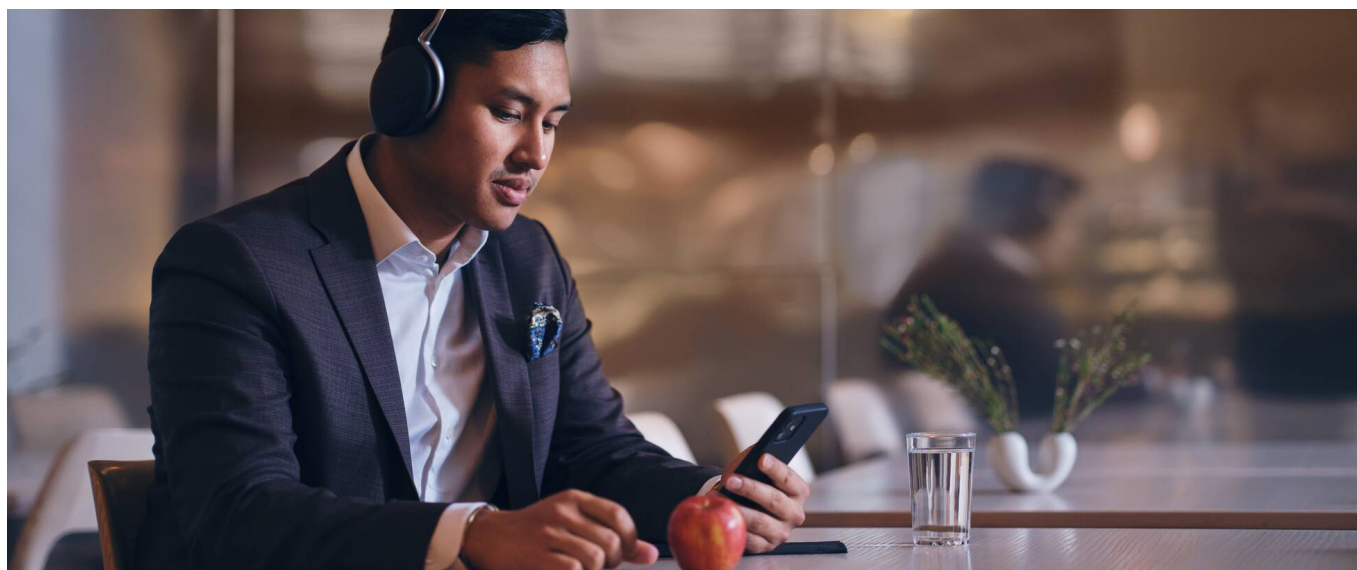


Privacy Policy

SEB Life International Assurance Company DAC



This Privacy Policy explains how we process (e.g. collect, use, share and otherwise process) any personal data about you in accordance with this Privacy Policy as well as applicable laws.

1. Who Are We?

The company responsible for the processing of your personal data is SEB Life International Assurance Company DAC, Bloodstone Building, Riverside IV, Sir John Rogerson's Quay, Dublin 2, D02 KF74, Republic of Ireland, company no. 218391, authorised by the Central Bank of Ireland as a life insurance undertaking under number C771 (the "Company"). Our contact address is as above, telephone number +353 1 487 0700, facsimile number +353 1 487 0704. You can reach our Data Protection Officer by writing to the above address or by email to: dataprotection@seb.ie.

2. What is personal data?

Personal data means any information that can be directly or indirectly attributed to a natural person, including, name and social security number or national identification number, but also other information relating to a person's physical, genetic, psychological, financial, cultural or social identity. Data such as your IP address can be considered personal data if they can be linked to you.

Some personal data are considered special categories of personal data or "sensitive data" and are subject to special rules. Sensitive personal data includes:

- Race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data that identifies a natural person;
- information about health; and
- information about a natural person's sex life or sexual orientation.

3. What data do we collect?

The company collects the following data:

- Personal identification information (Name, email address, phone number, tax identification details etc.);
- Financial information (bank account details, payment information etc.);
- Health and medical information (for underwriting and claims processing, where applicable);
- Information about beneficiaries; and
- Communication preferences

4. Whose data do we process?

We collect personal data about individuals who have entered or wish to enter into an agreement with us. Sometimes we also collect information about individuals who are insured, beneficiaries, custodians, asset managers, administrators, persons with power of attorney, insurance intermediaries, company authorised signatories; company directors or other forms of representatives, contact persons, or beneficial owners.

5. Why do we process your personal data?

We process personal data about you:

- to comply with our legal, regulatory and compliance obligations;
- to arrange, issue and administer you with a policy of insurance, or to record you as a life assured or beneficiary on a policy of insurance, to make payments of claims and benefits, and to respond to your queries relating to same;
- to reinsure the risks on your policy of insurance;
- to verify your identity, protect against potential fraud, investigate compliance oversights, and respond to complaints; and
- For policies with a nominated intermediary or asset manager: to liaise effectively with persons representing you such as your intermediary and financial adviser; and
- to invest your policy fund with an appointed asset manager and place custody of your assets and cash with a custodian.

6. What personal data do we process about You?

We only process personal data about you for the specific purposes mentioned above under Section 5, and we only process personal information that is necessary.

You provide directly to us the following categories of personal data: name and address; date and place of birth, gender; personal contact details; tax identification details; passport and personal identification card numbers and details; family members details; financial information; and details of your appointed life assured and beneficiaries.

In relation to certain life policies, we may also process certain special categories of data such as data concerning health. For anti-money laundering purposes, we collect information on whether you are a politically exposed person (PEP), which may indicate political opinions.

7. Why are we allowed to process your personal data?

Our processing of your personal data requires a legal basis. We may process your personal data described above based on the following legal bases:

- if you provide us with special categories of data (such as data concerning health), the processing may be performed with your explicit consent;
- If you are a proposer or a policyholder the processing is necessary for the performance of a contract with you or in order to take steps at your request prior to entering into a contract or the processing is necessary for our compliance with a legal obligation that we are subject to; and
- if you are a life assured (and not a policyholder) or a beneficiary or some other person (guardian, adviser, representative or pledgee) the processing is necessary for the purposes of legitimate interests pursued by us, being the payment of claims and benefits under a policy of insurance for the benefit of you or others or compliance with a legal obligation that we are subject to.

8. How do we obtain your personal data?

If you are a policyholder, we will obtain personal data directly from you and we may also receive personal data from persons acting for you, for example, intermediaries. If you are the life assured person, we will obtain personal data (which may include data concerning health) from you and also, with your consent from practitioners, physicians, dentists, members of medical professions, employees of hospitals and health authorities as well as medical facilities.

If you are named on a policy as a life assured or a beneficiary, we will obtain personal data which does not comprise data concerning health from the policyholder.

We may also obtain publicly accessible information from company registers, national population registers and compliance systems.

9. How do we share your personal data?

We may share your personal information with public authorities to comply with laws relating to anti-money laundering, terrorist financing, bribery, and corruption; to comply with laws relating to mandatory disclosure of reportable cross-border arrangements (DAC6); and for reportable accounts under the Common Reporting Standard and (if you are a 'US Person') the Foreign Account Tax Compliance Act (FATCA).

We also share information with our parent company Skandinaviska Enskilda Banken AB and its subsidiaries, agents, subcontractors and third-party service providers of the SEB Group and persons acting on our behalf such as custodians and asset managers and persons acting for you such as your intermediary. In relation to special categories of data (such as data concerning health) we also disclose the information to our reinsurer.

Your personal information may also be processed by us and other members of the SEB Group, our agents, subcontractors and third-party service providers for any other purpose required for or reasonably incidental to the performance of our duties or for the purpose of due diligence by any third parties in the context of any proposed merger, acquisition, refinancing or re-organization of our business involving such third party.

10. How do we protect your information?

Keeping financial and personal information protected is a big and important responsibility that rests with us. We have therefore taken, and continue to take, a series of protective measures which together contribute to a very high level of IT security.

Protection against computer viruses detects and prevents computer viruses from entering our computer system.

So-called firewalls and a number of other security components block intrusions by unauthorised persons. Firewalls are security systems used to protect the computer systems that are connected to the Internet.

Secure information transmission ensures that information cannot be accessed by unauthorised persons. We use encryption technology, Transport Layer Security (TLS), on those websites where sensitive information may be transmitted. With the TLS protocol, authenticity is guaranteed on the server through a digital ID certificate that is sent to the client. After that, a unique session key is generated that is used to encrypt all data sent between the server and the client. Only that client can decrypt the information and also detects if the information has changed along the way.

We continuously stay up to date with the latest trends in IT security to ensure that we always provide you with adequate information protection.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Information security

We at SEB Life International see it as a shared responsibility, together with you, to protect your data in the best possible way. Our IT security procedures and policies aim to ensure that the information we hold about you remains inaccessible to unauthorised persons.

We protect information in accordance with established security standards and procedures. And it cannot be written often enough: No employee at SEB Life International will ever contact you in any medium to obtain your password to our Customer Portal.

11. International transfers

We may transfer personal information that is collected from you to a third-party data processor located in a country that is outside of the European Economic Area in connection with the above purposes. We will only do so where the European Commission has decided that the country or the processor we are sharing your information with will protect your information adequately; or the transfer has been informed to the Data Protection Commissioner in Ireland (if required) and recorded in writing and we have entered into a contract with the processor with which we are sharing your information (on terms approved by the European Commission) to ensure your information is adequately protected.

You may request a copy of the suitable safeguards we implement for our third country processing by writing to: dataprotection@seb.ie.

12. For how long will we retain your personal data?

We will not retain your personal information any longer than necessary to fulfil the purposes for which the data were collected. This means that normally your personal data is retained 10 years after the end of the customer relationship and thereafter the data is deleted.

13. What if the provision of your personal data is mandatory?

You are obliged under certain statutory and/or contractual requirements to provide personal data to us, and the failure to comply with these requirements may mean that we are unable to issue a policy to you, or if your policy is in place, are unable to carry out wholly or partially certain matters which are necessary for the administration of your policy. Failure to provide complete and correct information may also void a claim on a policy or part of it.

14. Cookies

Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. When you visit our website, we may collect information from you automatically through cookies or similar technology.

You can set your browser not to accept cookies. However, in a few cases, some of our website features may not function as a result.

For more information on our cookies, please see our website: www.seb.ie

15. What are your rights?

We would like to make sure you are fully aware of all of your data protection rights. You are entitled to the following:

The right to access – You have the right to request the Company for copies of the personal data that the Company processes on you.

The right to rectification – You have the right to request that the Company correct any information you believe is inaccurate. You also have the right to request the Company to complete the information you believe is incomplete.

The right to erasure – You have the right to request that the Company erase your personal data, under certain conditions. You have this right if your data is no longer needed for the purposes for which it was collected, if the data have been processed illegally, or if you have objected to our processing as described below. There are limitations on this right where the processing is still necessary for the purpose it was collected and that purpose is necessary for the performance of the contract, compliance with legal obligations, or performance of a legitimate interest which outweighs your interest.

The right to restrict processing – You have the right to request that the Company restrict the processing of your personal data, under certain conditions. There are limitations on this right where the processing is still necessary for the purpose it was collected, and that purpose is necessary for the performance of the contract, compliance with legal obligations, or performance of a legitimate interest which outweighs your interest.

The right to object to processing – You have the right to object to the Company's processing of your personal data, under certain conditions.

The right to data portability – You have the right, under certain circumstances, to request the Company to provide to you a machine-readable copy of the personal data that you have provided to us. If technically possible, you also have the right to have the data moved to another actor.

The right to withdraw consent – If processing of your personal information is based on your consent, you have the right to withdraw your consent at any time. Your withdrawal will not affect the lawfulness of the processing carried out before you withdrew your consent. If you wish to withdraw your consent, such withdrawal may prejudice your right (or the right of others) to claim a benefit under a policy of insurance and/or may require us to terminate the policy as performance of the contract cannot be carried out.

There may be conditions or limitations on these data protection rights beyond those mentioned in this policy.

There is no cost for exercising any of these rights. To make any request please write to dataprotection@seb.ie.

You may lodge a complaint with the Company at dataprotection@seb.ie, or with the Data Protection Commissioner in Ireland, whom can be contacted at:

Office of the Data Protection Commissioner,

Canal House, Station Road, Portarlinton, Co. Laois, R32 AP23, Ireland.

Phone: +353 (0)761 104 800

LoCall: 1890 25 22 31

Fax: +353 57 868 4757

email: info@dataprotection.ie