

Nordben Life & Pension Insurance

Privacy Statement

TABLE OF CONTENTS

Purpose of this Privacy Statement.

How do you ensure that my data is secure?

Amendments to this Privacy Statement.

- a) What personal data do we collect?
- b) Do we collect special category data (such as health, criminal convictions)?
- c) Where do we collect personal data from?
- d) What are your legal justifications for collecting my personal data?
- e) What are the purposes for collecting my personal data?
- f) Do you process data based on automated processing?
- g) Do we collect children's data?
- h) How will my health data be used?
- i) What happens when I make a disability claim or a claim is made after my death?
- j) Who will we share personal data with?
- k) What about Direct Marketing?
- l) Where will you send my personal data?
- m) How long will you store my data for?
- n) What about Nordben employee and prospective Nordben employee data?
- o) What are my rights under the Data Protection Laws?
- p) What if I need to make a complaint?
- q) Contact Us.

GLOSSARY

This is the Privacy Statement (Statement) of Nordben Life and Pension Insurance Co. Limited ("**Nordben**", "**we**", "**our**", "**us**"). This Statement sets out how Nordben Processes Data, whether on individuals (including Personal Data in respect of individuals ("a Natural Person") who are clients, employees or former employees of corporate clients, family members or beneficiaries entitled to a payment in the event of a death of a life insurance with us) or otherwise. This Statement also sets out the rights of individuals in respect of their personal data.

There is a Glossary of terms at the end of the Statement. The terms defined in the Glossary are those with capital letters and underlined in the Statement and not otherwise explained in the Statement.

This Statement was drafted with brevity and clarity in mind. It does not provide exhaustive detail of all aspects of Nordben's collection and use of personal data.

For the purposes of the Data Protection (Bailiwick of Guernsey) Law, 2017 ("DPL") and the **EU General Data Protection Regulation 2016/679 ("GDPR")** (together the "Applicable Data Protection Laws") we are the Data Controller, which means that we are primarily responsible for making determinations about how and why we process your personal data.

PURPOSE OF THIS PRIVACY STATEMENT

To comply with the Applicable Data Protection Laws, Nordben ensures that personal data is collected in a transparent way, used fairly, stored safely and not disclosed unlawfully.

This Statement will inform you as to how we look after any personal data both when you visit our website (regardless of where you visit it from) and during the course of your relationship with us.

This Statement is accessible via our website, www.nordben.com ("Site") and is provided in a layered format so you can click through to the specific areas set out below.

HOW DO YOU ENSURE THAT MY DATA IS SECURE?

Nordben takes the protection of your personal information seriously, and has appropriate security measures and policies in place to address this. All our staff are made aware of their information security responsibilities

AMENDMENTS TO THIS STATEMENT

Nordben will amend this Statement from time to time. Where we do so, we will take appropriate steps to bring the amendment to your attention. This Statement was last updated on 25 May 2018.

If you have any questions about this Statement, including any requests to exercise your legal rights, please contact the us in writing by using the contact details set out under the heading "Contact Us" below.

(a) What personal data do we collect?

We may collect the following categories of personal data, including without limitation:

- names, addresses (including email), telephone numbers;
- bank account details;
- data relating to financial transactions;
- additional personal data details such as marital status, nationality, identification documentation (CDD), tax status/tax id numbers, professional title, employment history, income/source of wealth;
- health and medical information; and
- Technical Data including internet protocol (IP) address, login details, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this Site.

(b) Do we collect special category data (such as health, criminal convictions)?

Yes, in limited cases, we may also collect "special categories" of data ("Sensitive Personal Data").

Our money laundering, sanctions, financial crime and fraud prevention checks sometimes require us to obtain information about actual or alleged criminal convictions and offences, as well as (for example) information relating to a person's ethnicity, political opinions or religious beliefs. Such data may be processed where we check your personal data against any issued sanctions lists using third party software.

If you or your employer has applied for certain types of insurance in the past, you may have had to give details of the state of your health.

To the extent that we process such data, we will ensure that we have a lawful basis for processing it. This may either be because we are required to comply with a legal obligation imposed by an enactment, or because we have obtained your prior explicit Consent. You have a right to withdraw your consent at any time by writing to us.

(c) Where do we collect personal data from?

Such personal data may be collected:

- directly from you, your employer or former employer (as appropriate) or someone insured with us, in the course of your dealings with us, for example when you complete relevant documentation required by us (such as application forms) or in the ordinary course of interactions or communications with us (such as emails). If you email us: we may monitor emails sent to us, including file attachments, for viruses or malicious software; and
- where we record and/or monitor information for compliance or security purposes (e.g. recording of telephone calls, monitoring emails, etc.). If you call us: we may keep a written record of the phone discussion; or where you choose to leave a message on the voice mail system, this may be retained.
- **Recording of telephone calls and monitoring of emails**
 - Emails may be occasionally monitored internally to ensure compliance with acceptable policies (sender / receipt / subject lines only). Emails are also recorded by third party software whereby emails can be retrieved and reviewed as a whole; this is generally only used by Nordben to retrieve emails that have been 'lost'. This functionality is also backed up and saved as part of [Nordben's Business Continuity Plan](#)
 - Nordben does not have a telephone call recording capability to record 'live' telephone conversations. However, the voice mail system is a message recording mechanism, where users may elect to record a message.
 - From third parties or individuals acting on your behalf.
 - Where permitted, from third parties acting on our behalf and from other publicly available sources (such as an electoral register).
 - If you are applying for a job, please see our heading '[What about Nordben employee and prospective Nordben employee data?](#)'
- In addition, our Site may request and collect certain categories of data such as:
 - **Forms on Site:** name, address, phone number and e-mail address, any Policy data relating through various means, such as submitted forms and/or statement requests: To the extent that you submit any Personal Data to us via our 'Contact Us' page as an existing client.
 - **Information about your use of the Site:** An IP (Internet Protocol) address is a number that is assigned to your computer when you use the Internet. This information does not contain any personally identifiable information about you. In order to administer this Site and to help improve this Site, we may collect the IP address you are using, plus the date and time, the page requested, the type of web browser and the operating system you are using;
 - **Security and performance:** Nordben uses a third party service to help maintain the security and performance of the Site. To deliver this service it processes the IP addresses of visitors to the Site;
 - **Use of email:** Nordben's email service supports [TLS](#); should you choose to do so, if you do not use the encrypted functionality you should be aware that any emails sent or received may not be protected in transit. Nordben also monitors any emails sent, including file attachments, for viruses or malicious software. Please be aware that you have a responsibility to ensure that any email you send is within the bounds of the law; and
 - **Cookies:** A cookie is a piece of data that is sent to your web browser by a web server. It is usually stored on your computer. The same web server can subsequently retrieve the information contained in the cookie. Some cookies can be retrieved by different web servers to the one that sent them. This Site uses analytic software to collect certain data. For further information about how we uses cookies, please refer to our [Cookie Statement](#).

Policies OnLine:

In addition, users with a valid Policy login, may access a dedicated area of the Site called 'Policies OnLine'. Policies OnLine is an online database administered by us, which stores policy records electronically. By logging into Policies OnLine using your allocated username and personally set password, you are able to access and update contact details, addresses, beneficiary nomination and tax information (for tax reporting under [FATCA](#) and [CRS](#)). You may also, via Policies OnLine, prepare forms online for Policy payments (as allowable under the terms of the relevant insurance contract). Where you start to prepare a draft payment request, the website also contains 'personalised pending' functionality, which allows you to access and edit the draft form for up to 30 days. Following the period of 30 days, draft forms which have not been submitted will be deleted.

(d) What are your legal justifications for collecting my personal data?

We will only use your personal data in accordance with Applicable Data Protection Laws. Most commonly, we will use your personal data in the following circumstances:

- i. **Contract:** where we need to perform the contract we are about to enter into or have entered into with you;
- ii. **Legal obligation:** the processing is necessary for Nordben to comply with the law (not including contractual obligations);
- iii. **Legitimate interests:** the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests; and
- iv. **Consent:** in limited circumstances, where you have given clear unambiguous consent for us to process your personal data for a specific purpose. Please note we do not generally rely on this as a legal basis for processing your personal data. To the extent that consent is relied upon, you have the right to withdraw your consent at any time by writing to us.

(e) What are the purposes for collecting my personal data?

We will use your personal data for the following purposes:

- i. complying with our contractual obligations as agreed between you or a corporate client,
- ii. managing investments;
- iii. detecting and preventing financial crime such as fraud, money laundering, terrorist financing, bribery, corruption, tax evasion and to prevent the provision of financial and other services to persons who may be subject to economic or trade sanctions, on an ongoing basis ("Regulatory Assessments");
- iv. statistical analysis and assessment;
- v. retaining your personal data processed as part of our Regulatory Assessments for meeting contractual terms;
- vi. to monitor electronic communications for:
 - a. investigating, preventing, detecting and prosecuting financial crime;
 - b. enforcing and defending our and our affiliates' rights, either ourselves, or through third parties; and
 - c. quality, business analysis, training and related purposes.
- vii. otherwise as necessary to comply with applicable laws, regulations or codes of practice;
- viii. we will retain de-personalised information for as long as is necessary to help inform future actions; and
- ix. medical information received to manage disability cases or death claims (see the headings 'How will my health data be used?' and 'What happens when I make a claim for disability or a claim is made after my death?' below).

The provision of personal data by you, or a corporate client may be necessary in order for us, and other third parties to which personal data are disclosed, to comply with our legal and regulatory obligations or for the performance of any contractual relationship with you, or a corporate client, or for any other purposes, where it is in our legitimate interests to process such information, (such as those described under paragraphs i, ii, iv, v, vi(c), vii above).

(f) Do you process data based on automated processing?

No, we do not process personal data based on automated decision-making.

(g) Do you collect children's data?

We will only collect personal data relating to a child or minor where you or a corporate client has provided this information to us. Where personal data has been provided to us relating to a dependant or beneficiary who is under the age of 13 years old, we will rely upon the consent of a parent or person who has parental responsibility and who is authorised to provide such consent on behalf of that child.

(h) How will my health data be used?

Your state of health and other details (for example reports from a doctor) may have been used to decide whether and on what terms to offer insurance. It will also be used to process claims that are made. For these purposes, your health and other details may be disclosed to Nordben's appointed medical officer, to third party life reinsurers and third party administrators who are instructed to arrange medicals and tests and to return the results to Nordben.

(i) What happens when I make a disability claim or a claim is made after my death?

If you make a disability claim, Nordben may:

- obtain further information about your physical or mental health;
- obtain information about your past and concurrent claims from and share it with other third party reinsurers (this includes medical information). This may be used to assess the extent and the validity of the claim, to enable the sharing of the medical evidence and for general administrative purposes;
- pass your details to third parties (e.g. claims administrators, reinsurers, and occasionally private investigators) whom we instruct to assess certain aspects of your claim;
- obtain any other information we require (sharing your details where necessary) in order to assess your claim; and
- obtain information from your employer or former employer to assess the particular claim. This information may include details of earnings, benefits and occupational duties.

If a death claim is made after your death, Nordben will request personal data to substantiate the circumstances in relation to your death and personal details of the beneficiaries in order to make payment. Nordben may also pass your details and your beneficiaries' details to third parties (e.g. claims administrators, reinsurers, and occasionally private investigators) whom we instruct to assess certain aspects of your claim. Please note that whilst the data protection regime does not apply to deceased individuals, Nordben will continue to treat all data it handles as confidential.

(j) Who will we share personal data with?

We may disclose certain personal data:

- to external third parties in respect of the contractual services we provide. We may also engage third party technology providers who provide certain software or tax reporting capabilities, or assistance with business continuity systems;
- to our professional advisors, auditors, receivers, actuaries, investment managers, corporate services providers and administrators (where applicable);
- to reinsurers and if necessary a Nordben appointed medical officer who may, upon your prior consent, review your records to assess a claim;
- to banks;
- to courts, governmental and non-governmental regulators and ombudsmen;
- to law enforcement agencies;
- to relevant tax authorities;
- to fraud prevention agencies, who will use it to prevent financial crime such as fraud and money-laundering and to verify your identity. If financial crime is detected, you could be refused certain services, finance or employment;
- to any third party that acquires, or is interested in acquiring, all or part of our liabilities or shares, or that succeeds us in carrying on all or a part of its business, whether by merger, acquisition, reorganisation or otherwise;
- to an introducer where you have been introduced to us (for example our Shareholders); and
- as required or permitted by law.

(k) What about Direct Marketing?

Nordben does not share data with third-parties for marketing purposes.

(l) Where will you send my personal data?

Nordben will not share data with any Third Country or transfer personal data unless there are safeguards in place. We may, like many organisations, transfer your personal data outside of the European Economic Area ("EEA").

Not all countries outside of the EEA have data protection laws that are similar to those in the EEA. Some of these countries may have lower standards of data protection than in your home jurisdiction, so they may not be regarded by the European Commission (EU) as providing an adequate level of data protection. Where we transfer your information outside of the EEA, we will ensure that the transfer is subject to appropriate safeguards in accordance with the Applicable Data Protection Laws. Often, these safeguards include contractual safeguards, such as EU-approved Standard Contractual Clauses. Please do contact us if you would like more information about these safeguards or a copy of the contractual safeguards used (see the 'Contact Us' section below for further details).

(m) How long will you store my data for?

Nordben has obligations under the Applicable Data Protection Laws to only retain personal data for as long as required for the specific purpose. In general, Nordben will hold your personal data for a period of seven years after final payment is paid to you or your beneficiary (and results in the closure of the individual's business relationship with Nordben). Alternatively, Nordben will hold your personal data for a period which is more specifically documented by us in our internal data retention procedures if there is a relevant reason. Examples of relevant reasons include, where a contractual provision specifies otherwise; where the law requires a longer time period; where the length of time is reasonable to keep records to demonstrate compliance with our professional or legal obligations; and following the end of period in which litigation or investigations might arise in respect of the services that we provide to you.

Data Retention Period

Nordben's retention schedule for different categories of data is used to ensure the retention of business information for as long as it is needed. It takes account of the context within which Nordben operates, including the legal and regulatory environment, for example compliance with the fifth data protection principle, and the expectations of stakeholders.

It is intended primarily as a resource to consider the business risks of data retention and to assign relevant retention periods across Nordben's business to enable disposal activity to be carried out in a consistent and controlled manner.

(n) What about Nordben employee and prospective Nordben employee data?

Any information you send us for the purpose of a job application will be treated by us with the greatest care for that purpose only. Upon receipt, our recruitment personnel will make an informed decision as to whether to proceed with your application and invite you to attend an interview. All of the information gathered during the application/recruitment process will be taken into account when making our decision.

If you are unsuccessful following your interview for the position you have applied for, we will retain basic data about you and the reasons that you were not successful for a period of 3 months. We may ask if you would like your details to be retained on our recruitment records for a period of 6 months in case there are any opportunities in the future. If you say yes, we will keep your data for 6 months and then dispose of it in accordance with our data retention procedures.

If you are an employee of Nordben, information provided by you during the recruitment process and the course of your employment will be retained by us on your HR file for the duration of your employment plus 6 years following the end of your employment. This including any criminal records checks, fitness to work declaration, and references. After this time only basic records of employment will be retained unless deemed otherwise necessary.

(o) What are my rights under the DPL?

Under the DPL you have rights as an individual, which you can exercise in relation to the personal data that Nordben holds about you these include:

- The Right of Access to one's personal information;
- The right to object to the processing of your personal data in certain circumstances;
- The right to correct and rectify information which is regarded as inaccurate;
- The right to withdraw consent at any time, where relevant consent is relied upon as a lawful basis;
- The right to data portability, in certain circumstances;
- The right to erasure of certain information; and

- The right to request that your information is only used for restricted purposes.

These rights are not absolute: they do not always apply and exemptions may be engaged. We may, in response to a request, ask you to verify your identity and to provide information that helps us to understand your request better. If we do not comply with your request, we will explain why.

To exercise any of these rights, or if you have any other questions about our use of your information, please contact us at the details set out in the '[Contact Us](#)' section below.

If you are unhappy with the way we have handled your information you have a right to complain to the data protection regulator in the EU Member State / EEA where you live or work, or where you think a breach of your personal information has taken place.

For non EU countries to the Guernsey local [Data Protection Authority](#), this is 'The Office of the Data Protection Commissioner'. Details of her office, including your rights to appeal under the DPL can be found at: <https://dataci.gg/>

(p) What if I need to make a complaint?

Please contact us using the details under the heading '[Contact Us](#)' below. When Nordben receives a complaint a record is set up containing the details of the complaint. This normally contains the identity of the complainant and any other individuals involved in the complaint.

Nordben will only use the personal data collected to process the complaint and to check on the level of service Nordben provides. Nordben will keep personal data contained in complaint files in line with Nordben's retention policy. This means that information relating to a complaint will be retained for seven years from the closure of the individual's business relationship with Nordben. It will be retained in a secure environment and access to it will be restricted according to the 'need to know' principle.

Similarly, where enquiries are submitted, Nordben will only use the personal data supplied to deal with the enquiry and any subsequent issues and to check on the level of service Nordben provides.

(q) Contact Us

If you would like to update the personal information that you have provided or if you wish to review the personal data that we hold about you, please contact us at: dataprotection@nordben.com

However, Nordben would be happy to provide any additional information or explanation needed. Any requests for this should be sent to the address below:

Nordben Life and Pension Insurance Co. Limited
Harbour House
South Esplanade
St Peter Port
Guernsey
GY1 1AP, Channel Islands

GLOSSARY

Definitions explained.

"Applicable Data Protection Laws"

The GDPR and the DPL (once it becomes law).

"Business Continuity Plan"

Is a contingency plan put in place by Nordben should an event occur whereby Nordben is unable to operate normally.

"Consent"

Consent is to be freely given, specific, informed and unambiguous indication of an Individual's wishes, by which an individual, by a statement or clear affirmative action, agrees to the processing of personal data about her/him. Explicit consent is needed for processing special category data.

"CRS"

Common Reporting Standard is a "Global Standard for Automatic Exchange of Information" issued by the Organization for Economic Cooperation and Development (OECD) which facilitates the exchange of detailed account information between governments. Guernsey, like a number of other countries, signed an agreement in July 2015 to automatically exchange information under the Common Reporting Standard. This obliges a large number of financial institutions and non-financial foreign entities to collect, verify and report information on its customers to the Guernsey Tax Authorities.

"Data Controller"

Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or to be processed.

"Data Protection Authority"

The Office of the Data Protection Commissioner in Guernsey (or such other name as may be given to it from time to time) or shall bear the meaning ascribed in the GDPR.

"DPL"

Data Protection (Bailiwick of Guernsey) Law, 2017

"EEA"

The European Economic Area (EEA) includes EU countries and also Iceland, Liechtenstein and Norway.

"FATCA"

Foreign Account Tax Compliance Act is a United States federal law that requires US persons, including individuals who live outside the US, to report their financial accounts held outside of the US, and requires Foreign Financial Institutions to report to the US Internal Revenue Service (IRS) about their US clients.

"GDPR"

EU General Data Protection Regulation 2016/679

"Legitimate interest"

Legitimate interest is to have legitimate reasons for processing personal data that the other data conditions for processing do not specifically deal with. In order to rely on this condition as a lawful basis for processing, we must ensure that our legitimate business reasons for processing the personal data do not override your rights and freedoms as a data subject.

The “legitimate interests” condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual.

Where there is a serious mismatch between competing interests, the individual’s legitimate interests will come first.

"Natural Person"

A natural person is an identifiable, living individual.

"Personal data"

Means any information relating to an identified or identifiable natural person who can be identified directly from the data, or from the data and other information which is in Nordben's possession, or likely to come into possession of Nordben as the data controller.

In particular a natural person who can be identified by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity as defined under the GDPR.

It does not need to be particularly sensitive information and can be as little as a name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, including individuals or employees which benefit from a Policy where Nordben has a relationship with a corporate client.

"Policies Online"

Is an online database administered by Nordben which stores policy records electronically.

"Processes Data"

Data Processing means collecting, amending, handling, storing or disclosing personal information.

"Regulatory Assessments"

To undertake the detection and prevention of financial crime such as fraud, money laundering, terrorist financing, bribery, corruption, tax evasion and to prevent the provision of financial and other services to persons who may be subject to economic or trade sanctions, on an ongoing basis.

"Right of Access"

All individuals have the right to access the information Nordben holds about them and to request correction of data where inaccuracies have been identified. The DPL requires Nordben to take reasonable steps to ensure that the rights of people about whom information is held can be fully exercised under the DPL.

"Sensitive Personal data"

Means personal data consisting of data about:

- Racial or ethnic origin;
- Political affiliations;
- Religion or similar beliefs;
- Trade union membership;
- Physical or mental health; and
- Sexuality or Criminal record or proceedings

"Site"

www.nordben.com

"Standard Contractual Clauses"

Means the standard contractual clauses for the transfer of personal data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU (or as may be amended from time to time).

"Technical Data"

The log file maintained by the servers hosts both the public site and an internal Policies Online site that records the following details:

- Date & time on the server the site was visited;
- IP address of the visiting computer;
- The browser software used to view the site;
- Plug-ins for the browser to view specific content (i.e. Adobe Acrobat to view a PDF document);
- The type of computer used to view the site (i.e. PC, MAC, iPhone etc.);
- The Operating System software the viewer's computer is using; and
- The referring site (i.e. was the site / page arrived at as a result of a search from the likes of Google, Bing etc.)

"Third Country"

A country that is not subject to a positive finding of adequacy by the Commission nor signed up to the EU-US Privacy Shield.

"TLS"

Transport Layer Security is a protocol that utilises encryption to provide privacy and data integrity between two communicating applications such as email or a web site.