restriction of processing.
- Right to make a complaint.

Data Transfers
The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission website: "Adequacy of the protection of personal data in non-EU countries".

Personal data breach
A personal data breach is a security incident that results in accidental or unlawful destruction, loss or alteration or unauthorized disclosure of or unauthorized access to the personal data that has been transferred, stored or otherwise processed.

In the case of a personal data breach, we shall, without undue delay, and, if possible, not later than 72 hours after knowing about it, report the personal data incident to Datainspektionen, unless it is unlikely that the personal data breach involves a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it must be accompanied by a reason for the delay.

If the personal data breach is likely to lead to a high risk for the rights and freedoms of natural persons, we shall also inform the data subject of the personal data breach without undue delay.

Personal Data Record
Proxy has a register of its processing of personal data. What is included in the register is explicitly stated in the GDPR, for example the purposes of the processing, description of the categories of data subjects and categories of personal data, any external recipients of the personal data and whether data is transferred to a third country.

Obligation to report under contract or law
The personal data collected from you are in many cases partly those required by law, partly those that are contractual requirements and partly those that are

necessary to conclude an agreement. This means that we may be prevented from entering into an agreement with you if information is not provided.

Effective date and changes to the Policy
The Policy is effective as of 25 May 2018. We are continually improving and adding to the features and functionality of our website and the services we offer. As a result of these changes (or changes in the law), we may need to update or revise the Policy. Accordingly, we reserve the right to update or modify the Policy at any time, without prior notice.

Contact us
If you have any questions about the Policy or if you would like to exercise any rights you may have in relation to your personal information, please contact: Dan Lindström on dan.lindstrom@proxypm.se.

The right to make a complaint to Datainspektionen
You can also file a complaint or contact Datainspektionen (www.datainspektionen.se).