

PRIVACY POLICY

Oberon Insurance Intermediation AB

Table of contents

1	DATA CONTROLLER	3
2	TERMINOLOGY AND DEFINITIONS	3
3	THE COMPANY'S PROCESSING OF PERSONAL DATA.....	4
3.1	BACKGROUND.....	4
3.2	CONTACTS WITH PROSPECTIVE CLIENTS.....	4
3.3	CLIENT REGISTRATION	5
3.4	CLIENT DUE DILIGENCE (KNOW YOUR CUSTOMER)	5
3.5	ADMINISTRATION OF CLIENT ASSIGNMENTS (INCLUDING EXECUTION OF INSURANCE DISTRIBUTION SERVICES)	7
3.6	RECRUITMENT	8
3.7	SUPPLIERS AND BUSINESS PARTNERS.....	9
3.8	WHISTLEBLOWING.....	10
4	THE RIGHTS OF THE DATA SUBJECT	11
4.1	RIGHT TO ACCESS (SO-CALLED EXTRACT FROM THE REGISTER)	11
4.2	RIGHT TO RECTIFICATION, DELETION OR LIMITATION	12
4.3	RIGHT TO OBJECT TO CERTAIN TYPES OF PROCESSING.....	12
4.4	RIGHT TO DATA PORTABILITY	12
4.5	THE RIGHT TO WITHDRAW CONSENT	13
4.6	RIGHT TO COMPLAIN ABOUT THE PROCESSING OF PERSONAL DATA.....	13
5	HOW DOES THE COMPANY PROTECT THE DATA SUBJECTS PERSONAL DATA?.....	13
6	TRANSFER OF DATA TO THIRD PARTIES.....	13
7	TRANSFER OF DATA TO THIRD COUNTRIES	14
8	CHANGES TO THE PRIVACY POLICY	15

1 DATA CONTROLLER

As data controller Oberon Insurance Intermediation AB, 559472-4642, (the 'Company', 'we', 'us' or 'our') is responsible for the processing of personal data relating to the Company's activities as stated by this policy. If you have any questions regarding the processing of personal data or wishes to exercise your rights in accordance with section 4, kindly contact us as follows.

Oberon Insurance Intermediation AB

Hovslagargatan 5

111 48 Stockholm

INFO@OBERONINSURANCE.COM

2 TERMINOLOGY AND DEFINITIONS

For the purposes of this policy, the following terms shall have the meanings set forth below:

Personal data refers to any information that can be directly or indirectly attributed to a natural person. For example, images and sound recordings processed electronically may constitute personal data even if no names are mentioned. Encrypted data and various kinds of electronic identities (such as IP numbers) are personal data if they can be linked to natural persons.

Sensitive data refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing of personal data means any operation or set of operations which is performed on personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, transmission or deletion.

The **data subject** refers to the person to whom the personal data relates. In this policy, we will refer to the data subject as 'you' and 'your'.

Rights refer to the rights that data subjects have under the GDPR, which are set out below under section 5. The relevant rights are described in more detail [on the website of the Swedish Authority for Privacy Protection](#).

3 THE COMPANY'S PROCESSING OF PERSONAL DATA

3.1 Background

As a distributor of insurances, the Company is engaged in insurance distribution. In our business, we process personal data related to clients, prospective clients, suppliers/partners and persons seeking employment with us. Information about how we process personal data within each area and function where we are a data controller is set out in sections 3.2-3.8 below.

3.2 Contacts with prospective clients

Purpose and legal basis

We process personal data for the purpose of managing contacts with prospective clients. The legal basis for the processing of personal data is our legitimate interest to be able to manage contacts with prospective clients. In the balancing of interests, we have assessed that the prospective client has an interest in us being able to contact the prospective client in order to offer insurance distribution.

Categories of personal data

We process the following categories of personal data:

- Name, e-mail address and telephone number.

Recipients of personal data

The personal data is stored in Microsoft Teams. The Company may share the data with other IT and system providers that provide support for the Company's systems and cloud services.

Storage of personal data

If the contact results in a client relationship, the data is stored for the duration of the contractual relationship with the client and for a period of ten (10) years thereafter to enable the Company to defend itself against any legal claims. If no client relationship is initiated, we will store the data for one (1) year based on the Company's legitimate interest in retaining information about whom we have provided information about prices and terms and conditions. However, we will delete the personal data on an ongoing basis if you have declined further contact with us.

3.3 Client registration

Purpose and legal basis

We process personal data for the purpose of entering into a contract with the client and registering the client with the Company. The legal basis for the processing of personal data is a contract (for natural persons) and a legitimate interest for us to be able to enter into and manage client agreements (for legal persons). In the balancing of interests, we have assessed that the client has an interest in us providing insurance distribution services in a satisfactory manner and safeguarding the client's interests, which includes having contact with representatives of the client.

The provision of personal data is not a legal requirement, but it is necessary for the conclusion of a contract between the Company and the client. If the Company does not have information about its clients, the Company cannot enter into the contract with the client.

Categories of personal data

We process the following categories of personal data:

- Name, e-mail address and telephone number.

To ensure that the information is accurate and up to date, we also collect information from population registers and company registers.

Recipients of personal data

The data is stored in the Company's server provided through Office 365 Sharepoint. The Company may share data with IT and system providers that provide support for the Company's systems and cloud services.

Storage of personal data

Personal data is stored for the duration of the contractual relationship with the client and for a period of ten (10) years thereafter to enable the Company to defend itself against any legal claims.

3.4 Client due diligence (Know Your Customer)

Purpose and legal basis

Under the Money Laundering and Terrorist Financing (Prevention) Act (SFS 2017:630) the Company is obligated to have knowledge of the client before establishing a business relationship with the client. The purpose of the processing of personal data is to comply with

the legal requirements regarding client due diligence in the Money Laundering and Terrorist Financing (Prevention) Act. The legal basis for the client due diligence measures carried out by the Company is a legal obligation.

If the Company does not have sufficient knowledge of the client, including information about representatives, beneficial owners, etc. the Company cannot enter into a business relationship with the client.

Categories of personal data

In the context of our client due diligence measures, we process the following categories of personal data:

When the client is a legal person:

- Name, registered address, citizenship and social security number of the contact person/representative, which shall be evidenced by a copy of an ID document, and proof of residence according to EU standards (if the ID document is a passport copy, we will also collect information on gender and height).
- Name, registered address, citizenship and social security number, and/or tax number if different of the beneficial owner or alternate beneficial owner, which shall be evidenced by a copy of an ID document, and proof of residence according to EU standards (if the ID document is a passport copy, we will also collect information on gender and height).
- The reference number of the ID document.
- Financial information.
- Information about the beneficial owner's status as a Politically Exposed Person (hereinafter referred to as PEP), including information about profession/function.
- Name of family member or known associate who is a PEP (in the event that the beneficial owner's family member or known associate is a PEP),
- Information about offences related to the beneficial owner, and/or representative, that may be detected during checks against sanctions lists.

When the client is a natural person:

- Name, registered address, place of residence other than the place of registration, citizenship and social security number, which shall be evidenced by a copy of an ID document (if the ID document is a passport copy, we will also collect information on gender and height).
- The reference number of the ID document.
- Financial information.

- Status as PEP, including information about profession/function.
- Name of family member or known associate who is a PEP (in the event the client's family member or known associate is a PEP).
- Information about offences that may be detected during checks against sanctions lists.

Third parties with roles to the insurance:

Name, registered address, citizenship and social security number of the of appointed lives assured and/or beneficiaries to the policy, which shall be evidenced by a copy of an ID document (if the ID document is a passport copy, we will also collect information on gender and height).

In order to ensure that information processed by the Company is accurate and up to date, the Company may also obtain information from population registers, the company registers, the beneficial ownership register, sanctions list and register of persons with PEP-status.

Recipients of personal data

The personal data is stored in the Company's server provided through Office 365 Sharepoint, which is the cloud-based document storage service used by the Company. The Company may share the data with other IT and system providers who provide support for the Company's systems and cloud services.. The Company may also share data with the Swedish Financial Supervisory Authority (Sw. Finansinspektionen) and law enforcement authorities if such disclosure is required by law.

Storage of personal data

We will retain the personal data collected in accordance with our obligations under the Money Laundering and Terrorist Financing (Prevention) Act during the ongoing client relationship and for five (5) years after the end of the client relationship. If the conditions in the Swedish Financial Supervisory Authority's regulations and general guidelines (FFFS 2017:11) regarding measures against money laundering and terrorist financing are met, we are obligated to retain the personal data for ten (10) years. This may be the case, for example, if there is a suspicion of money laundering or terrorist financing, if suspected money laundering or terrorist financing has been reported to the Swedish Police Authority, or if a law enforcement authority has requested it.

3.5 Administration of client assignments (including execution of insurance distribution services)

Purpose and legal basis

We process personal data to carry out and administer the assignment and to protect the client's interests.

We process personal data for the following purposes in order to fulfil contractual obligations:

- To carry out and administer the assignment and to protect the client's interests.
- To communicate with the client by e-mail, post, and telephone.
- To manage and book meetings.
- To provide efficient and accurate documentation, administration, and management of the assignment.

The provision of personal data is not a legal requirement, but it is necessary to enable us to fulfil our agreement or our obligations towards the client.

Categories of personal data

We process the following categories of personal data.

- Name, e-mail address, address and telephone number.
- Personal identity number.
- Financial information.
- Insurance information.
- Information on tax residence and foreign tax identification number.

Recipients of personal data

The data is stored in Office 365 Sharepoint which acts as a personal data processor for us. The Company may share the data with other IT and system providers that provide support for the Company's systems and cloud services.

Storage of personal data

Personal data is stored for the duration of the contractual relationship with the client and for a period of ten (10) years thereafter in order for the Company to defend itself against any legal claims.

3.6 Recruitment

Purpose and legal basis

In order to manage applications, conduct interviews and make decisions in a recruitment process, we collect and process personal data. The overall purpose of a recruitment process is to enable us to hire people with the right characteristics for the vacant position. We may also

store personal data for the purpose of contacting the applicant in future recruitments. The legal basis for the processing is the conclusion of a contract and our legitimate interest in being able to receive and process an application for employment.

You are not required to provide us with your personal data. If you do not provide us with your personal data, we will not be able to fulfil our obligations towards you and carry out the recruitment process.

Categories of personal data

In the context of a recruitment process, we process the following categories of personal data:

- Name, address, e-mail address and telephone number.
- Where applicable, photograph of the applicant.
- Details of previous work experience as well as professional references.
- Education and training certificate.
- Contact details of any references.

It is important that you, as an applicant, do not provide information that is not relevant to the application. The application shall not contain information on ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex. Job applicants should only provide personal information about themselves in their cover letter. If we obtain references about you, we will share and receive personal data in the reference process.

Recipients of personal data

The recipients of the personal data are mainly employees and managers of the Company, and when applicable, recruitment agencies.

Storage of personal data

We will retain the personal data during the recruitment process. Deletion of collected data for those who have not been offered employment takes place after two (2) years in accordance with the Swedish Discrimination Act (SFS 2008:567).

We may save applications from candidates who are interesting for future recruitment. In such cases, the data will be stored for a maximum of two (2) years. However, you always have the option to object to such future contact by objecting to the data processing.

3.7 Suppliers and business partners

Purpose and legal basis

In order to enter and fulfil a contract with suppliers and business partners, we process personal data belonging to their representatives. The processing of personal data relating to contact persons/representatives of suppliers/business partners is intended to enable us to administer the agreement, fulfil our obligations towards our suppliers/business partners, handle deliveries and to be able to contact and communicate with suppliers/business partners.

The legal basis for our processing is our legitimate interest in being able to administer and fulfil the agreements with our suppliers/business partners. In the balancing of interests, we have assessed that the contact person/representative has an interest in us fulfilling our obligations towards our suppliers/business partners.

Categories of personal data

We process the following categories of personal data:

- Name, e-mail address, telephone number and professional title.

Recipient of personal data

The personal data is stored in Microsoft Teams.

The Company may share the data with other IT and system providers that provide support for the Company's systems and cloud services.

Storage of personal data

We store personal data in order to fulfil our agreement with each supplier/business partner. Data about contact persons/representatives is therefore processed as a starting point for as long as it is necessary for us to administer the agreement, exercise our rights and fulfil our obligations in relation to each individual supplier/business partner. In the event that your employment or assignment with the supplier/business partner ends, we will cease processing your personal data as soon as we receive such information. Agreements containing your personal data will be stored for ten (10) years from the end of our business relationship due to the limitation period in the Swedish Act on Limitation (SFS 1981:130). Furthermore, we store your personal data for seven (7) years where applicable for the purpose of verifying a transaction in accordance with the Accounting Act.

3.8 Whistleblowing

Purpose and legal basis

We process personal data in connection with reports of malpractice (whistleblowing) in order to receive and investigate the matter. The legal basis for processing personal data is a legal obligation.

It may also be necessary to process personal data in order to take any measures and to be able to provide feedback to the reporting person. In this case, the legal basis for our processing is our legitimate interest in following up on the matter and providing feedback to the reporting person. In the balancing of interests, we have assessed that the reporting person has an interest in the Company following up on the matter.

Categories of personal data

The categories of personal data that will be processed depend on the content of the report, the information provided by the reporting person and the information deemed relevant to the investigation.

Recipient of personal data

The personal data collected and processed will only be accessible to selected members of the Company's management. If a report is received by means other than the Company's reporting channel and is received by an employee who is not authorised, the documents will be forwarded to the authorised recipient as soon as possible.

Storage of personal data

Documentation in connection with a report will be handled and stored for two (2) years after the case has been closed, with the exception for violations of the money laundering regulations, in which case the documentation will be handled and stored for five (5) or ten (10) years.

4 THE RIGHTS OF THE DATA SUBJECT

4.1 Right to access (so-called extract from the register)

You have the right to be informed of the personal data processing we carry out on you. Such information shall include, among other things, a description of the purpose and legal basis for the processing, the categories of personal data concerned and the recipients of the personal data. We have summarised this information at a general level above, which is an easy way for you to obtain information about how we work with personal data. A register extract provides you with an overview of the processing so that you understand whether, and if so for what purpose, your personal data is being processed.

However, it should be noted that the right of access to data does not apply to data that we are not permitted to disclose by law, for example when we have exercised our obligation to report suspected money laundering or terrorist financing under the Money Laundering and Terrorist Financing (Prevention) Act. We may therefore refuse a request from a data subject to exercise the aforementioned right.

4.2 Right to rectification, deletion or limitation

If you believe that we have processed your personal data incorrectly or that it needs to be supplemented, you have the right to request that we correct it, and if you do not want us to continue processing your personal data, you have the right to request that we delete it. We will correct and delete personal data if this is possible in relation to our purpose for processing and the legal regulations we are obliged to comply with.

If you believe that the personal data we hold about you is incorrect, that our processing is unlawful or that we do not need the data for a specific purpose, you have the right to request that we restrict our processing of that personal data. You may also request that we do not process your personal data while we investigate whether your request to exercise your rights can be granted.

However, it should be noted that the right to rectification or deletion may be limited in some cases, as we have a legal obligation to retain certain data, for example for the purpose of preventing money laundering and terrorist financing.

4.3 Right to object to certain types of processing

You have the right to object to the processing of your personal data at any time if the legal basis for the processing is a public interest or a balance of interests. If you object, we will assess whether our interest in processing your data outweighs your interest in the personal data not being processed.

You also have the right to object to the processing of your personal data for direct marketing purposes at any time. If you no longer wish to receive marketing from us, we will stop direct marketing.

4.4 Right to data portability

You have the right to obtain the personal data you have provided to us and to transfer this data to another data controller, provided that

- (a) it is technically possible, and

(b) the legal basis for the processing is consent or that the processing was necessary for the performance of a contract.

4.5 The right to withdraw consent

If the processing of personal data is based on your consent, you have the right to withdraw this consent at any time. Such withdrawal does not affect the lawfulness of the processing of personal data prior to the withdrawal of consent.

4.6 Right to complain about the processing of personal data

You always have the right to contact the Swedish Authority for Privacy Protection if you wish to lodge a complaint regarding our processing of personal data. Contact details for the Swedish Authority for Privacy Protection is listed below.

Telephone number: 08-657 61 00

E-mail address: imy@imy.se

If you wish to exercise your rights or obtain answers to other questions, the contact details to the Company can be found in section 1. You have the right to contact the Company instead of the Swedish Authority for Privacy Protection.

5 HOW DOES THE COMPANY PROTECT THE DATA SUBJECTS PERSONAL DATA?

The Company uses IT-systems to protect the confidentiality, integrity, and availability of personal data. We have taken special security measures to protect your personal data against unlawful or unauthorized processing (unlawful access, loss, destruction or damage). Only those persons who need to process your personal data in order for us to fulfil the purposes specified in this privacy policy have access to the data.

6 TRANSFER OF DATA TO THIRD PARTIES

The Company will, from time to time, disclose information to relevant third parties (including, but not limited to, situations where the Company has a legal obligation to do so). In each case, to ensure that personal data is processed in a safe and secure manner, we have a routine of entering into data processing agreements with each external party that processes personal

data on behalf of the Company. The personal data shared by the Company is described in section 3.

7 TRANSFER OF DATA TO THIRD COUNTRIES

The Company always endeavours to process personal data only within the EU/EAA. Where applicable, the Company may share personal data with an entity in a country outside the EU/EEA, a so-called third country. In the event of a transfer to a third country, we will ensure that such transfer is carried out in accordance with applicable data protection legislation, either by basing the transfer on a decision by the European Commission on an adequate level of protection, or by using the European Commission's standard contractual clauses in combination with organisational and technical safeguards.

The following recipients outside the EU/EEA may be involved:

Courts, authorities and other public bodies

In connection with the performance of tasks for clients of the Company, the Company may need to share necessary information with courts, authorities and other public bodies outside the EU/EEA. The countries that may be involved depend on the circumstances of the individual case.

System suppliers

Microsoft Office 365 is used in the Company's operations. When Microsoft receives personal data about you, the personal data may be transferred to, for example, the United States. For more information about Microsoft's processing of personal data, kindly visit:

<https://privacy.microsoft.com/sv-se/privacystatement>

To read more about transfers to third countries and for more information about the standard contractual clauses, kindly visit:

<https://learn.microsoft.com/en-us/compliance/regulatory/offering-eu-model-clauses>

Social media (LinkedIn)

The Company uses LinkedIn. When you visit LinkedIn and use the service, your personal data is processed by LinkedIn Ireland Unlimited Company. For more information about the processing, transfer to third countries and to read the standard contractual clauses, kindly visit:

<https://se.linkedin.com/legal/privacy-policy>

<https://www.linkedin.com/help/linkedin/answer/a1343190>

8 CHANGES TO THE PRIVACY POLICY

The Company reserves the right to change and update the policy. In the event of material changes to the policy or if existing information is to be treated in a manner other than specified in the policy, the Company will provide appropriate notice.

This privacy policy was last updated on the 17 November 2025.